REVISTA ELECTRÓNICA DE DIREITO

RED

La protección de datos desde el diseño y por defecto como obligación legal preventiva de la domótica

Data protection by design and default as a preventive legal obligation of home automation

Idoia Landa Reza

Profesora Ayudante Doctora de la Unviersidad del País Vasco (UPV/EHU)

Manuel Lardizabal Ibilbidea, 2, 20018 Donostia, Gipuzkoa, España

idoia.landa@ehu.eus

https://orcid.org/0000-0002-8345-4117

Mayo de 2024

RESUMEN: Aunque el control de la luz, agua, calefacción o persianas parezca parte de una película de ciencia ficción, ya es una realidad. Por ende, el derecho ha de dar respuesta a los riesgos jurídicos que plantea el uso de esta tecnología. No solo a los problemas técnicos y de seguridad tanto para el inmueble o el usuario, sino los relativos al derecho fundamental a la protección de datos personales del interesado. El hecho de recoger y almacenar automáticamente datos en un hogar tiene sus riesgos, si un dispositivo no tiene una medida de seguridad suficiente, puede existir una brecha de seguridad, lo cual puede traer la perdida de control de los datos personales. Un sistema domótico está compuesto de muchos dispositivos que pueden ser de diversos fabricantes. Por ello, es necesario identificar un sistema que acredite el respeto del derecho a la protección de datos personales durante todo el ciclo de vida de los mismos.

PALABRAS CLAVE: domótica; protección de datos; certificado, interesado.

ABSTRACT: Although the control of light, water, heating or blinds seems like part of a science fiction movie, it is already a reality. Therefore, the law must respond to the legal risks posed by the use of this technology. Not only to technical and security problems for the property or the user, but also those related to the fundamental right data protection of the data subject. The action of collecting and storing data automatically in a home has its risks; if a device does not have a sufficient security measure, there may be a security breach, which can lead to loss of control of personal data. A home automation system is made up of many devices that can be from various manufacturers. Therefore, it is necessary to identify a system that accredits the respect of the data protection throughout their entire life cycle.

KEY WORDS: home automation; data protection; certificate; data subject.

SUMARIO:

1. Introducción

Se podría llegar a pensar que el concepto de la domótica es algo nuevo, sin embargo, su origen se remonta a los años 70 del siglo pasado. Hoy en día no se puede concebir un edificio sin agua o electricidad, pero las viviendas no siempre han incluido estas comodidades[1]. En esta línea, la revolución digital ha llegado a los hogares, siendo cada vez más habitual que los ciudadanos cuenten, entre otras cuestiones, con detectores, persianas motorizadas, sensores de temperatura y humedad, controladores de climatización o bombillas inteligentes en sus hogares, pudiendo todos estos elementos ser controlados y programados desde la aplicación móvil del usuario. Aunque este control de la electricidad, agua o gas parezca parte de una película de ciencia ficción, ya es una realidad, por ende, el derecho ha de dar respuesta a los riesgos jurídicos que plantea el uso de esta tecnología.

Cualquiera de las tareas que se realizan en una vivienda susceptibles de ser automatizadas (tareas repetitivas o que deban ejecutarse como consecuencia de unas condiciones predeterminadas y unos resultados prestablecidos) pueden ser controladas por un sistema electrónico o un autómata. Este toma información del entorno (detectores, pulsadores, interruptores, termostatos, etc.) y acciona, cuando se cumplan unas determinadas condiciones prestablecidas por el usuario. Hasta hace poco tiempo, en las viviendas podían únicamente instalarse pequeñas automatizaciones, independientes entre sí, para controlar distintos servicios (iluminación, calefacción, etc.). Hoy puede decirse que las posibilidades de la domótica solo se ven limitadas por la imaginación humana[2].

En suma, la domótica ha evolucionado, ofreciendo soluciones a todo tipo de vivienda y necesidades del usuario. Su utilización es cada vez más intuitiva y para todo tipo de público. Sin perjuicio de lo anterior, desde el momento en que se tratan datos personales, su uso plantea riesgos desde la perspectiva del derecho a la protección de datos personales del usuario, debiendo analizar si existe alguna herramienta jurídica que haga frente a los mismos.

2. ¿Qué es la domótica?

El término de la domótica proviene de la palabra latina *domus*, que significa casa, y de la palabra francesa *informatique*, de la que ha derivado la palabra informática. La domótica proporciona algún nivel de automatización dentro de la casa, pudiendo ser desde un simple temporizador para encender la luz hasta el sistema más complejo capaz de interactuar con cualquier elemento eléctrico de la casa. La vivienda domótica es aquella que integra una serie

[1] SUSANA MILLÁN ÁNGELES, *Metodología y criterios para evaluar la influencia de la domótica y su preinstalación en los edificios en función de los condicionantes constructivos y de la envolvente interior*, Tesis doctoral, Universidad Politecnica de Madrid, 2014, p. 35; CRISTOBAL ROMERO; FRANCISCO VÁZQUEZ, CARLOS DE CASTRO, *Domótica e Inmótica. Viviendas y edificios inteligentes*, Ra-ma, Madrid, 2010, p. 23.
[2] FRANCISCO, GUZMÁN NAVARRO, *Domótica: gestión de la energía y gestión técnica de edificios*, RA-MA, Madrid, 2015, pp. 20-25.

de automatismos en materia de electricidad, electrónica, robótica, informática y telecomunicaciones, con el objetivo de asegurar al usuario, entre otras cuestiones, un aumento del confort y ahorro energético[3].

Por su parte, la Real Academia Española (RAE) define el presente concepto como un conjunto de sistemas que automatizan las diferentes instalaciones de una vivienda[4]. La definición de la vivienda domótica o inteligente presenta múltiples versiones y matices, y son diversos los términos utilizados en distintos idiomas: casa inteligente (*smart home*), automatización de viviendas (*home automation*), domótica (*domotique*), sistemas domóticos (*home systems*), etc[5]. Sin perjuicio de lo anterior, entre las definiciones existen elementos comunes: una tecnología de automatismos de maniobra, gestión y control de los diversos aparatos de una vivienda, que permiten aumentar el confort del usuario, su seguridad y el ahorro del consumo energético; conjunto de sistemas de seguridad y de la regulación de las tareas domésticas; conjunto de servicios de la vivienda garantizado por sistemas que realizan varias funciones[6].

Para la creación de este sistema se requiere un cerebro o central (unidad del sistema capaz de recibir y procesar la información), sensores (transforma una variable física medida y la transforma en una señal) y actuadores (recibe las órdenes: sirenas, lámparas, etc.). En relación con lo anterior, con el fin de controlar remotamente la vivienda, aparte de la red domótica interna necesitamos una red de acceso a Internet. Es posible una domótica sin Internet, pero si no existe esta conexión a la red no podremos controlar las funciones de forma remota desde una aplicación móvil. Usando un simple ejemplo, en el cuento "Alibaba y los 40 ladrones", la única forma para entrar o salir de la cueva era haciendo uso de una palabra mágica "ábrete sésamo". Aunque se podría decir que la puerta se abría o cerraba con magia, lo cierto es que se utilizaba un comando de voz, y este es un elemento de la domótica[7].

La domótica proporciona una integración de las diferentes instalaciones de las que se compone una vivienda, ya sea en materia de electricidad, electrónica, informática, ocio, multimedia y comunicaciones[8]. Lo que diferencia una vivienda domótica de una vivienda tradicional es que, en la primera, mediante la instalación de un sistema se permite controlar de forma eficiente, entre otros, el agua, el gas, la electricidad y la calefacción. Entre los objetivos de la domótica destacan el ahorro energético, el confort, la seguridad de la vivienda, las comunicaciones y la accesibilidad[9] .

