REVISTA CARIBEÑA DE CIENCIAS SOCIALES
ISSN 2254-7630
https://doi.org/10.51896/caribe
CARIBEÑA DE CIENCIAS SOCIALES

EL CONSENTIMIENTO DEL INTERESADO ¿UNA HERRAMIENTA ADECUADA?

Idoia Landa Reza
Personal Investigador Contratado. Universidad del País Vasco (UPV/EHU)
0000-0002-8345-4117
idoia.landa@ehu.eus

Para citar este artículo puede utilizar el siguiente formato:

Idoia Landa Reza: "El consentimiento del interesado ¿una herramienta adecuada?", Revista Caribeña de Ciencias Sociales (Especial noviembre 2021, pp. 1-14) En línea: https://doi.org/10.51896/caribe/WSFJ4576

RESUMEN

Desde su incepción, el consentimiento del interesado ha constituido el núcleo del sistema europeo de protección de datos. Aunque pueda verse como una base legitimadora más del ordenamiento, lo ciertos es que, hasta la fecha, las normas declaran que el consentimiento del interesado constituye la principal herramienta que legitima el tratamiento de los datos personales. Mediante el mismo, se ha querido asegurar que sea la persona, desde su libertad individual, la que decida cómo, cuándo y para qué se tratarán sus datos personales. En este sentido, es importante recordar que el consentimiento del interesado ha sido creado para proporcionar a cada persona un control sobre su información personal. Con todo, el valor del consentimiento como instrumento de control y de protección del interesado ha sido criticado debido a que el desarrollo que se ha producido en los últimos años ha banalizado la prestación de dicho consentimiento a través de formas más blandas que llevan a prestarlo casi por defecto. Por ello, en los tiempos en los cuales la obtención y análisis masivo de datos es una práctica habitual, cabe preguntarse si realmente el consentimiento sigue siendo una herramienta adecuada para proteger la autodeterminación informática del sujeto en un mundo dominado por las TIC o por el contrario debemos considerarla una herramienta obsoleta que es preciso sustituir o al menos complementar.

Palabras clave: consentimiento, protección de datos personales, datos sanitarios, control, TIC.

CONSENT OF THE DATA SUBJECT, A SUITABLE TOOL?

ABSTRACT

Since its inception, the consent of the data subject has been the core of the European data protection system. Although it can be seen as one more legitimizing basis, the truth is that, nowadays, the regulations declare that the consent of the interested party constitutes the main lawful basis for the processing of personal data. By the tool of the consent, it has been wanted to ensure that it is the person who decides how, when and for what will be processed the personal data. In this sense, it is

important to remember that the consent of the data subject has been created to provide each person the control over his/her personal information. However, the value of consent as an instrument of control and protection has been criticized because the technological development that has occurred in recent years, which has trivialized the provision of the consent through softer forms that lead to giving it almost by default. For this reason, in the times in which the massive collection and analysis of data is a common practice, it is worth wondering if consent is still an adequate tool to protect the personal data protection in a world dominated by ICT or, on the contrary, we must consider it an obsolete tool that must be replaced or at least supplemented.
Keywords: consent, personal data protection, health data, control, ICT.

INTRODUCCIÓN

El consentimiento del interesado para el tratamiento de los datos personales

En el ámbito del derecho a la protección de datos, el artículo 6.1.a) del RGPD identifica al consentimiento como una de las bases legitimadoras para el tratamiento de datos personales, tratándose de esta manera de una forma de autorización autónoma. El concepto de "autorización autónoma" se refiere a que el interesado otorga un permiso por sí mismo, sin depender de nadie, para que se proceda al tratamiento de sus datos personales. Es decir, el titular de los datos autoriza al responsable del tratamiento de los mismos para que este los procese. El acto transformador que el consentimiento produce consiste en que, lo que de otro modo se consideraría una violación del derecho a la protección de datos del individuo no sea percibido como tal. Por otra parte, el interesado tiene derecho a elegir bajo qué circunstancias y para qué objetivos se pueden tratar sus datos personales (Schermer, Custers y Van Der Hor, 2014). En este segundo sentido, "el consentimiento se convierte en su instrumento de control" (Mittal y Sharma, 2017, p.76).

En base al artículo 4.11 del RGPD, el consentimiento del interesado se cifra en cualquier manifestación de voluntad libre, específica, informada e inequívoca por la que el interesado acepta, ya sea mediante una declaración o bien mediante una clara acción afirmativa, el tratamiento de los datos personales que le conciernen. La normativa habla de "manifestación de voluntad", y es exactamente, así como ha de ser catalogado dicho acto jurídico. "Una manifestación de voluntad que produce efectos jurídicos" (Polo, 2020, p.187).

El término "libre" 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 que este ejerza su libre voluntad. Para verificar si el consentimiento se ha otorgado de forma libre se han de considerar cuatro elementos: el desequilibrio de poder, la condicionalidad, la granularidad y el perjuicio.

