IUS ET SCIENTIA
2023 • Vol. 9 • Nº 1• ISSN 2444-8478
https://editorial.us.es/es/revistas/ius-et-scientia
https://dx.doi.org/10.12795/IETSCIENTIA • © Editorial Universidad de Sevilla 2023

El marco jurídico de la Unión Europea sobre protección de datos y garantías ciudadanas ante la Administración pública electrónica

EUROPEAN UNION LEGAL FRAMEWORK ON DATA PROTECTION AND CITIZENS' GUARANTEES TOWARDS ELECTRONIC PUBLIC ADMINISTRATION

Enrique Manuel Puerta Domínguez
CEU Cardenal Spínola
empuerta@ceuandalucia.es 0000-0003-1816-5703

Recibido: 24 de diciembre de 2022 | Aceptado: 11 de junio de 2023

RESUMEN

El presente estudio aborda, en clave analítica tanto de la legalidad europea como de la jurisprudencia del Tribunal de Justicia, las virtualidades aplicativas que tiene la normativa de la UE en materia de protección de datos en lo que afecta a las relaciones entre las Administraciones públicas y los ciudadanos. Tal normativa es exigente a la hora de deparar las obligaciones que competen a los que realizan el tratamiento o depósito de datos personales, y es de recibo que sean los entes públicos los que deban, antes que nada, dar ejemplo de una buena gestión. Materia rica y compleja, aun no ampliamente abordada, conoce una sugerente casuística jurisprudencial.

PALABRAS CLAVE

Protección de Datos
Administración pública
Unión Europea

ABSTRACT

This study addresses, in an analytical key both European legality and the jurisprudence of the Court of Justice, the application potentialities that the EU legal provisions have on data protection in what affects the relations between public administrations and the citizens. Such regulations are demanding when it comes to establishing the obligations that are incumbent on those who process or deposit personal data, and it is acceptable that public entities should, first of all, set an example of good management. Rich and complex matter, not yet widely addressed, is matter of such a suggestive case-law.

KEYWORDS

Data protection
Public Administration
European Union

I. NOCIONES PRELIMINARES; ADMINISTRACIÓN ELECTRÓNICA Y PROTECCION DE DATOS EN CLAVE RELACIONAL JURÍDICO-PÚBLICA

La Administración electrónica (también conocida quizás con matices más amplios y ambiciosos como e-Gobernanza) cubre un amplio campo de aplicaciones, entre las cuales, y sin ánimo de ser exhaustivos, podemos referir algunos ejemplos. El primero comprendería las relaciones de los usuarios con las entidades públicas fuera de sus dependencias presenciales al uso. Otro vendría deparado por la contribución de las Administraciones a la animación del debate público, y la consiguiente participación ciudadana, especialmente mediante la difusión de datos públicos esenciales mediante foros públicos, consultas en línea, y más ampliamente, los nuevos mecanismos de consulta a los ciudadanos. Por añadidura vendría al menos un tercer grupo de aspectos esenciales, identificado con las relaciones entre empresas privadas y corporaciones de naturaleza públicas.

Lo cierto es que tan pronto como la Administración electrónica proporcionó a los usuarios servicios tangibles, y que éstos a su vez han percibido como ventajas reales, otra cuestión, la de igualdad de acceso a los beneficios de la e- Gobernanza, emerge cada vez más agudamente. Tales circunstancias son las identificadas con la consabida brecha digital, por la cual la Administración electrónica parece quedar reservada únicamente a personas u hogares tecnológicamente equipados y conectados a internet. Caso de no disponerse de tales medios o habilidades otras soluciones han venido descartándose, tales como el acceso generalizado desde terminales interactivos en edificios administrativos o puntos de acceso público, bien desde cualquier mostrador o con la ayuda de un mediador. Dichas exclusiones son suplidas por la denodada entrega de ciertos servicios asistenciales, especialmente Trabajadores Sociales y Voluntarios, así como con arreglo al recurso intergeneracional deparado por los más jóvenes hacia los más mayores o menos tecnificados. Por lo tanto, un primer problema que debe resolver el de la e-Gobernanza es el de su eventual carácter discriminatorio o excluyente. Pero no es el único. Una vez garantizada la igualdad de acceso, quedaban otros muchos retos, que fueron desvelándose conforme avanzaba la implantación de la e-Gobernanza en el continente europeo.