En cuanto al ahorro energético, mediante la gestión eficiente de la vivienda, lo cual hace referencia, entre otras cuestiones, a la programación de las calderas, persianas y cargas eléctricas, la domótica ofrece una posibilidad de ahorro energético. Así, contribuye a conseguir

[3] JOSÉ MANUEL HUIDOBRO MOYA y RAMÓN JESÚS MILLÁN TEJEDOR, *Manual de Domótica*, Creaciones copyright, Madrid, 2010, p. 4.
[4] RAE, Definición de domótico, disponible en: https://dle.rae.es/dom%C3%B3tico (Última consulta: 27.05.2024).
[5] Véase al respecto: MARÍA AURORA FLÓREZ DE LA COLINA, "Hacia una definición de la domótica", *Informes de la construcción*, Vol. 56, núm. 494, 2004, pp. 13 y ss.
[6] MANUEL JIMÉNEZ BUENDÍA, *Desarrollo de sistemas domóticos utilizando un enfoque dirigido por modelos*, Tesis doctoral, Universidad Politécnica de Cartagena, 2009, p. 10.
[7] S TARLEARN, *Robótica, biónica y domótica: usando arduino y tinkercad*. Ra-Ma, Madrid, 2023, p. 145.
[8] NÚÑEZ A., *Domótica e inmótica KNX: guía práctica para el instalador*, Ediciones Experiencia, Barcelona, 2015, p.11.
[9] JOSÉ MANUEL HUIDOBRO MOYA y RAMÓN JESÚS MILLÁN TEJEDOR, *Manual de Domótica*, *cit*., p. 6.

la eficiencia energética al permitir realizar una gestión más eficiente del uso de la energía del hogar[10]. A su vez, la posibilidad de gestionar y programar el uso energético desde un dispositivo móvil otorga un confort al usuario del sistema[11]. Ni tan siquiera es necesario que el interesado se encuentre dentro del hogar, puede controlar todas las funciones desde la aplicación que se encuentra en su móvil. El concepto de confort va dirigido principalmente a las instalaciones de climatización, ventilación y calefacción, aunque también se incluyen en este campo los sistemas de audio y vídeo, control de iluminación, riego y jardines, mando a distancia y todo aquello que contribuya al bienestar y la comodidad de las personas que utilicen las instalaciones.

Son ejemplos de sistemas de seguridad las alarmas de intrusión para evitar robos o los detectores de fuego, humo, gas, fugas y escapes de agua. Todo ello hace que las viviendas sean más seguras, evitando accidentes en el hogar. Igualmente, el sistema instalado en la vivienda suele estar dotado de una infraestructura de comunicaciones que proporciona teleasistencia, telemantenimiento, informes de consumo y costes, así como la transmisión de las alarmas y resto de avisos.

Por último, la domótica es una de las herramientas que hacen que una casa sea accesible para las personas con limitaciones funcionales, puesto que favorece su autonomía personal, mejora su calidad de vida y seguridad. Especialmente interesante para las personas mayores o personas con discapacidad, tanto física como mental, para fomentar una vida idenpendiente. Por ejemplo, apagar la estufa y así evitar un posible fuego, apagar las luces mediante voz desde la cama, encenderlas según sensores de movimiento por si se levantan a la noche, videollamada controlada por voz para casos de caídas, etc. Las principales actuaciones de la domótica estos casos se centrarían en la automatización, según sus necesidades, con el fin de crear una vivienda segura y de confort. La seguridad a través de la domótica dota de mayor autonomía al enfermo, pero también al cuidador, en el sentido de que pueda compaginar el cuidado con la actividad laboral lo mejor posible[12].

En relación con todo lo antedicho, y destacando la característica del ahorro energético, cabe manifestar que la domótica cobra especial importancia ante los problemas energéticos de la sociedad actual debido a la eficiencia energética que brinda. No obstante, a pesar de los evidentes beneficios que ofrecen las viviendas verdes, tal y como se ha indicado en el punto anterior, es necesario responder a los riesgos que puede implicar el uso de estas herramientas desde la perspectiva del derecho fundamental a la protección de datos personales del usuario final.

---

[10] Véase al respecto: JAIME TORRES-JAIME; JAIME VÁZQUEZ-COLÍN; FRANCISCO JAVIER CASTILLO-SUBDIAZ; ENRIQUE CONTRERAS-CALDERÓN; ROBERTO URZÚA-RANGEL; y GABRIEL BELTRÁN-ROMÁN, "Ahorro de energía en aplicaciones electrónicas de la domótica", *Programación Matemática y Software*, Vol. 6, núm. 2, 2014.

[11] El concepto de confort va dirigido principalmente a las instalaciones de climatización, ventilación y calefacción, aunque también se incluyen en este campo los sistemas de audio y vídeo, control de iluminación, riego y jardines, mando a distancia y todo aquello que contribuya al bienestar y la comodidad de las personas que utilicen las instalaciones. Véase al respecto: MANUEL JIMÉNEZ BUENDÍA, *Desarrollo de sistemas domóticos utilizando un enfoque dirigido por modelos*, *cit.*, p. 13.

[12] FRANCISCA RAMÓN FERNÁNDEZ, *Vivienda inteligente: domótica, inteligencia artificial y regulación legal*, Tirant lo Blanch, Valencia, 2022, p. 100.

Con la irrupcion de la Inteligencia Artificial, en adelante IA, la domótica se separa en dos vertientes: la domótica tradicional y la domótica inteligente. Se ha de tener en cuenta que la IA es una disciplina científica que se ocupa de crear programas informáticos que ejecutan operaciones comparables a las que realiza la mente humana, como el aprendizaje o el razonamiento lógico. La IA emula algunas de las facultades intelectuales humanas (percepción sensorial como la visión y audición, y su posterior reconocimiento de patrones[13]. Así, tras la recopilación de los datos personales mediante los diversos sensoles y la posterior aplicación de la IA, se reconocerán los patrones del usuario pudiendo tomar decisiones.

La vivienda inteligente (*Smart Home*) basada en la IA no debe entenderse como una vivienda futurista en la que la persona que la habite esté rodeada de una alta tecnología que permita controlar distintas funciones. Se trata de una vivienda que se adpta, que "piensa" y responde a una serie de necesidades del usuario. Esto es, es una vivienda contemporánea, adaptada a las nuevas trecnologías. Sin embargo, hay que tener en cuenta que el factor humano es esencial, ya que la optimización de resultado de la instalación domótica va a depender del grado de actuación del habitante. El sistema puede tomar decisiones para paliar que se produzca un consumo excesivo, pero toda esta información también permite al habitante observar su actividad, pudiendo tomar decisiones sobre su consumo.

En otras palabras, la domótica hace referencia a la automatización mediante dispositivos y aplicaciones. Sin embargo, la vivienda inteligente utiliza la inteligencia artificial para tomar decisiones automáticas en el hogar. El objetivo de estas dos vertientes es la automatización, pero la forma de conseguir dicho fin es distinta.

3. Normativa aplicable

Actualmente no existe una única norma que regule la dómotica a nivel nacional. Por consiguiente, es necesario analizar las distintas normas que hacen referencia a la automatización de la vivienda, con el fin de comprender los diversos aspectos de la automatización e informatización.

Entre la normativa más destacable, cabe mencionar el Real Decreto 842/2002, de 2 de agosto, por el que se aprueba el Reglamento electrotécnico para baja tensión (BOE núm. 224, de 18.09.2002). En este Real Decreto se establecen las condiciones técnicas y las garantías necesarias que deben cumplir las instalaciones de baja tensión para garantizar la seguridad de las personas y asegurar el normal funcionamiento de las instalaciones y servicios. En la instrucción técnica complementaria del reglamento electrotécnico de baja tensión número 51 sobre instalaciones de sistemas de automatización, gestión técnica de la energía y seguridad para viviendas y edificios (ITC-BT-51), se contempla la domótica de forma específica.

[13] RAÚL ENÍTEZ; GERARD ESCUDERO; SAMIR KANAAN y DAVID MASIP, Inteligencia artificial avanzada, UOC, Barcelona, 2014, p. 12.

Según la ITC-BT-51, los sistemas de automatización, gestión de la energía y seguridad para viviendas y edificios son aquellos sistemas centralizados o descentralizados, capaces de recoger información proveniente de unas entradas (sensores o mandos), procesarla y emitir órdenes a unos actuadores o salidas. Se entiende por sensores a los dispositivos encargados de recoger la información de los diferentes parámetros a controlar (temperatura, presencia de una persona, escape de gas, etc.) y enviársela al nodo. El nodo recibe y procesa la información. Por último, los actuadores son los dispositivos encargados de realizar el control de algún elemento del sistema, como por ejemplo, electroválvulas (suministro de agua, gas, etc.), motores (persianas, puertas, etc.), sirenas de alarma o reguladores de luz[14].