El Considerando 43 del RGPD tiene en cuenta el desequilibrio de la relación entre el responsable del tratamiento y el interesado a la hora de valorar si el consentimiento ha sido otorgado

libremente o no (GT29, 2018). En los casos en los que existe un claro desequilibrio entre el responsable del tratamiento y el sujeto interesado, no podrá considerarse que el consentimiento haya sido otorgado con todas las garantías. A modo de ejemplo, podemos citar la referencia del Comisión Europea en materia de protección de datos personales (CEPD), cuando considera que existirá un desequilibrio siempre que el interesado no se encuentre en buen estado de salud, pertenezca a un grupo desfavorecido desde el punto de vista económico o social o si se encuentra en una situación de dependencia institucional o jerárquica (CEPD, 2019). Por ello, se deberán tomar todas las medidas necesarias para que dicha relación desigual no condicione el consentimiento del interesado.

En cuanto al elemento de la condicionalidad, el consentimiento no debe de vincularse a la aceptación de los términos o condiciones, o "vincular" la prestación de un contrato o servicio a una solicitud de consentimiento para el tratamiento de datos personales que no sean necesarios para la ejecución de dicho contrato o servicio. Si el consentimiento se da en esta situación, el consentimiento no será libre. Por ejemplo, si un proveedor de sitios web introduce un "*script*" que oculta el contenido y no es posible acceder al contenido sin pulsar el botón "aceptar las cookies", el interesado no manifestará un consentimiento libre, dado que no se le ofrece una posibilidad real de elección. No implica un consentimiento válido, ya que la prestación del servicio se supedita a que el interesado pulse el citado botón (CEPD, 2020).

Es necesario prestar la debida atención a si la aceptación de los términos y condiciones que son objeto del consentimiento están "agrupadas" o si el consentimiento se encuentra innecesariamente "atado" a la provisión de un contrato o un servicio cuando los datos personales solicitados no resultan necesarios para ejecutar o cumplir el contrato o prestar efectivamente el servicio (STJUE C-673/17). Para evaluar si tiene lugar esa situación de vinculación, resulta necesario determinar el alcance del contrato o servicio y que datos serían necesarios para la realización del mismo (Berrocal, 2019). Si existe este agrupamiento o vinculación, el consentimiento estará condicionado y, por tanto, no será libre.

En este mismo sentido, la AEPD indicó que la instalación y utilización de un aplicativo no puede estar condicionada a la obtención de un consentimiento para un tratamiento que no sea necesario para proporcionar el servicio definido en la misma (AEPD, 2019). Por ejemplo, si una persona quiere descargarse una aplicación para controlar el ejercicio diario que realiza, para que la aplicación funcione, el usuario deberá activar su localización GPS. Sin embargo, si a la hora de descargarse la aplicación en cuestión la misma solicita que el usuario active el micrófono del teléfono y no se completa la descarga hasta que lo autorice, el consentimiento otorgado por el usuario no será libre. El micrófono no es necesario para calcular la distancia recorrida por el usuario, es decir, el tratamiento de esos datos no es necesario para la prestación de dicho servicio, va más allá de lo necesario. Dado que el usuario no puede utilizar la aplicación sin consentir que el micrófono se active, el consentimiento se convierte en una contraprestación del contrato. Si en cambio el usuario ha activado el micrófono y por consiguiente se ha descargado la aplicación, y posteriormente retira el consentimiento, puede que la aplicación no funcione en su totalidad, así en base al Considerando 42

del RGPD, el consentimiento no será libre, puesto que el interesado no puede retirar su consentimiento sin sufrir perjuicio alguno.

El tercer elemento es la granularidad. Según Considerando 43 del RGPD, se presume que el consentimiento no se ha dado libremente cuando se impide o dificulta autorizar por separado las distintas operaciones de tratamiento de datos personales pese a ser adecuado en el caso concreto. Si el responsable del tratamiento ha combinado varios propósitos para el procesamiento y no ha solicitado un consentimiento por separado para cada propósito, existe una falta de libertad. Esto es, el consentimiento no será libre cuando no se le permita al interesado autorizar por separado los distintos tratamientos de datos personales. Para que el consentimiento sea válido, la solución radica en la separación de estos propósitos y la obtención del consentimiento para cada uno de los mismos, y por ello se encuentra la granularidad estrechamente relacionada con la necesidad de que el consentimiento sea específico.

Por último, debemos referirnos al elemento del perjuicio. Si el interesado no puede negar o retirar su consentimiento sin perjuicio, el consentimiento no será libre. El interesado debe tener la posibilidad de negar o retirar el consentimiento sin sufrir perjuicio alguno. El responsable del tratamiento debe poder demostrar que la retirada del consentimiento no conllevará ningún coste para el interesado y, por tanto, ninguna clara desventaja para quienes retiren el consentimiento. Otros ejemplos de prejuicio son el engaño, la intimidación, la coerción o consecuencias negativas importantes si un interesado no da su consentimiento. El responsable del tratamiento debe ser capaz de demostrar que el interesado pudo ejercer una elección libre o real a la hora de dar su consentimiento y que le era posible retirarlo sin sufrir ningún perjuicio.