Efectivamente, desde el comienzo del presente siglo todos los países de la Unión fueron poniendo en marcha programas más o menos ambiciosos. Ya en la lejana fecha de junio de 2000, los Jefes de Estado y de Gobierno adoptaron en el Consejo Europeo de Santa María da Feira el denominado "Plan de Acción e-Europa 2002". Dicha iniciativa dedicaba un capítulo a la Administración electrónica, en virtud del cual se asignaba a las diversas corporaciones públicas de los Estados miembros diversos conjuntos de objetivos a alcanzar, junto con un calendario. Desde entonces, los Directores Generales encargados de la Función Pública de los Estados miembros de la Unión Europea se han venido reuniendo con regularidad para abordar este tipo de cuestiones. En etapas posteriores se procedió principalmente a examinar temas de interés común; aquí se han tocado cuestiones como la identificación electrónica o firma electrónica,

IUS ET SCIENTIA • 2023
Vol. 9 • Nº 1 • pp. 23-45
ISSN 2444-8478 • https://doi.org/10.12795/IESTSCIENTIA.2023.i01.03

las relaciones concernientes a la protección de datos de los europeos con respecto a autoridades de países terceros, etc.) Igualmente se procedió a calibrar los logros alcanzados en clave de mejorar las prácticas de la e-Gobernanza. Aun hoy se considera necesario ir mucho más allá del mero intercambio de puntos de vista para pasar a mecanismos de consulta real entre las Administraciones europeas, lo que pasa por su intercambiabilidad. Pero no es menos cierto que nos enfrentamos con todo este proceso al riesgo tangible derivado del hecho de que la tecnificación aliente tentaciones experimentadas por esos mismos poderes públicos encuadrados en tal e-Gobernanza global, y que podrían abocar a un manejo irresponsable o manipulador de los datos de los ciudadanos. E igualmente se produce el problema inverso, determinado por la enorme dificultad que para unas Administraciones estatales de base territorial supone dar respuesta a una cuestión como la del tratamiento de datos en un medio como internet, que es sustancialmente transnacional. Sobre estas inquietudes expresadas por los justiciables europeos, y las inexcusables garantías jurídicas que aquéllas suscitan, es como significativamente emerge cierta jurisprudencia del Tribunal de Justicia de la UE tocante a salvaguarda de datos personales en el entorno telemático, concretamente en lo concerniente a su trato por las Administraciones nacionales, y también de la UE, versa la presente aportación. Esta inquietud, que reflejamos y ponemos al día en la presente aportación, ya vino expresada por ciertos autores desde los primeros avances de las entonces nuevas tecnologías telemáticas, muy con concreto por las preocupantes resultas que de aquéllas se derivaban para la privacidad de datos. En concreto, se trataría de Problemas derivados de la misma naturaleza de la red, como la aplicación de una ley nacional a un fenómeno esencialmente transfronterizo o incluso la dificultad de conocer la verdadera identidad de los intermediarios, debido a la abstracción de los intercambios, posibilidades de alias y otros signos virtuales susceptibles de ocupar la verdadera personalidad de quién está al otro lado de una terminal (Andrieu; 2000, p. 155).

Consecuentemente, un especial interés suscita conocer (en el ámbito de las relaciones de los ciudadanos, y en cuanto a usuarios que somos de las tecnologías con respecto a las Administraciones) dónde exactamente han de centrarse las principales preocupaciones en materia de privacidad, protección de datos personales y gestión de la identidad. Se volvió necesario garantizar, en particular para los datos o aspectos más sensibles o más confidenciales, que solo la persona interesada pudiese manejarlos y realizar sus trámites en una relación protegida con respecto a las Administraciones públicas, y que éstas por su parte, respondiesen con un tratamiento que respetase idéntico nivel de confidencialidad. A estos efectos se entendió necesario codificar y asegurar los modos de acceso, así como repensar los sistemas de identificación y autenticación. Se tomó una cierta conciencia consistente en equilibrar la facilidad de uso, la ergonomía de los métodos de identificación y los niveles de seguridad. La introducción de la Administración electrónica debería en todo caso permitir a los ciudadanos guardar el control sobre sus datos personales. En este sentido, podría posibilitarse un ejercicio en línea, e incluso en tiempo real, de los derechos de acceso y rectificación de los datos que la Administración tiene sobre los ciudadanos.