Por ejemplo, dentro de una vivienda un sensor de movimiento detecta un cuerpo extraño, se procesa la información y se emite la orden de encender la luz, cuya duración dependerá de lo que haya programado el usuario. Siguiendo este ejemplo, el sensor es un dispositivo de entrada, la información de la detección del cuerpo se envía al nodo, quien procesa la misma y envía la orden de encender la luz al actuador. Cuando todos los componentes del sistema se unen a un nodo central, y este dispone de funciones de control y mando, estaremos ante un sistema centralizado. Por el contrario, cuando cada dispositivo tiene su propio procesador, hablamos de un sistema descentralizado.

Por su parte, el Real Decreto 346/2011, de 11 de marzo, por el que se aprueba el Reglamento regulador de las infraestructuras comunes de telecomunicaciones para el acceso a los servicios de telecomunicación en el interior de las edificaciones (BOE núm. 78, de 1 de abril de 2011), ICT, entre otras cuestiones, incide en la necesidad de que las infraestructuras de telecomunicaciones de las edificaciones sean diseñadas de forma que resulte sencilla su evolución y adaptación contribuyendo al proceso de acercamiento de las viviendas al concepto de "hogar digital", y a la obtención de los beneficios que éste proporciona a sus usuarios. En este sentido, se define el presente concepto como el lugar donde, mediante la convergencia de infraestructuras, equipamientos y servicios, son atendidas las necesidades de sus habitantes en materia de confort, seguridad, ahorro energético e integración medioambiental, comunicación y acceso a contenidos multimedia, teletrabajo, formación y ocio.

El artículo 36 del Real Decreto 106/2018, de 9 de marzo, por el que se regula el Plan Estataal de Vivienda 2018-2021, relativo a las acciones destinadas a la mejora de la eficiencia energética y la sostenibilidad de las viviendas, hace referencia a la instalación de sistemas de domótica. Igualmente, en base al artículo 43 de la citada norma, la instalación de un sistema domótico es identificado como una tecnologia que favorece la autonomia personal de las personas de edad avanzada o personas con discapacidad. Por su parte, el Real Decreto-ley

[14] Los sensores son dispositivos encargados de recoger la información de los diferentes parámetros a controlar (temperatura, presencia de una persona, escape de gas, etc.) y enviársela al nodo. El nodo recibe y procesa la información. Por último, los actuadores son los dispositivos encargados de realizar el control de algún elemento del sistema, como por ejemplo, electroválvulas (suministro de agua, gas, etc.), motores (persianas, puertas, etc.), sirenas de alarma, reguladores de luz, etc. Véase al respecto: JOSÉ MANUEL HUIDOBRO MOYA y RAMÓN JESÚS MILLÁN TEJEDOR, *Manual de Domótica*, *cit.*, p. 28; apartado 2º de la ITC-BT-51 ("terminología").

25/2020, de 3 de julio, de medidas urgentes para apoyar la reactivación económica y el empleo, en su artículo 14 recoge a la domótica entre las categorías de proyectos financiables.

A su vez, cabe citar la norma UNE-EN IEC 63044-6:2022 relativa a los sistemas electrónicos para viviendas y edificios (HBES por sus siglas en inglés) y sistemas de automatización y control de edificios (BACS por sus siglas en inglés) del Organismo de Normalización en España, designado por el Ministerio de Economía, Industria y Competitividad ante la Comisión Europea. En esta norma se recogen los requisitos generales de seguridad funcional para productos destinados a integrarse en las indicadas viviendas.

En relación directa con la automatización, cobra especial importancia citar Reglamento de inteligencia artificial, recientemente aprobado. El reglamento centra el grueso de su regulación en los sistemas de alto riesgo, los cuales deben cumplir los requisitos de los artículos 8-15 de la sección 2 para poder ser permitidos. Asimismo, se introducen unos requisitos específicos para los proveedores, fabricantes de productos, importadores, distribuidores y usuarios. Los cuales serán responsables del tratamiento en base a la normativa de protección de datos personales.

Entre los requisitos generales, adquiere especial importancia la vigilancia humana que se regula en el artículo 14 del reglamento, elemento que está claramente inspirado en la prohibición de la toma de decisiones basada únicamente en el tratamiento automatizado del artículo 22 del RGPD. Los sistemas de IA de alto riesgo se han de diseñar y desarrollar de modo que puedan ser vigilados de manera efectiva por personas físicas durante el período que estén en uso, lo que incluye dotarlos de una herramienta de interfaz humano-máquina adecuada, entre otras cuestiones.

4. Datos de consumo: datos personales

En relación directa con el apartado anterior, y en materia de protección de datos personales, se ha de indicar que cuando una persona utiliza un sistema de dómotica en su hogar, concede una serie de datos personales necesarios para realizar el registro, pero también entran en juego los datos de consumo energéticos. Aunque no se encuentran regulados específicamente en 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 (DOUE núm. 119, de 4 de mayo de 2016), en adelante RGPD, se clasifican como datos personales porque pueden dar información sobre las costumbres o hábitos de los usuarios. Valga como ejemplo el uso de los aplicativos que controlan los horarios de uso de la luz o de la calefacción, lo cual permite saber si esa persona vive sola o acompañada y los horarios en los que se encuentra en casa. Por todo ello, pueden ser clasificados como datos personales, dado que ofrecen una información social determinada de una persona.

En este mismo sentido, el Tribunal Supremo en su sentencia de 12 de julio de 2019[15] declaró que los datos de consumo energéticos domésticos son datos personales por reflejar determinados hábitos de conducta privados de una persona física identificable, lo cual atañe sustancialmente a la esfera privada de la intimidad de cada consumidor.

Dada su consideración de datos de carácter personal quedan sometidos a la normativa de protección de datos personales, esto es, RGPD, y Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (BOE núm. 294, de 6 de diciembre de 2018), en adelante LOPDGDD. Toda esta información, junto con otros datos de las personas, puede utilizarse para la generación de perfiles y diversas finalidades adicionales, lo cual cobra gran importancia desde la perspectiva del derecho a la protección de datos personales.

5. El consentimiento del interesado como base legal aplicable

Dado que ha quedado acreditado que lo datos de consumo son datos personales, se requiere de una base legal para realizar el tratamiendo de los mismo. En este sentido, el referido tratamiento de los datos personales se puede justificar, principalmente, en la base legal del consentimiento del interesado (artículo 6.1.a del RGPD y artículo 6.1 de la LOPDGDD). Esto no significa que el indicado tratamiento no pueda justificarse en otra base legal del RGPD, como por ejemplo, cuando el tratamiento es necesario para la ejecución de un contrato (artículo 6.1.b del RGPD), sino que esta es la vía o base principal. Tal y como se ha manifestado anteriormente, la domótica se estructura mendiante un cerebro o central, sensores y actuadores. Los diversos fabricantes ofrecen su producto, y para el funcionamiento de este el usuario debe ofrecer su consentimiento.

Igualmente, si en el uso de la domótica se realiza el tratamiento de datos biométricos del usuario, como sucede en el caso de utilizar un asistente de voz, la base legitimadora será el consentimiento explicito del interesado regulado en el artículo 9.2.a) del RGPD[16].

En todo caso será necesario que este consentimiento sea libre, informado, específico e inequívoco. Esto es, se han de cumplir los indicados cuatro requisitos para comprender que el consentimiento del interesado es válido, y por tanto, el tratamiento de los datos personales es lícito. El usuario tendrá derecho a retirar su consentimiento en cualquier momento y no deberá sufrir ningún perjuicio por ello (Art. 7.3 del RGPD).

[15] STS, Sala Tercera de lo Contencioso-administrativo, 1062/2019, de 12 de julio de 2019 (Rec. núm. 4980/2018).
[16] CEPD, Directrices 2/2021 sobre los asistentes de voz virtuales, 7 de julio de 2021, p.14.

5.1. Libre

El presente término implica elección y control reales por parte del interesado. El consentimiento quedará invalidado por cualquier influencia o presión inadecuada ejercida sobre el interesado que impida un ejercicio libre de su voluntad. Para comprender que el consentimiento ha sido concedido de forma libre, se tienen que cumplir cuatro requisitos: inexistencia del desequilibrio de poder, inexistencia de la condicionalidad, la granularidad y inexistencia de perjuicio[17].