Para que el consentimiento pueda considerarse específico, el responsable del tratamiento debe realizar tres acciones: especificar el fin del tratamiento como garantía contra la desviación del uso, disociar las solicitudes de consentimiento, y separar la información para las actividades de tratamiento de datos personales y la información relativa a otras cuestiones. Con estas tres acciones 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 (Polo et al., 2020). 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 (STJUE et al. C-673/17).

Respecto a la especificación del fin del tratamiento, el artículo 5.1.b) del RGPD recoge que los datos personales serán recogidos con fines determinados, explícitos y legítimos, y no serán tratados ulteriormente de manera incompatible con dichos fines. Por su parte, el Considerando 50 del mismo cuerpo legal recoge que el tratamiento de datos personales con fines distintos de aquellos para los que hayan sido recogidos inicialmente solo debe permitirse cuando sea compatible con los fines de su recogida inicial. El principio de limitación de la finalidad implica, por una parte, la obligación de que los datos sean tratados con una o varias finalidades determinadas, explícitas y legítimas y, por otra parte, que se prohíbe que los datos recogidos con unos fines determinados,

explícitos y legítimos sean tratados posteriormente de una manera incompatible con esos fines.

En este sentido, se ha afirmado que la evolución tecnológica hace cuestionable el principio de limitación de la finalidad (Moerel y Prins, 2016). Por ejemplo, el procesamiento de datos en masa (Big Data) a menudo no tiene un propósito fijo, y el uso potencial de los datos se llega a vislumbrar una vez son recopilados (Van der Sloot y Van Schendel, 2016). Según esta línea, no es posible saber de antemano que tratamiento puede realizarse, y para averiguarlo, es necesario recopilar todos los datos posibles y posteriormente deducir cuáles son los realmente relevantes (Hildebrandt, 2013).

En cuanto a la compatibilidad, el artículo 5.1.b) del RGPD recoge que, de acuerdo con el artículo 89.1 del mismo cuerpo legal, el tratamiento ulterior de los datos personales con fines de archivo en interés público, fines de investigación científica e histórica o fines estadísticos no se considerará incompatible con los fines iniciales. Por tanto, el tratamiento ulterior de los datos personales con fines de archivo, fines de investigación científica e histórica o fines estadísticos, no se considerará, incompatible con los fines iniciales, siempre que se produzca de conformidad con las disposiciones del artículo 89 del RGPD, que prevé garantías y excepciones específicas. En tal caso, el responsable del tratamiento podrá, en determinadas condiciones, realizar el tratamiento ulterior de los datos sin necesidad de una nueva base jurídica (CEPD, 2019).

Una vez que se haya otorgado el consentimiento por parte del titular de los datos y se haya procedido a la recolección de los mismos en base al fin o fines estipulados, no se podrá realizar ningún tratamiento posterior incompatible a dicho fin o fines. Esta prohibición funciona como garantía frente a la ampliación de los fines para los que se realiza el tratamiento de los datos una vez que un interesado haya dado su autorización a la recogida inicial de los datos. Este fenómeno, también conocido como desviación del uso, supone un riesgo para los interesados ya que puede dar lugar a un uso imprevisto de los datos personales por parte del responsable del tratamiento o de terceras partes y a la pérdida de control por parte del interesado (GT29, 2018).

Asimismo, el responsable del tratamiento debe disociar las solicitudes de consentimiento. Es decir, debe separar o desglosar las solicitudes de consentimiento para cada fin, dado que, cuando el tratamiento de los datos personales tenga como base legitimadora el consentimiento, este deberá ser otorgado para un fin específico. Si hubiese más de un fin para los datos, deberá solicitarse el consentimiento para cada uno de ellos. Esto significa que no es válido obtener un consentimiento “general” o “amplio” que cubra todos los tratamientos de datos, sino que deben separarse por finalidades. En el documento de consentimiento debe reflejarse claramente qué actividades de procesamiento de datos tiene la intención de realizar el responsable del tratamiento, otorgando al sujeto la oportunidad de dar su consentimiento para cada actividad.

Por último, el responsable del tratamiento deberá separar la información para las actividades de tratamiento de datos personales y la información relativa a otras cuestiones. Los interesados deben recibir la información separada para que conozcan la repercusión de las diferentes opciones que tienen. Esta obligación del responsable cobra especial importancia en el ámbito sanitario, donde

se deberá separar la información relativa al tratamiento de los datos del resto de la información relativa al tratamiento sanitario con el objetivo de evitar cualquier confusión.

El citado artículo 4.11 del RGPD requiere una declaración del interesado o una clara acción afirmativa como forma de manifestación del consentimiento, lo que significa que siempre debe darse el consentimiento mediante una acción o declaración. Se trata, por tanto, de una voluntad manifestada de forma unívoca mediante una conducta activa. Para que el consentimiento se otorgue de forma inequívoca, el procedimiento de su obtención y otorgamiento no tiene que dejar ninguna duda sobre la intención del interesado al dar su consentimiento. En otras palabras, la manifestación mediante la cual el interesado consiente no debe dejar lugar a ningún equívoco sobre su intención. Si existe una duda razonable sobre la intención de la persona se producirá una situación equívoca.