IUS ET SCIENTIA • 2023
Vol. 9 • N° 1 • pp. 23-45
ISSN 2444-8478 • https://doi.org/10.12795/IESTSCIENTIA.2023.i01.03

La marcha hacia la e-Gobernanza y sus consecuencias se han podido observar comparativamente en todos los países de la OCDE. Las Tecnologías de la Información y Comunicación (TIC), también denominadas Nuevas Tecnologías (NN TT), han aportado mucho a la vida cotidiana, incluidas las relaciones jurídico públicas; pero también han creado no poca alarma social en cuanto a sus potencialidades negativas en caso de un empleo no idóneo. Cierto es que los puestos administrativos están cubiertos por seres humanos corrientes, y en cuanto tales, no son ni infalibles ni inmunes a toda circunstancia que ponga a prueba su virtud y probidad. Cuenta el viejo proverbio que no existe mejor prédica que el ejemplo; en consecuencia, y por lo que atañe a una cuestión tan controvertida como la protección de los datos personales a través del medio telemático, deberán ser pues las Administraciones públicas las que, en su manejo, deberán ostentar los índices de mayor transparencia y salvaguarda con respecto a los ciudadanos. La preocupación por la privacidad, correlativamente a la proliferación de datos que circulan de forma mucho más fluida, también se está trasladando de las entidades públicas a las empresas.

Un primer hito significativo fue deparado por la Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre de 1995, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos reflejó en su momento esta nueva percepción de los riesgos. En aquellas fechas, algunos autores (Guadamuz; 2000, p. 3), propusieron inclusive el término *Habeas Data* rememorando el tradicional *Habeas Corpus* en lo tocante a la necesidad de mantener la privacidad de su titular en las relaciones informáticas, preocupándose muy especialmente en recalcar que el sistema europeo de protección de datos imponía una carga al resto del mundo al imponer restricciones a la transferencia de datos a países que no cuentan con ningún tipo de protección de la privacidad.

La tendencia en la UE se vio consolidada por la aprobación del actual Reglamento 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 (y que denominaremos a partir de ahora RPD). La literatura científica sobre este instrumento es inmensa, destacando tal vez por sus mayores preocupaciones en el terreno de su impacto en el entorno internet y de cara a las Administraciones públicas, especialmente en lo que atañe a su proceso de elaboración, y al modo en que el Legislador europeo muestra con cierto orgullo la experiencia de aprendizaje recibida a lo largo de las casi dos décadas que median entre ambos instrumentos (Brunet; 2016, p. 567).

Desde el prisma de la técnica legislativa se confirma una vez más el proceso de paulatina sustitución en la construcción jurídica europea del instrumento de la Directiva, característico del S. XX, por el del Reglamento en el presente S. XXI. A lo largo del presente estudio podremos calibrar hasta qué punto dichas normativas, como apuesta europea en la materia (y en contraposición a la filosofía de otras partes del mundo, concretamente EE UU, por no hablar de la policía informática exhaustiva existente en la R. P. De China), tienen mucho que aportar en las relaciones entre la Administración electrónica

IUS ET SCIENTIA • 2023
Vol. 9 • Nº 1 • pp. 23-45
ISSN 2444-8478 • https://doi.org/10.12795/IESTSCIENTIA.2023.i01.03

y los ciudadanos, existiendo ya al respecto una no muy abundante, pero sí significativa aportación jurisprudencial a cargo del Tribunal con sede en Luxemburgo.

La gran cuestión inicial versa en concreto hacia qué clase de Administración electrónica se está tendiendo como meta deseable. La idea generalmente compartida es que acabasen siendo realizables únicamente en línea, como así ha sido finalmente, todos los trámites administrativos para personas físicas, asociaciones y empresas, así como el pago de impuestos y seguridad social, entre otros. El objetivo habría sido el de garantizar gradualmente que cada usuario se beneficiase de las TIC en las transacciones con los servicios públicos, y consiguientemente pudiese, (superadas todas las discriminaciones propias de la brecha digital), acceder de forma sencilla y rápida a toda la información y ayuda personalizada sobre servicios públicos y trámites administrativos. Ello incluiría muy especialmente el seguimiento de sus archivos, la definición de calendarios provisionales personalizados, la recepción de recordatorios por correo electrónico el acceso a todos sus trámites anteriores, así como almacenar en línea (a plena discreción y con total seguridad), los resultados desmaterializados resultantes de estos. También podrían los ciudadanos ejercer en línea su derecho de acceso a sus datos personales de los que disponga toda entidad pública, para en su caso, estar al corriente de toda modificación que se produzca con arreglo a toda información que le concierna, y que se halle en poder, o resulte intercambiada entre las diversas Administraciones cuando interactúen con relación a unos mismos ciudadanos.

La e-Gobernanza, en aplicación de todos los deseos o metas acabados de expresar, se construiría a partir de una serie de mecanismos técnicos que, no sólo habrían de dar la talla en términos de mera operatividad técnica, sino además ser capaces de propiciar unas garantías básicas, como serían las de una identidad fehaciente de los ciudadanos o administrados, así como la de un acceso generalizado sin discriminaciones y en salvaguarda de la intimidad representada en sus datos personales. Serían pues unos requisitos técnicos, debidamente fiscalizados (sin exceso ni defecto) respecto de la normativa europea de protección de datos, en lo que atañe al vínculo entre la Administración electrónica y los e-gobernados.