Si existe un desequilibro entre la posición del responsable del tratamiento y el interesado, el consentimiento no tendrá todas las garantías. Por consiguiente, se deben tomar todas las medidas necesarias para que la desigualdad no condicione el consentimiento del interesado. Igualmente, el consentimiento no debe de vincularse a la aceptación de los términos o condiciones. En este sentido, según manifestó la AEPD, la instalación y utilización de un aplicativo no puede estar condicionada a la obtención de un consentimiento para un tratamiento no necesario para proporcionar el servicio definido en la misma[18], lo cual cobra especial importancia en el ámbito de la domótica.

En cuanto a la granularidad, el consentimiento no será libre cuando se impide o dificulta autorizar por separado las distintas operaciones de tratamiento de datos personales (Considerando 43 del RGPD). Para que el consentimiento sea válido, la solución radica en separar los propósitos y la obtención del consentimiento para cada uno de los mismos. Por último, si el interesado sufre un perjuicio al negar o retirar su consentimiento, no estaremos ante un consentimiento libre (Considerando 42 del RGPD).

5.2. Específico

El responsable del tratamiento debe identificar y expresar adecuadamente el fin del tratamiento como garantía contra la desviación del uso, separar las solicitudes de consentimiento, y diferenciar la información para las actividades de tratamiento de datos personales y la información relativa a otras cuestiones. Con ello se pretende garantizar un nivel de control y transparencia para el interesado, dando opción a este a elegir con respecto a cada uno de dichos fines y una garantía contra la desviación del uso[19]. El consentimiento debe tener concretamente por objeto el tratamiento de datos de que se trate y no puede deducirse de una manifestación de voluntad que tenga un objeto distinto[20].

[17] CEPD, Directrices 5/2020 sobre el consentimiento en el sentido del Reglamento (UE) 2016/679, 4 de mayo de 2020, p. 6.
[18] AEPD, "El deber de informar y otras medidas de responsabilidad proactiva en apps para dispositivos móviles", *aepd*, 17 de septiembre de 2019, p. 2, disponible en: https://www.aepd.es/sites/default/files/2019-11/nota-tecnica-apps-moviles.pdf (Última consulta: 27.05.2024).
[19] ANDONI POLO ROCA, "El derecho a la protección de datos personales y su reflejo en el consentimiento del interesado", *Revista de derecho político*, núm. 108, 2020, p. 185.
[20] STJUE, Gran Sala, de 1 de octubre de 2019, Planet 49, C-673/17, ECLI:EU:C:2019:801, apartado 58.

El principio de limitación de la finalidad implica la obligación de que los datos sean tratados con una o varias finalidades determinadas, explícitas y legítimas y, la prohibición de que los datos recogidos con unos fines determinados, explícitos y legítimos sean tratados posteriormente de una manera incompatible con esos fines[21]. Así, según el artículo 5.1.b) del RGPD los datos personales serán recogidos con fines determinados, explícitos y legítimos, y no serán tratados ulteriormente de manera incompatible con dichos fines[22]. Por ende, se autorizará el tratamiento posterior siempre que no sea incompatible y si los requisitos de legalidad también se cumplen simultáneamente[23]. En cuanto a la posible reutilización de los datos para una nueva finalidad, si el primer tratamiento se basó en el consentimiento específico del titular, se requiere siempre un nuevo consentimiento específico para el segundo tratamiento[24].

5.3. Informado

El interesado tiene derecho a ser informado sobre todos aquellos elementos que son necesarios para que pueda formar su voluntad y decidir si consiente el tratamiento de sus datos personales o no[25]. En este sentido, según ha manifestado el Tribunal Constitucional, el deber de información es parte del contenido esencial del derecho a la protección de datos, dado que resulta un complemento indispensable de la necesidad de consentimiento del afectado. El responsable del tratamiento tiene la obligación de facilitar toda la información necesaria al titular de los datos personales[26].

El artículo 13 del RGPD recoge la información que deberá facilitarse cuando los datos personales se obtengan directamente del interesado, y el artículo 14 del RGPD la información que deberá facilitarse cuando los datos no se obtengan del interesado. Junto con la obligación de informar del responsable del tratamiento, se ha de identificar un principio que cambia las reglas del juego: el principio de transparencia. No solo se ha de cumplir con la obligación de informar, sino que se ha de analizar la forma en la que se ha informado. Según el Considerando 39 del RGPD, el principio de transparencia exige que toda información y comunicación relativa al tratamiento de los datos personales debe ser fácilmente accesible y fácil de entender, y que se utilice un lenguaje sencillo y claro. Si el responsable no proporciona información accesible,

[21] AEPD, "Principios", *aepd*, 30 de agosto de 2019, disponible en: https://www.aepd.es/es/derechos-y-deberes/cumple-tus-deberes/principios#:~:text=Principio%20de%20%E2%80%9C%20limitaci%C3%B3n%20de%20la,leg%C3%ADtimos%20sean%20tratados%20posteriormente%20de (Última consulta: 27.05.2024).
[22] STJUE, Sala Primera, de 20 de octubre de 2022, Digi Távközlési és Szolgáltató Kft contra Nemzeti Adatvédelmi és Információszabadság Hatóság, asunto C-77/21, ECLI:EU:C:2022:805.
[23] GT29, Opinión 3/2013 sobre la limitación de la finalidad (WP 203), de 2 de abril de 2013, p. 21.
[24] STJUE, Gran Sala, de 1 de octubre de 2019, Planet 49, C-673/17, ECLI:EU:C:2019:801.
[25] AEPD, "Informe sobre políticas de privacidad en internet", *aepd*, septiembre de 2018, p. 15, disponible en: https://www.aepd.es/sites/default/files/2019-09/informe-politicas-de-privacidad-adaptacion-RGPD.pdf (Última consulta: 27.05.2024).
[26] GT29, Dictamen 1/2010 sobre los conceptos de «responsable del tratamiento» y «encargado del tratamiento», 00264/10/ES (WP 169), de 16 de febrero de 2010, p. 4; STJUE (Gran Sala), de 10 de julio de 2018, Jehovan todistajat, C–25/17, ECLI:EU:C:2018:551.

el control del usuario será ilusorio y el consentimiento no constituirá una base válida para el tratamiento de los datos. Se recomienda adoptar un modelo de información por capas o niveles. Este enfoque consiste en presentar una información básica en un primer nivel y remitir a la información adicional en un segundo nivel donde se presentará detalladamente el resto de la información.

5.4. Inequívoco

En base al artículo 4.11 del RGPD, el consentimiento debe prestarse mediante una acción o declaración afirmativa por parte del interesado. No debe existir ninguna duda sobre la voluntad del interesado. Para ello, el procedimiento de su obtención y otorgamiento no tiene que dejar ninguna duda sobre la intención del interesado al dar su consentimiento[27].

El interesado debe realizar una declaración verbal, por escrito o incluso por medios electrónicos. La acción positiva e inequívoca puede consistir en marcar una casilla de un sitio web en Internet, escoger parámetros técnicos para la utilización de servicios de la sociedad de la información, o cualquier otra declaración o conducta que indique claramente que el interesado acepta la propuesta de tratamiento de sus datos personales. El silencio, las casillas previamente marcadas[28] o la inactividad no deben constituir un consentimiento[29]. En consecuencia, seguir navegando en una página web no se considera suficiente para comprender que existe un consentimiento válido[30].

En el caso de las categorías especiales de datos personales, se requiere un consentimiento explícito del interesado, esto es, una declaración activa, clara e inequívoca del interesado que podrá ser por escrito, verbalmente, mediante comunicación telemática o por cualquier otro medio[31]. Por ende, debido a la sensibilidad de dichos datos personales, el legislador introduce mayores requisitos para la base legal de consentimiento del interesado.