Esta declaración o acción del interesado puede realizarse verbalmente, por escrito o incluso por medios electrónicos. Esto puede incluir 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. En cuanto al consentimiento explícito, tradicionalmente ha sido por escrito, en papel o en soporte electrónico, pero no tiene que ser necesariamente así, ya que también puede ser verbal. El silencio, las casillas previamente marcadas o la inactividad no deben constituir un consentimiento.

Por último, el interesado debe ser informado sobre todos aquellos elementos que son necesarios para que este pueda formar su voluntad y decidir si consiente el tratamiento de sus datos personales o no (AEPD, 2018). En este sentido, el Tribunal Constitucional ha declarado que el deber de información previa forma parte del contenido esencial del derecho a la protección de datos, pues resulta un complemento indispensable de la necesidad de consentimiento del afectado. Por ello, a la hora de valorar si se ha vulnerado el derecho a la protección de datos por incumplimiento del deber de información, la dispensa del consentimiento al tratamiento de datos en determinados supuestos debe ser un elemento a tener en cuenta dada la estrecha vinculación entre el deber de información y el principio general de consentimiento (STC 39/2016).

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 del mismo cuerpo legal la información que deberá facilitarse cuando los datos no se obtengan del interesado. Los citados dos artículos requieren, al menos, la siguiente información: la identidad del responsable del tratamiento y, en su caso de su representante; los datos de contacto del delegado de protección de datos; los fines del tratamiento de los datos personales; en su caso, el interés legítimo del responsable o de un tercero; los destinatarios de los datos personales y la información sobre los posibles riesgos de transferencia de datos debido a la ausencia de una decisión de adecuación y de garantías adecuadas.

A su vez, para que el tratamiento sea considerado leal y transparente, en el momento en que se obtengan los datos personales, el responsable del tratamiento deberá facilitar al interesado la siguiente información: el plazo durante el cual se conservarán los datos personales; los derechos que tiene como interesado (acceso, rectificación, supresión, limitación del tratamiento, oposición y portabilidad de los datos); la existencia del derecho a retirar el consentimiento; el derecho a presentar una reclamación ante una autoridad de control; si la comunicación de los datos personales es un requisito legal o contractual y la información sobre el uso de los datos para decisiones automatizadas. Asimismo, el Comité Europeo de Protección de Datos, en adelante CEPD, señala que, dependiendo de las circunstancias y el contexto de un caso, puede requerirse más información para que el interesado entienda realmente las operaciones de tratamiento que van a tener lugar (CEPD, 2020).

Por todo lo antedicho, se ha de entender por consentimiento del interesado la autorización libre (otorgada sin coacción ni intimidación), específica (para un determinado tratamiento) e inequívoca (declaración o acción afirmativa) que concede el titular de los datos después de haber sido informado con todos los requisitos legales, para que se realice un tratamiento de los mismos.

El valor añadido del derecho a la información y el principio de transparencia

Debido a que la evolución tecnológica ha puesto en peligro el valor del consentimiento del interesado, el legislador europeo trató de hacer frente a dicha realidad otorgando un valor especial al derecho a la información y al principio de transparencia en el RGPD con el fin proteger la presente base legitimadora. Según la lógica seguida por el RGPD, el derecho fundamental a la protección de datos concede al interesado un poder de disposición y control sobre los datos personales, le permite saber quién posee esos datos personales y para qué, pudiendo oponerse a esa posesión o uso. Sin embargo, el interesado no podrá ejercer dicho derecho si desconoce, entre otras cuestiones, el fin que justifica el tratamiento de sus datos personales, quién es el responsable del tratamiento y que derechos tiene. Gracias a este derecho, el interesado adquiere un conocimiento, y es este conocimiento el que le permite ejercer un control sobre sus datos personales, de manera que puede otorgar el consentimiento para el tratamiento de sus datos o ejercitar sus derechos. Para poder consentir sobre cómo se tratan los datos, se ha de tener una información clara y veraz, si no se tiene información no se puede consentir y si no se está bien informado ni se pueden tomar decisiones, ni se puede ejercer la autonomía ni la libertad (Sánchez, 2009).

El artículo 5.a) del RGPD relativo a los principios del tratamiento de datos personales prevé que los datos personales serán tratados de manera lícita, leal y transparente. Así, el RGPD contempla un nuevo principio del tratamiento de los datos personales en el citado artículo, el cual es desarrollado en el artículo 12 del mismo cuerpo legal (Piñar, 2016). El principio de transparencia se refiere tanto al deber que tiene el responsable de informar al interesado acerca de ciertos elementos del tratamiento de sus datos personales como a la manera en que se cumple dicha obligación. No se

limita al deber de información del responsable del tratamiento. En este sentido, el Considerando 39 del RGPD recoge que el principio de transparencia exige que toda información y comunicación relativa al tratamiento de dichos datos sea fácilmente accesible y fácil de entender, y que se utilice un lenguaje sencillo y claro. En definitiva, la transparencia obliga a informar al interesado sobre el tratamiento de sus datos personales de una manera sencilla, prohibiendo igualmente realizar cualquier otro tratamiento que no conozca el interesado (STJUE, C-61/19).

El legislador afirma que, por ejemplo, en el ámbito tecnológico, el simple cumplimiento de informar al interesado no garantiza de un modo efectivo que este sea consciente de la lógica a que obedece el tratamiento de sus datos personales, de modo que aumenta su sensación de no tener un poder efectivo de disposición sobre sus datos. Esta grave situación es la que se busca solucionar imponiendo que las informaciones indicadas en los artículos 13 y 14 del RGPD, así como cualquier comunicación con arreglo a los artículos 15-22 y 34 del RGPD se realicen conforme a un principio de transparencia. Por tanto, si el responsable no proporciona información accesible, el control del usuario será ilusorio y el consentimiento no constituirá una base válida para el tratamiento de los datos (GT29, 2018).

El responsable ha de utilizar frases breves y claras para informar al interesado. De esta manera, se pretende evitar la fatiga informativa del interesado. Asimismo, esta información debe diferenciarse claramente de otra información no relacionada con la privacidad. Es errónea la idea de que cuanta más información se proporcione al interesado mejor comprenderá este su contenido. De ahí la importancia de la “información por capas”. Para hacer compatible la obligación de informar y la concisión y comprensión en la forma de presentarla, desde las Autoridades de Protección de Datos se recomienda adoptar un modelo de información por capas (AEPD 210070/2018) o niveles. El enfoque de información multinivel consiste en presentar una información básica en un primer nivel, de forma resumida, en el mismo momento y en el mismo medio en que se recojan los datos, y remitir a la información adicional en un segundo nivel donde se presentarán detalladamente el resto de las informaciones. Este enfoque multinivel se introduce con la finalidad, por un lado, de facilitar la tarea del responsable del tratamiento a la hora de diseñar sus procedimientos y formularios, y por otro, de conseguir que las personas interesadas obtengan la información más relevante de forma rápida y simplificada (AEPD, 2018).

Así, en cuanto a la primera capa, debe estar identificada con un título tal como “información básica sobre protección de datos”, y la forma de presentación preferente es en forma de tabla, garantizando que dicha información quede dentro del “campo de visión” del interesado, según sea el medio utilizado en la recogida de la información. Dentro de la tabla se han de recoger los siguientes cinco epígrafes: “responsable”, “finalidad”, “legitimación”, “destinatarios” y “derechos”. A estos cinco epígrafes se les añadirá un sexto, el de la “procedencia” cuando los datos no procedan del propio interesado. Respecto a la segunda capa, desarrolla los puntos de la primera capa y añade información adicional. Por tanto, complementa con todos los detalles necesarios la información resumida de la primera capa.

En suma, la información por capas consiste en separar la información facilitada a los usuarios en una primera capa más genérica y una segunda capa más detallada. Por tanto, esta modalidad permite que el usuario adquiera una información clave desde el primer momento, logrando información más amplia posteriormente. El responsable tiene el deber de otorgar la información, pero si no lo hace de forma concisa, transparente, inteligible, utilizando un lenguaje claro y sencillo y poniéndolo accesible para el interesado, estará infringiendo la normativa de protección de datos. Gracias a la estructura de capas, se consigue que el interesado no sea abrumado con la información, y que pueda comprenderla adecuadamente.

RESULTADOS Y DISCUSIÓN

Aunque el RGPD otorgó un valor añadido al derecho a la información e introdujo el principio de transparencia, optó por alejarse de cierta manera de una lectura estricta del sistema individualista mediante la incorporación de “la protección de datos desde el diseño y por defecto”, en adelante PddDpD, en su artículo 25. Por tanto, aunque la normativa mantenga los estrictos requisitos del consentimiento del interesado, otorgando, como se ha expuesto anteriormente, un valor especial al derecho a la información apuesta por proteger el entorno que rodea a su solicitud, en vez de simplemente limitarse a robustecer sus requisitos. Así, cabe afirmar que la introducción de la PddDpD es la verdadera vía para lograr el reforzamiento del consentimiento del interesado.

El objetivo de esta disposición es velar por una protección adecuada y efectiva de los datos desde el diseño y por defecto, lo que significa que los responsables del tratamiento deben poder acreditar que han incorporado las medidas oportunas y las garantías necesarias en el tratamiento para que los principios de protección de datos y los derechos y libertades de los interesados sean efectivos. Este concepto se compone de dos principios: la “protección de datos desde el diseño” en adelante PddD, y la “protección de datos por defecto”, en adelante PdpD. El primer principio se refiere a la incorporación de las medidas necesarias para que el derecho a la protección de datos sea respetado a lo largo de todo el ciclo de vida del objeto. Por su parte, el segundo principio se refiere a las decisiones relativas a valores de configuración que afecten a la cantidad de datos personales recogidos, a la extensión de su tratamiento, a su plazo de conservación y a su accesibilidad.