[27] STJUE, Gran Sala, de 1 de octubre de 2019, Planet 49, C-673/17, ECLI:EU:C:2019:801, apartado 54: "*el consentimiento del interesado puede hacer que tal tratamiento se considere lícito siempre que dicho consentimiento haya sido dado «de forma inequívoca» por el interesado. Pues bien, solo un comportamiento activo por parte del interesado con el que manifieste su consentimiento puede cumplir este requisito".*
[28] Ibid, apartado 52: *"el consentimiento dado mediante una casilla marcada por defecto no implica un comportamiento activo por parte del usuario de un sitio de Internet".*
[29] Considerando 32 del RGPD.
[30] CEPD, Directrices 5/2020 sobre el consentimiento en el sentido del Reglamento (UE) 2016/679, *cit.*, pp. 18-19.
[31] JAVIER APARICIO SALOM y MARÍA VIDAL LASO, *Estudio sobre la protección de datos*, *cit.*, p. 151.

6. La protección de datos desde el diseño y por defecto como obligación legal preventiva

Gracias a la introducción del artículo 25 del RGPD, el legislador europeo ha creado un nuevo concepto que ha de ser aplicado con el fin de respetar en todo momento el derecho fundamental de protección de datos personales del usuario; cumplimiento que se acredita mediante la herramienta de la certificación[32]. Así, se persigue evitar una brecha de seguridad, comprendido como un incidente de seguridad que afecta a datos de carácter personal. Este nuevo concepto puede ser separado en dos partes: la protección de datos desde el diseño y la protección de datos por defecto.

6.1. La protección de datos desde el diseño

En base al artículo 25 del RGPD, se han de establecer estrategias que incorporen medidas para respetar el derecho a la protección de datos a lo largo de todo el ciclo de vida del objeto. El concepto del objeto hace referencia a cualquier sistema, aplicación, producto y servicio; y por ciclo de vida del objeto todas las etapas por las que atraviesa este, desde su concepción hasta su retirada, pasando por las fases de desarrollo, puesta en producción, operación, mantenimiento y retirada[33]. Así, a la hora de crear un objeto que vaya a realizar un tratamiento de datos personales se deberán identificar los posibles riesgos y crear las medidas oportunas para evitar que los mismos se materialicen.

El responsable del tratamiento debe crear una estrategia para proteger el derecho fundamental a la protección de datos del interesado desde el principio[34] y hasta el final del tratamiento de los datos personales. Desde el diseño inicial o creación y el desarrollo de un instrumento tecnológico[35], se ha de tener en consideración el derecho a la protección de datos como un elemento indispensable. Mediante el artículo objeto de análisis, se ha instaurado un modelo de cumplimiento preventivo y proactivo en lugar de defensivo y sancionador[36]. Es una manera de prevenir e impedir el daño, en vez de repararlo una vez se haya producido. En otras palabras, el enfoque es la prevención y la reducción de los riesgos con el objetivo de proteger el derecho a la protección de datos personales del usuario.

Las medidas y las garantías necesarias deben ser idóneas para conseguir el fin previsto, deben aplicar los principios de protección de datos de forma efectiva, el requisito de que sean

[32] Artículos 25.3 y 42 del RGPD.
[33] AEPD, Guía de privacidad desde el diseño, 5 de octubre de 2019, pp. 6-7, disponible en: https://www.aepd.es/documento/guia-privacidad-desde-diseno.pdf (Última consulta: 27.05.2024).
[34] MIGUEL RECIO GAYO, "Protección de datos desde el diseño: principio y obligación en el RGPD", *elderecho*, 20 de febrero de 2017, disponible en: https://elderecho.com/proteccion-de-datos-desde-el-diseno-principio-y-obligacion-en-el-rgpd (Última consulta: 27.05.2024).
[35] ELENA GIL GONZÁLEZ, *Big data, privacidad y protección de datos*, Boletin Oficial del Estado, Madrid, 2016, p. 135.
[36] GARCÍA MEXÍA PABLO y PERETE RAMÍREZ CARMEN, "Internet y el Reglamento General de Protección de Datos", en JOSÉ LÓPEZ CALVO (coord), *El nuevo marco regulatorio derivado del Reglamento Europeo de Protección de Datos*, Bosch, Madrid, 2018, p. 180.

apropiadas está estrechamente ligado al requisito de la efectividad. Una medida técnica u organizativa o una garantía puede ser cualquier cosa desde la aplicación de soluciones técnicas avanzadas hasta la formación básica del personal. Las empresas deberán adoptar políticas internas, utilizar técnicas innovadoras y realizar evaluaciones de impacto[37] para cumplir con esta obligación[38]. Las medidas elegidas garantizarán que la actividad de tratamiento de datos personales no incumpla los principios del artículo 5 del RGPD.

No es una capa adicional que se añade a algo preexistente, sino que debe estar integrada en el conjunto de requisitos desde el mismo momento en el que se concibe y diseña el producto. Igualmente, el derecho a la protección de datos debe estar asegurado durante todo el ciclo de vida del sistema, aplicación, servicio o producto. Esto es, las estrategias que incorporen el derecho a la protección de datos deberán estar establecidas a lo largo de todo el ciclo de vida del mismo; debiendo analizar detenidamente las distintas operaciones e implementar, en cada una de ellas, las medidas más adecuadas para proteger los datos[39].

Es obligación del responsable del tratamiento tener en cuenta el progreso actual de la tecnología disponible en el mercado a la hora de determinar las medidas técnicas y organizativas adecuadas. El responsable del tratamiento debe conocer y mantenerse al día de los avances tecnológicos, de cómo la tecnología puede presentar riesgos u oportunidades para la protección de datos, y de cómo aplicar las medidas y garantías que aseguran la aplicación efectiva de los principios y derechos de los interesados teniendo en cuenta la evolución del panorama tecnológico. Este criterio también se aplica a las medidas de carácter organizativo como las relativas a formaciones de reciclaje tecnológica. La falta de medidas organizativas adecuadas puede reducir o incluso restar toda efectividad a la tecnología elegida[40].

El responsable debe tomar en consideración la naturaleza, ámbito, contexto y fines del tratamiento de datos personales para determinar las medidas que han de ser adoptadas. Debe analizar adecuadamente las características del tratamiento de los datos personales que se realizará con el fin de comprender el impacto que tendrá dicho tratamiento en el derecho a la protección de datos del titular. No es lo mismo tratar un dato personal "normal" que uno sensible, como por ejemplo un dato biométrico como es la voz.

De la misma manera, es obligación del responsable del tratamiento determinar los riesgos que entraña una violación de los principios para los derechos de los interesados, su probabilidad y gravedad para poder aplicar medidas que mitiguen de forma efectiva los riesgos detectados. En este sentido, se identifica a la evaluación de impacto como elemento clave para la correcta implantación de la protección de datos desde el diseño. La evaluación de impacto consiste en realizar un análisis de los riesgos que un servicio, producto o aplicación puede suponer para el derecho a la protección de datos de los interesados, de manera que tras la realización de ese

[37] Artículo 35 del RGPD.
[38] ANNA ROMANOU, "The necessity of the implementation of Privacy by Design in sectors where data protection concerns arise", *Computer law & security review*, vol. 34, núm. 1, 2018, p. 102.
[39] AEPD, Guía de privacidad desde el diseño, *cit.*, p.9.
[40] CEPD, Directrices 4/2019 relativas al artículo 25 Protección de datos desde el diseño y por defecto, *cit.*, pp.8-9.

análisis se pueda realizar un plan de acción para eliminar o, al menos, reducir a niveles aceptables los riesgos identificados. Por ende, esta acción trata de identificar e implementar medidas orientadas a eliminar o mitigar los riesgos con carácter previo a la puesta en marcha de aquellos tratamientos que sea probable que conlleven un alto riesgo para los derechos y libertades de los interesados[41].

Por todo lo antedicho, el derecho fundamental a la protección de datos personales ha de ser uno de los aspectos esenciales a incluir en cualquier plan de negocio o diseño de una aplicación, servicio o producto, ya que ello facilitará desarrollar el programa de cumplimiento que permita, al mismo tiempo, generar o impulsar la confianza de los interesados. Constituye un elemento estratégico que el responsable del tratamiento debe tener en consideración para asegurar el derecho fundamental a la protección de datos mediante la adopción e implementación de medidas técnicas y organizativas que consideren a la persona, titular de los datos personales desde el principio[42] y hasta el final del tratamiento de los datos personales. Mediante esta práctica, ganan tanto las organizaciones como los interesados[43]. Un producto, servicio o aplicación puede estar plenamente operativo con todas las funcionalidades activas, sin dejar a un lado los derechos de los usuarios.