El apartado 1 del artículo 25 del RGPD recoge la definición de la PddD. Este enfoque está orientado a 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, ya sea este un sistema, un servicio un producto hardware o software o un proceso. Se entiende 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. Más aun, implica que se tengan en cuenta, no sólo la aplicación de medidas de protección del derecho a la protección de datos en las etapas tempranas del proyecto, sino que además se contemplen también todos los procesos y prácticas de negocio involucrados en el tratamiento de datos asociado, logrando así una verdadera

gobernanza de la gestión de los datos personales por parte de las organizaciones (AEPD, 2019). Las tecnologías deben ser construidas teniendo en cuenta la necesidad de la protección de los derechos del usuario (Gil, 2016). Operar desde el momento del diseño inicial y del desarrollo de una tecnología teniendo en consideración el derecho a la protección de datos como un elemento más para su buen funcionamiento, responde a una visión de prevención y de reducción de riesgos que puede limitar en gran medida la vulneración de derechos en este contexto (Duaso, 2016).

Los responsables del tratamiento deben aplicar “medidas técnicas y organizativas apropiadas” e integrar “las garantías necesarias” para aplicar los principios que se recogen en el RGPD, y así, proteger los derechos de los interesados. La normativa no elabora una lista con las medidas y garantías apropiadas, sino que otorga una libertad a los responsables para que estos decidan cuales son las adecuadas para el caso concreto.

En pocas palabras, el PddD tiene como objetivo que el derecho fundamental a la protección de datos personales sea 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. Por tanto, la PddD es una cuestión de estrategia 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 (Recio, 2017) y hasta el final del tratamiento de los datos personales.

En cuanto a la PdpD, en el ámbito informático, el término “por defecto” se refiere al valor preexistente o preseleccionado de un parámetro configurable que se asigna a una aplicación informática, a un programa informático o a un dispositivo periférico. Estos parámetros se denominan “preajustes” o “ajustes de fábrica”, especialmente en dispositivos electrónicos. En base al PdpD, cuando una aplicación informática, un servicio o un dispositivo sale al mercado, se deben aplicar las configuraciones más estrictas de manera predeterminada, sin que el interesado tenga que realizar ninguna acción.

Para la aplicación de este principio se tomarán decisiones relativas a valores de configuración u opciones de tratamiento establecidos o prescritos en un sistema de tratamiento que afecte a la cantidad de datos personales recogidos, a la extensión de su tratamiento, a su plazo de conservación y a su accesibilidad (CEPD, 2020). Las organizaciones solo podrán, por defecto, tratar los datos personales que sean estrictamente necesarios para cada uno de los fines de tratamiento. Esto es aplicable, como se ha expuesto, a la cantidad de los datos recogidos, los tratamientos que realizan, el tiempo de conservación y el acceso a los mismos. Así, el responsable del tratamiento no puede recoger más datos personales de los que necesita, realizar un tratamiento más amplio de lo necesario para lograr los fines establecidos, ni conservar los datos personales más tiempo de lo necesario. En este sentido, en cuanto a las aplicaciones informáticas, solo podrán acceder a los datos que realmente necesitan para poner a disposición del usuario una función (GT29, 2013). Como norma inquebrantable, la configuración establecida por defecto será la más protectora.

CONCLUSIONES

La corriente doctrinal que defiende que el consentimiento individual ha fracasado como mecanismo de control critica, entre otras cuestiones, el requisito de que el consentimiento sea específico. Tal y como se ha afirmado, debido a la especial naturaleza y desarrollo del Big data, se afirma que sería difícil determinar las finalidades o comunicaciones que van a producirse. Con los sistemas de inteligencia artificial y decisiones automatizadas, no es fácil consentir unas finalidades de uso de los datos que por lo general ni se conocen ni se sospechan (Cotino, 2017).

Respecto a la transparencia e información como elementos para proteger la figura del consentimiento del interesado, se manifiesta que, aunque el RGPD aboga por la utilización de un lenguaje sencillo, políticas fáciles de comprender y casillas o ventanillas fáciles de identificar en las que los usuarios pueden indicar su consentimiento, los pocos usuarios que leen las políticas de privacidad no llegan a comprenderlas realmente. Los textos escritos en este lenguaje sencillo no permiten tener información suficiente para elaborar un consentimiento informado. Por contra, el detalle que sería necesario para que la política de privacidad diera información suficiente sería abrumador (Git, et al., 2016).