Los productores de los productos, servicios y aplicaciones han de tener en cuenta el derecho a la protección de datos al desarrollar, diseñar, seleccionar y usar aplicaciones, servicios y productos basados en el tratamiento de datos personales o que tratan datos personales para cumplir su función[44]. No solo se requiere saber programar, sino hacerlo con todas las garantías.

6.2. La protección de datos por defecto

Antes de que un objeto salga al mercado, se han de aplicar las configuraciones más estrictas de manera predeterminada[45], sin requerir ninguna acción por parte del interesado[46]. El responsable solo podrá tratar los datos personales que por defecto sean estrictamente necesarios para cada uno de los fines de tratamiento[47]. No se pueden recopilar más datos personales de los que e necesitan, realizar un tratamiento más amplio de lo necesario para

[41] RUBÉN CABEZAS VÁZQUEZ, "Proteger la privacidad desde el diseño del producto", *Cincodías.elpaís*, 31 de julio de 2019, disponible en: https://cincodias.elpais.com/cincodias/2019/07/30/companias/1564510266_593013.html (Última consulta: 27.05.2024).
[42] MIGUEL, RECIO GAYO, "Protección de datos desde el diseño: principio y obligación en el RGPD", *elderecho*, 20 de febrero de 2017, disponible en: https://elderecho.com/proteccion-de-datos-desde-el-diseno-principio-y-obligacion-en-el-rgpd (Última consulta: 27.05.2024).
[43] ELENA GIL GONZÁLEZ, *Big data, privacidad y protección de datos*, *cit.*, p. 136.
[44] Considerando 78 del RGPD.
[45] Un estudio puso de manifiesto que la aplicación de mensajería WhatsApp Messenger no cumple este principio. Cuando se instala esta aplicación, por defecto, cualquier persona que tenga el contacto de otra podrá ver su estado, foto de perfil y la última vez que se conectó. Es el interesado el que tiene que cambiar manualmente la configuración. Véase al respecto. MIGUEL MOJICA LOPEZ; JOSÉ LUÍS RODRIGO OLIVA; VÍCTOR GAYOSO MARTÍNEZ; LUIÍS HERNANDEZ ENCINAS y AGUSTÍN MARTÍN MUÑOZ, "Análisis de la privacidad de WhatsApp Messenger", *Revista de sistemas, cibernética e informática*, vol. 14, núm. 2, 2017, p. 74.
[46] ICS, "What is privacy by design & default?", *ics*, disponible en: https://www.ics.ie/news/what-is-privacy-by-design-a-default (Última consulta: 27.05.2024).
[47] EDPS, "Privacy by default", *edps*, disponible en: https://edps.europa.eu/data-protection/our-work/subjects/privacy-default_en (Última consulta: 27.05.2024).

lograr los fines establecidos, ni conservar los datos personales más tiempo de lo necesario. Así, las aplicaciones informáticas, solo podrán acceder a los datos que realmente necesitan para poner a disposición del usuario una función[48].

La configuración establecida debe ser siempre la más protectora para interesado, de forma que ningún titular de los datos pueda por defecto verse expuesto a diferentes riesgos que ignora o que no sabe valorar en su justa medida[49]. Sin perjuicio de lo anterior, la misma configuración puede permitir que el interesado realice cambios para consentir otras utilidades que requieran un nivel de protección menor[50].

Aunque la configuración por defecto sea la más protectora, el interesado podrá autorizar que se procesen más datos personales, ampliar la extensión del tratamiento, que los datos se conserven durante un tiempo mayor y que otras terceras personas puedan acceder a sus datos personales. Corresponde al responsable del tratamiento implementar medidas técnicas y organizativas adecuadas para asegurarse de que se traten los datos personales que sean necesarios para cada uno de los fines específicos del tratamiento[51].

El responsable del tratamiento debe tener en cuenta la cantidad de datos personales tratados, el nivel de detalle, las diferentes categorías, la categorías de los datos necesarios para llevar a cabo una operación de tratamiento, incluyendo tanto los datos recogidos como los generados o inferidos a partir de estos[52]. La extensión del tratamiento, se refiere a que los tratamientos realizados por el responsable se limitarán a lo estrictamente necesario para cumplir con el propósito declarado por este[53]. El tratamiento ha de ser configurable por el responsable, y en su caso por el usuario, para ajustar el grado de accesibilidad a los distintos casos de uso. Solo se podrán realizar las operaciones necesarias, y, en relación con lo antedicho, sobre los datos necesarios para el cumplimiento de la finalidad de dichas fases[54].

Es obligación del responsable del tratamiento limitar el período de conservación de los datos personales a lo estrictamente necesario para el fin previsto, lo cual tiene relación directa con el principio de limitación del plazo de conservación establecido en el artículo 5.1.e) del RGPD. Cuando los datos personales dejen de ser necesarios para la finalidad del tratamiento, serán suprimidos o anonimizados. Cuando sean anonimizados, quedarán fuera del ámbito de aplicación de la normativa de protección de datos a los datos.

---

[48] GT29, Dictamen 02/2013 sobre las aplicaciones de los dispositivos inteligentes, *cit.*, p. 23.
[49] ROSARIO DUASO CALÉS, "Los principios de protección de datos desde el diseño y protección de datos por defecto", *cit.*, p. 310.
[50] AMAYA NOAIN-SÁNCHEZ, "Privacy by default and active informed consent by layers: Essential measures to protect ICT users' privacy", *Journal of Information, Communication and Ethics in Society*, vol.14, núm.2, 2016, p. 130.
[51] MIKKEL HANSEN, *Data protection by design and by default à la European General Data Protection Regulation*, Springer, Cham, 2016, p. 33.
[52] AEPD, Guía de privacidad desde el diseño, *octubre 2019,* p. 21, disponible en: https://www.aepd.es/guias/guia-privacidad-desde-diseno.pdf (Última consulta: 27.05.2024).
[53] ECONOMIST & JURIST, "5 preguntas sobre la nueva guía de protección de datos por defecto", *economistjurist*, 11 de noviembre de 2020, disponible en: https://www.economistjurist.es/noticias-juridicas/5-preguntas-sobre-la-nueva-guia-de-proteccion-de-datos-por-defecto/ (Última consulta: 27.05.2024).
[54] AEPD, Guía de privacidad desde el diseño, *cit.,* p. 21.

6.3. La certificación como herramienta de acreditación del cumplimiento de la normativa de protección de datos personales

En el artículo 25.3 del RGPD se introduce el mecanismo de la certificación que tiene como objetivo acreditar el cumplimiento de la protección de datos desde el diseño y por defecto con arreglo al artículo 42 del RGPD. Los Estados miembros, las autoridades de control, el Comité y la Comisión han de promover la creación de mecanismos de certificación en materia de protección de datos y de sellos y marcas de protección de datos a fin de demostrar el cumplimiento de lo dispuesto en el RGPD en las operaciones de tratamiento de los responsables y los encargados. En base al Considerando 100 del RGPD, a fin de aumentar la transparencia y el cumplimiento de la normativa, 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. El problema es que el RGPD no define que son los certificados, sellos o marcas, y utiliza los citados términos conjuntamente.

La certificación puede ser equiparada a los mecanismos de certificación de calidad industrial[55], pero para acreditar el cumplimiento de la normativa de protección de datos personales. En base al artículo 42.3 del RGPD, la certificación es voluntaria y no limita la responsabilidad del responsable del tratamiento en cuanto al cumplimiento del RGPD. Por consiguiente, es un modo de crear confianza en el interesado, pero no un instrumento que implique impunidad para el responsable del tratamiento.

Tras la evaluación independiente de las pruebas por parte de un organismo acreditado de certificación o autoridad de control competente que indique que los criterios de certificación se han cumplido podrá concederse la certificación[56], por ello, se comprende como un medio para demostrar el cumplimiento y para generar confianza en la sociedad[57]. En este sentido, según el artículo 24.3 del RGPD, los mecanismos de certificación pueden ser utilizados para demostrar el cumplimiento de las obligaciones por parte del responsable del tratamiento. Para ello, se han de presentar informes describan cómo se cumplen los criterios y, en su caso, las correcciones y acciones correctivas tomadas[58].