En esta misma línea, el Grupo de trabajo del artículo 29 expresó que la complejidad de las prácticas de recogida de datos, los nuevos modelos empresariales, las relaciones con los vendedores y las nuevas aplicaciones tecnológicas llegan en muchos casos a sobrepasar la capacidad o la voluntad de la persona para tomar decisiones de control sobre el uso e intercambio de información por medio de una elección activa (GT29, 2009). Los ciudadanos no pueden dedicar el tiempo necesario, ni disponen, al menos en la mayoría de los casos, de la formación precisa para poder comprender y valorar la información que se les facilite en el ejercicio de este derecho (Oliver y Muñoz 2013). Es más, la lógica subyacente, entre otros, del Big data y la inteligencia artificial es tan completa que incluso, como sucede con las redes neuronales, ni tan siquiera sus propios desarrolladores la dominan del todo (Oliver y Muñoz et al., 2013).

En base a lo antedicho, algunos autores defienden que, el ideal normativo de “consentimiento y control” es un mito, un mantra cuya capacidad para modelar la realidad es poca: una persona corriente no puede hoy esperar tener un control sustancial de su información ni de como la usan otros (estado, empresas y conciudadanos) (Oliver y Muñoz et al., 2013). La aplicación del consentimiento en la realidad tecnológica escapa de los límites de la autonomía individual (Schermer et al, 2014) y el empoderamiento dentro de una sociedad moderna (Giannopoulou, 2020).

Aún hoy, la gran mayoría de los interesados tienen un limitado conocimiento tecnológico y, por lo tanto, no están en condiciones de tomar las medidas de seguridad necesarias por sí mismos con el fin de proteger sus datos personales. No obstante, el problema no solo reside en la falta de conocimiento técnico, las generaciones que han crecido rodeados de tecnología y, por tanto, tienen un conocimiento técnico superior, tampoco llegan a vislumbrar realmente los riesgos que conlleva su uso. Esto último está directamente relacionado con el hecho de que, en la actual sociedad, no existe

una cultura arraigada de protección de datos, lo cual constituye una ventaja para los empresarios. El interesado/usuario busca un beneficio final, y para lograrlo, acepta acríticamente todas las condiciones que le introduce el responsable del tratamiento, siendo un claro ejemplo de esta práctica las aplicaciones informáticas o apps. Por ejemplo, el interesado puede querer llevar un control de la enfermedad que padece mediante una app, y para conseguir dicho fin, acepta todas las condiciones que le introduce el responsable del tratamiento. Es decir, solo se enfoca en el beneficio, y no en el riesgo que se crea en el proceso de conseguir su objetivo.

Que el efecto del consentimiento no sea visible también dificulta que la sociedad comprenda la importancia del derecho a la protección de datos personales. Es en este punto donde entra en juego la PddDpD (Schaar, 2010). Frente a las garantías subjetivas, que en buena medida dependen del consentimiento y la acción del individuo, se argumenta que deben reforzarse las obligaciones legales preventivas de la PddDpD (Cotino et al., 2017). Por tanto, en vez de enfocarse en endurecer los requisitos del consentimiento, se ha de proteger el entorno que rodea al consentimiento.

Tanto la PddD como la PdpD son mecanismos poderosos y pueden cambiar las reglas del juego (Bourassa, Gallois, Mullan y Joly, 2019) si los productores, responsables del tratamiento y autoridades de control los toman en serio. Aunque la industria tecnológica alegue que estos cambios perjudicarán gravemente el desarrollo tecnológico, lo único que cambiaría son los modelos de negocio, dado ya no solo se tendrían en cuenta los intereses de los empresarios, entrando en juego los intereses de los usuarios finales.

Es más, la PddDpD beneficia a las organizaciones, puesto que, uno de los objetivos de este enfoque es la transparencia, y su aplicación permite lograr la confianza del posible usuario. Esta 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 (Cabezas, 2019). Así, la aplicación de la PddDpD puede verse como una ventaja competitiva necesaria para tener éxito en el mercado.

El interesado tiene que llegar a dar por hecho que se respetará su derecho a la protección de datos. Esta seguridad solo puede construirse a través de la concienciación de las personas y del desarrollo de ambientes que viabilicen un verdadero diálogo, donde libertades y derechos no negociables no sean moneda de cambio de los servicios ofrecidos. La tecnología ha de ser comprendida como aliada del Derecho y el Derecho como aliado de la tecnología (De la Mata y Bariñas, 2014).

REFERENCIAS

Berrocal Lanzarot, A. I. (2019). *Estudio jurídico-crítico sobre la Ley Orgánica 3/2018, de 5 de diciembre, de protección de datos personales y garantía de los derechos digitales: análisis conjunto del Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo de 27 de*

abril de 2016 y de la Ley Orgánica 3/2018 de 5 de diciembre. Reus

Gil, E. (2016). *Big data, privacidad y protección de datos*. Madrid: Agencia Estatal Boletín Oficial del Estado. https://www.aepd.es/sites/default/files/2019-10/big-data.pdf

Oliver Lalana, A. D.; Muñoz Soro, J. F. (2013). El mito del consentimiento y el fracaso del modelo individualista de protección de datos. En: *La protección de datos personales en internet ante la innovación tecnológica: riesgos, amenazas y respuestas desde la perspectiva jurídica*. Aranzadi Thomson Reuters