Esta "insignia" ha de ser expedida por los organismos de certificación, por la autoridad de control competente o por el CEPD. La duración de la acreditación es de 5 años, aunque podrá ser renovada siempre y cuando se sigan cumpliendo los requisitos. En el caso de que no

[55] LUÍS ANTONIO FERNÁNDEZ VILLAZÓN, "El nuevo reglamento europeo de protección de datos". *Foro. Revista de Ciencias Jurídicas y Sociales, Nueva Época,* vol. 19, núm. 1, 2016, p. 403; CHRISTINA TIKKINEN-PIRI; ANNA,Ç ROHUNEN y JOUNNI MARKKULA, "EU General Data Protection Regulation: Changes and implications for personal data collecting companies", *Computer Law & Security Review*, vol. 34, núm. 1, 2018, p. 138.
[56] CEPD, Directrices 1/2018 sobre la certificación y la determinación de los criterios de certificación de conformidad con los artículo 42 y 43 del Reglamento, 4 de junio de 2019, p. 9.
[57] CARLOS FERNÁNDEZ SÁNCHEZ y MIGUEL RECIO GAYO, "Certificación en protección de datos personales", en JOSÉ LUÍS PIÑAR MAÑAS, *Reglamento General de Protección de Datos. Hacia un nuevo modelo de Privacidad*, Reus, Madrid, 2016, pp. 413-414.
[58] CEPD, Directrices 1/2018 sobre la certificación y la determinación de los criterios de certificación de conformidad con los artículo 42 y 43 del Reglamento, *cit.*, p. 8.

cumplan los requisitos, la autoridad de control competente o el organismo nacional de acreditación podrá revocar la acreditación[59].

Antes de expedir la certificación o proceder a su retirada, los organismos de certificación deben comunicar a la autoridad de control competente en qué se han basado a la hora de tomar dicha decisión. Según el artículo 39 de la LOPDGDD, ENAC deberá comunicar a la AEPD y a las autoridades de protección de datos de las comunidades autónomas las concesiones, denegaciones o revocaciones, así como su motivación. Es competencia de las autoridades de control aprobar los criterios de certificación (58.3.f del RGPD), revisar (artículo 57.1.o del RGPD) y retirar (artículo 58.2.h del RGPD) las certificaciones.

El CEPD debe acreditar a los organismos de certificación, revisarlos y llevar un registro público de los organismos acreditados (artículo 70.1.o del RGPD), igualmente, debe aprobar los criterios de certificación. El RGPD incorpora un sello Europeo de Protección de Datos es un certificado de privacidad, protección de datos y seguridad, transparente e independiente, para productos y servicios tecnológicos en el entorno europeo[60].

La certificación tiene dos fases: la evaluación y el informe. En la primera fase, se realiza la evaluación del producto o servicio a certificar por expertos jurídicos e informáticos. Tras la evaluación, los expertos evacuan un informe que debe ser revisado por una entidad de certificación, para posteriormente, y siempre y cuando se cumpla con la normativa europea, otorgar el Sello Europeo de Privacidad[61]. Corresponde al CEPD archivar en un registro todos los mecanismos de certificación y sellos de protección de datos y los ponerlos a disposición pública por cualquier medio apropiado.

7. Conclusiones

En base a todo lo antedicho, se ha de velar por una protección adecuada y efectiva de los datos desde el diseño y por defecto; los responsables del tratamiento deben poder acreditar que han incorporado las medidas oportunas y las garantías necesarias en el tratamiento de los datos para que los principios de protección de datos y los derechos y libertades de los interesados sean efectivos. Este concepto ha sido introducido para la implementación efectiva de la responsabilidad proactiva.

Es obligación de los fabricantes y desarrolladores aplicar medidas de protección de datos por defecto y desde el diseño. El tratamiento de datos que se realice mediante los diversos dispositivos ha de respetar en todo momento el artículo 5 del RGPD, prestando especial

[59] Artículo 43.7 del RGPD.
[60] Véase al respecto: ANN CAVOUKIAN y MICHAEL CHIBBA, "Privacy Seals in the USA, Europe, Japan, Canada, India and Australia", en ROWENA RODRIGES y VAGELIS PAPAKONSTANTINOU, *Privacy and Data Protection Seals*, Asser, Berlin, 2018, p. 70.
[61] EUROPEAN PRIVACY SEAL., "EuroPriSe - Sello Europeo de Privacidad", *europrivacyseal,* disponible en: https://www.euprivacyseal.com/EPS-en/Europrise-sello-europeo-de-privacidad (Última consulta: 27.05.2024).

atención a la seguridad de los tratamientos, las posibles transferencias internacionales de datos, la transparencia en las finalidades para las que se tratarán los datos personales, la elaboración de perfiles y las decisiones automáticas individualizadas.

La aplicación de la protección de datos desde el diseño y por defecto beneficia a las organizaciones, puesto que, uno de los objetivos de este enfoque es la transparencia, elemento necesario cuando se trata de lograr la confianza del posible usuario. Debido al avance exponencial de la tecnología y la aparición de nuevos riesgos se requiere un nuevo enfoque. Esta nueva visión debe ser adaptable y poder evolucionar a medida que progresa la tecnología y los riesgos asociados.

El interesado ha de confiar en que se respetará su derecho a la protección de datos personales. En este sentido, la certificación es una herramienta valiosa en la medida en que sirve para demostrar el cumplimiento de la normativa de protección de datos personales y así generar un sentimiento de seguridad en el titular de los datos personales. Por consiguiente, es de vital importacia fomentar la creación y uso en la práctica del certificado que declara el cumplimiento de la normativa de protección de datos personales.

La óptica proactiva, sistemática e innovadora es la clave para que la protección de datos personales sea parte indisoluble de la cultura de las empresas y que, de esta manera, se contribuya a la creación de confianza entre los clientes, confianza que tan necesaria resulta para el despegue y correcto funcionamiento de la economía digital. Así, su aplicación puede verse como una ventaja competitiva necesaria para tener éxito en el mercado.

Bibliografía

AEPD, Guía de privacidad desde el diseño, octubre de 2019, disponible en: https://www.aepd.es/guias/guia-privacidad-desde-diseno.pdf (Última consulta: 27.05.2024)

AEPD, "El deber de informar y otras medidas de responsabilidad proactiva en apps para dispositivos móviles", *aepd*, 17 de septiembre de 2019, disponible en: https://www.aepd.es/sites/default/files/2019-11/nota-tecnica-apps-moviles.pdf (Última consulta: 27.05.2024)

AEPD, Informe sobre políticas de privacidad en internet, septiembre de 2018, disponible en: https://www.aepd.es/sites/default/files/2019-09/informe-politicas-de-privacidad-adaptacion-RGPD.pdf (Última consulta: 27.05.2024)

AEPD, "Principios", *aepd*, 30 de agosto de 2019, disponible en: https://www.aepd.es/es/derechos-y-deberes/cumple-tus-deberes/principios#:~:text=Principio%20de%20%E2%80%9C%20limitaci%C3%B3n%20de%20la,leg%C3%ADtimos%20sean%20tratados%20posteriormente%20de (Última consulta: 27.05.2024)

AEPD, Guía de privacidad desde el diseño, 5 de octubre de 2019, disponible en: https://www.aepd.es/documento/guia-privacidad-desde-diseno.pdf (Última consulta: 27.05.2024)

APARICIO SALOM, JAVIER y VIDAL LASO, MARIA, *Estudio sobre la protección de datos*, Aranzadi, Pamplona, 2019

BENÍTEZ, RAÚL; ESCUDERO, GERARD; KANAAN, SAMIR y MASIP, DAVID, Inteligencia artificial avanzada, UOC, Barcelona, 2014

CABEZAS VÁZQUEZ, RUBÉN, "Proteger la privacidad desde el diseño del producto", *Cincodías.elpaís*, 31 de julio de 2019, disponible en: https://cincodias.elpais.com/cincodias/2019/07/30/companias/1564510266_593013.html (Última consulta: 27.05.2024)

CAVOUKIAN, ANN y CHIBBA, MICHAEL, "Privacy Seals in the USA, Europe, Japan, Canada, India and Australia", en RODRIGES, ROWENA y PAPAKONSTANTINOU, VAGELIS, *Privacy and Data Protection Seals*, Asser, Berlin, 2018