Piñar Mañas, J.L. (2016). *Reglamento General de Protección de Datos. Hacia un nuevo modelo de Privacidad*. Reus

Bourassa Forcier, M., Gallois, H., Mullan, S. y Joly, Y. (2019). Integrating artificial intelligence into health care through data access: can the GDPR act as a beacon for policymakers?. *Journal of Law and the Biosciences*, 6 (1), 317-335

Cotino Hueso, L. (2017). Big data e inteligencia artificial. Una aproximación a su tratamiento jurídico desde los derechos fundamentales. *Dilemata. Revista Internacional de Éticas Aplicadas*, 24 (2017), 131-150

De La Mata Barranco, N. J. y Barinas Ubiñas, D. (2014). La privacidad en el diseño y el diseño de la privacidad, también desde el derecho penal. *Eguzkilore*, 28, 253-274

Giannopoulou, A. (2020). Algorithmic systems: the consent is in the detail?. *Internet Policy Review*, 9 (1), 1-19

Hildebrandt, M. (2013). Slaves to big data. Or are we?. 16 IDP *Revista de Internet, Derecho y Política*, 17, 27-44

Mittal, S. y Sharma, P. (2017). The role of consent in legitimising the processing of personal data under the current EU data protection framework. *Asian Journal of Computer Science And Information Technology*, 7 (4), 76-78

Moerel, L. y Prins, C. (2016). Privacy for the Homo Digitalis: Proposal for a New Regulatory Framework for Data Protection in the Light of Big Data and the Internet of Things, 1-98. Disponible en: http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2784123

Polo Roca, A. (2020). El derecho a la protección *de datos personales y su reflejo en el consentimiento del interesado*. Revista de Derecho Político, 1 (108), 165–194

Sánchez Carazo, C. (2009). La protección de datos personales de las personas vulnerables. *Anuario de la Facultad de Derecho de la Universidad de Alcalá II*, 2, 203-227

SCHAAR, P. (2010). Privacy by design. *Identity in the Information Society*, 3 (2), 267-274

Schermer, B. W., Custers, B. & Van Der Hof, S. (2014). The crisis of consent: How stronger legal protection may lead to weaker consent in data protection. Ethics and Information Technology, 16 (2), 171-182

Van der Sloot, B y Van Schendel, S. (2016). Ten Questions for the Future Regulation of Big Data: A Comparative and Empirical Legal Study. JIPITEC: Journal of Intellectual Property, Information Technology and E-Commerce Law, 7, 110-145

Referencias jurisprudenciales:

STJUE (Sala Segunda), de 11 de noviembre de 2020, Orange Romania, C-61/19, ECLI:EU:C:2020:901

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

STJUE (Gran Sala), Conclusiones del abogado general, de 21 de marzo de 2019, Planet 49, C-673/17, ECLI:EU:C:2019:801

STC 39/2016 de 3 de marzo de 2016

Otros documentos:

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

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

Comité Europeo de Protección de Datos. Dictamen 3/2019 sobre las preguntas y respuestas acerca de la relación entre el Reglamento sobre ensayos clínicos (REC) y el Reglamento general de protección de datos (RGPD) [artículo 70, apartado 1, letra b)], 23 de enero de 2019

Agencia Española de Protección de Datos, El deber de informar y otras medidas de responsabilidad proactiva en apps para dispositivos móviles, 17 de septiembre de 2019

Agencia Española de Protección de Datos, Guía de privacidad desde el diseño, octubre de 2019

Agencia Española de Protección de Datos, Informe jurídico 210070/2018 de 19 de diciembre de 2018

Agencia Española de Protección de Datos. Informe sobre políticas de privacidad en internet, septiembre de 2018

Agencia Española de Protección de Datos, Guía para el cumplimiento del deber de informar, 25 de mayo 2018

Grupo de trabajo del artículo 29, Directrices sobre el consentimiento en el sentido del Reglamento (UE) 2016/679 (WP 259), 10 de abril de 2018

Grupo de trabajo del artículo 29, Dictamen 02/2013 sobre las aplicaciones de los dispositivos inteligentes (WP 202), 27 de febrero de 2013

Grupo de trabajo del artículo 29, El futuro de la privacidad: contribución común a la consulta de la Comisión Europea sobre el marco jurídico para el derecho fundamental a la protección de los datos de carácter personal (WP 168), 1 de diciembre de 2009

Páginas webs:

Recio Gayo, M. (20 de febrero de 2017). *Protección de datos desde el diseño: principio y obligación en el RGPD*. El derecho. https://elderecho.com/proteccion-de-datos-desde-el-diseno-principio-y-obligacion-en-el-rgpd

Cabezas Vázquez, R. (2019). *Proteger la privacidad desde el diseño del producto*. Cinco días. https://cincodias.elpais.com/cincodias/2019/07/30/companias/1564510266_593013.html