CEPD, Directrices 1/2018 sobre la certificación y la determinación de los criterios de certificación de conformidad con los artículo 42 y 43 del Reglamento, 4 de junio de 2019

CEPD, Directrices 2/2021 sobre los asistentes de voz virtuales, 7 de julio de 2021

CEPD, Directrices 4/2019 relativas al artículo 25 Protección de datos desde el diseño y por defecto, 20 de octubre de 2020

CEPD, Directrices 5/2020 sobre el consentimiento en el sentido del Reglamento (UE) 2016/679, 4 de mayo de 2020

DUASO CALÉS, ROSARIO, "Los principios de protección de datos desde el diseño y protección de datos por defecto", en PIÑAR MAÑAS, JOSÉ LUÍS, *Privacidad para un mundo global*, Valencia, 2023

ECONOMIST & JURIST, "5 preguntas sobre la nueva guía de protección de datos por defecto", *economistjurist*, 11 de noviembre de 2020, disponible en: https://www.economistjurist.es/noticias-juridicas/5-preguntas-sobre-la-nueva-guia-de-proteccion-de-datos-por-defecto/ (Última consulta: 27.05.2024)

EDPS, "Privacy by default", *edps*, disponible en: https://edps.europa.eu/data-protection/our-work/subjects/privacy-default_en (Última consulta: 27.05.2024)

EUROPEAN PRIVACY SEAL, "EuroPriSe - Sello Europeo de Privacidad", *europrivacyseal,* disponible en: https://www.euprivacyseal.com/EPS-en/Europrise-sello-europeo-de-privacidad (Última consulta: 27.05.2024)

FERNÁNDEZ SÁNCHEZ, CARLOS y RECIO GAYO, MIGUEL, "Certificación en protección de datos personales", en PIÑAR MAÑAS, JOSÉ LUÍS, *Reglamento General de Protección de Datos. Hacia un nuevo modelo de Privacidad*, Reus, Madrid, 2016

FERNÁNDEZ VILLAZÓN, LUÍS ANTONIO, "El nuevo reglamento europeo de protección de datos". *Foro. Revista de Ciencias Jurídicas y Sociales, Nueva Época,* vol. 19, núm. 1, 2016, pp. 395-411

FLÓREZ DE LA COLINA, MARÍA AURORA, "Hacia una definición de la domótica", *Informes de la construcción*, Vol. 56, núm. 494, 2004, pp. 11-18

GARCÍA MEXÍA, PABLO y PERETE RAMÍREZ, CARMEN, "Internet y el Reglamento General de Protección de Datos", en LÓPEZ CALVO, JOSÉ (coord), *El nuevo marco regulatorio derivado del Reglamento Europeo de Protección de Datos*, Bosch, Madrid, 2018

GIL GONZÁLEZ, ELENA, *Big data, privacidad y protección de datos*, Boletin Oficial del Estado, Madrid, 2016

GT29, Dictamen 02/2013 sobre las aplicaciones de los dispositivos inteligentes, 00461/13/ES (WP 202), 27 de febrero de 2013

GT29, Dictamen 1/2010 sobre los conceptos de "responsable del tratamento" y "encargado del tratamento", 00264/10/ES (WP 169), de 16 de febrero de 2010

GT29, Opinión 3/2013 sobre la limitación de la finalidad (WP 203), de 2 de abril de 2013

GUZMÁN NAVARRO, FRANCISCO, *Domótica: gestión de la energía y gestión técnica de edificios*, RA-MA, Madrid, 2015

HANSEN, MARIT, *Data protection by design and by default à la European General Data Protection Regulation*, Springer, Cham, 2016

HUIDOBRO MOYA, JOSÉ MANUEL y MILLÁN TEJEDOR, RAMÓN JESÚS, *Manual de Domótica*, Creaciones copyright, Madrid, 2010

ICS, "What is privacy by design & default?", *ics*, disponible en: https://www.ics.ie/news/what-is-privacy-by-design-a-default (Última consulta: 27.05.2024)

JIMÉNEZ BUENDÍA, MANUEL, *Desarrollo de sistemas domóticos utilizando un enfoque dirigido por modelos*, Tesis doctoral, Universidad Politécnica de Cartagena, 2009

MILLÁN ÁNGELES, SUSANA, *Metodología y criterios para evaluar la influencia de la domótica y su preinstalación en los edificios en función de los condicionantes constructivos y de la envolvente interior*, Tesis doctoral, Universidad Politecnica de Madrid, 2014

MOJICA LOPEZ, MIGUEL; RODRIGO OLIVA, JOSÉ LUÍS; GAYOSO MARTÍNEZ, VÍCTOR; HERNANDEZ ENCINAS, LUÍS y MARTÍN MUÑOZ, AGUSTÍN, "Análisis de la privacidad de WhatsApp Messenger", *Revista de sistemas, cibernética e informática*, vol. 14, núm. 2, 2017, pp. 109-114

NOAIN-SÁNCHEZ, AMAYA, "Privacy by default and active informed consent by layers: Essential measures to protect ICT users' privacy", *Journal of Information, Communication and Ethics in Society*, vol.14, núm.2, 2016, pp. 124-138

NÚÑEZ, ANTONIO, *Domótica e inmótica KNX: guía práctica para el instalador*, Ediciones Experiencia, Barcelona, 2015

POLO ROCA, ANDONI, "El derecho a la protección de datos personales y su reflejo en el consentimiento del interesado", *Revista de derecho político*, núm. 108, 2020, pp. 165-194

RAE, Definición de domótico, disponible en: https://dle.rae.es/dom%C3%B3tico (Última consulta: 27.05.2024)

RAMÓN FERNÁNDEZ, FRANCISCA, *Vivienda inteligente: domótica, inteligencia artificial y regulación legal*, Tirant lo Blanch, Valencia, 2022

RECIO GAYO, MIGUEL, "Protección de datos desde el diseño: principio y obligación en el RGPD", *elderecho*, 20 de febrero de 2017, disponible en: https://elderecho.com/proteccion-de-datos-desde-el-diseno-principio-y-obligacion-en-el-rgpd

ROMANOU, ANNA, "The necessity of the implementation of Privacy by Design in sectors where data protection concerns arise", *Computer law & security review*, vol. 34, núm. 1, 2018, pp. 125-149

ROMERO, CRISTOBAL; VÁZQUEZ, FRANCISCO y DE CASTRO, CARLOS, *Domótica e Inmótica. Viviendas y edificios inteligentes*, Ra-ma, Madrid, 2010

STAR LEARN, *Robótica, biónica y domótica: usando arduino y tinkercad*. Ra-Ma, Madrid, 2023

TIKKINEN-PIRI, CHRISTINA; ROHUNEN, ANNA y MARKKULA, JOUNI, "EU General Data Protection Regulation: Changes and implications for personal data collecting companies", *Computer Law & Security Review*, vol. 34, núm. 1, 2018, pp. 134-153

TORRES-JAIME, JAIME; VÁZQUEZ-COLÍN, JAIME; CASTILLO-SUBDIAZ, FRANCISCO JAVIER; CONTRERAS-CALDERÓN, ENRIQUE; URZÚA-RANGEL, ROBERTO; Y BELTRÁN-ROMÁN, GABRIEL, "Ahorro de energía en aplicaciones electrónicas de la domótica", *Programación Matemática y Software*, Vol. 6, núm. 2, 2014, pp. 1-9

Jurisprudencia

STJUE, Sala Primera, de 20 de octubre de 2022, Digi Távközlési és Szolgáltató Kft contra Nemzeti Adatvédelmi és Információszabadság Hatóság, asunto C-77/21, ECLI:EU:C:2022:805

STJUE, Gran Sala, de 1 de octubre de 2019, Planet 49, C-673/17, ECLI:EU:C:2019:801

STJUE, Gran Sala, de 10 de julio de 2018, Jehovan todistajat, C–25/17, ECLI:EU:C:2018:551

STS, Sala Tercera de lo Contencioso-administrativo, 1062/2019, de 12 de julio de 2019 (Rec. núm. 4980/2018)

(texto submetido a 22.03.2024 e aceite para publicação a 24.05.2024)