II. CUESTIONES ESPECIALMENTE DEBATIDAS EN MATERIA DE ADMINISTRACIÓN ELECTRÓNICA Y PROTECCIÓN DE DATOS

Toda esta realidad trata de dar respuestas a una serie de inquietantes cuestiones de base, que están en el centro de la implantación y consolidación de la Administración electrónica y sus límites respecto a la salvaguarda de los datos personales del usuario o administrado. Una cosa es desear aspectos como eficacia y prontitud en los servicios, y otra bien distinta asumir hasta qué limites o riesgos son asumibles en todo este proceso. Corresponde pues al Legislador establecer una normativa que asegure el equilibrio. Y en ese debate a la hora de legislar aparecen toda una serie de cuestiones, las cuales son objeto de vivos debates, y que, como veremos, determinan unas pautas diferentes en cuanto a su tratamiento y respuesta según nos ubiquemos a una u otra orilla del Atlántico.

IUS ET SCIENTIA • 2023
Vol. 9 • N° 1 • pp. 23-45
ISSN 2444-8478 • https://doi.org/10.12795/IESTSCIENTIA.2023.i01.03

2.1. El debate sobre la propiedad por parte de los administrados de los datos que les conciernen y que son manejados por las Administraciones

Mientras que la legalidad en materia de protección de datos otorga a las personas unos derechos de acceso, comunicación, rectificación y oposición a sus datos, que a decir verdad en gran parte siguen aún siendo relativamente teóricos, la realidad de la sociedad de la información contempla la recogida y venta de datos con fines comerciales, hasta el punto de que el principal derecho a los datos a veces parecen ser un derecho de propiedad. De prevalecer tal análisis, los cauces de la actividad administrativa *online* y su régimen de control podrían sufrir determinados efectos de parálisis o confusión. De hecho, esto justificaría un enfoque contractual del control de los individuos sobre sus datos, y pondría en entredicho el control ejercido sobre el tratamiento administrativo, que es protector pero también restrictivo para los usuarios y para las corporaciones públicas. Es por esto que debemos preguntarnos cómo se deben analizar jurídicamente los derechos de los usuarios sobre sus datos.

Es tentador a primera vista considerar a las personas como titulares de un derecho real de propiedad sobre sus datos. Efectivamente, aparece enormemente extendida la convicción según la cual, con arreglo a los modelos económicos implantados desde la web en el entorno de los negocios privados, las personas ceden o "venden" sus datos personales, en particular a cambio de servicios gratuitos. Y es cierto que si se debe reconocer un derecho de propiedad sobre los datos personales, este derecho de propiedad debe conferirse más bien a la persona a la que conciernen los datos que al titular de la base de datos. Esta es una excepción al principio de que la información pertenece a la persona que la recopila o formula. En efecto, los datos personales que las Administraciones pueden tener sobre los usuarios (nombre, fecha de nacimiento, domicilio, situación familiar, incluso base imponible o contenido de los antecedentes penales) son datos objetivos, que las corporaciones públicas se limitan a registrar sin añadir una apreciación subjetiva que justificaría una apropiación por su parte. Si existe un derecho de propiedad sobre los datos personales, por lo tanto, solo puede ser el de la persona interesada.

En cualquier estado de causa, argumentos serios llevan a rechazar esta idea de un derecho de propiedad sobre los datos personales. Los datos personales en su contexto telemático, que se basan en una base objetiva, no pueden ser modificados a voluntad por el interesado, salvo, por supuesto, que la modificación de los datos corresponda a una modificación en la situación objetiva correspondiente (domicilio, nombre, etc.). Para un derecho real de dominio ha de existir necesariamente un elemento de libre disposición de la propiedad. No obstante, en la etapa de su formulación, estos datos no son más obra del interesado que de la Administración. Así las cosas, semejante formulación depende de la Ley, o bien se adjunta automáticamente a los actos del sujeto (adquisiciones de bienes inmuebles, estado de cuentas bancarias, etc.). Además, la idea de un derecho de propiedad no es en la que sirve de base a la legislación sobre tratamiento de datos y libertades, la cual aparece mucho más centrada en una perspectiva

IUS ET SCIENTIA • 2023
Vol. 9 • Nº 1 • pp. 23-45
ISSN 2444-8478 • https://doi.org/10.12795/IESTSCIENTIA.2023.i01.03

de protección de las libertades. Este enfoque estaría mucho más cerca de un enfoque estadounidense que europeo, en donde no acaba de cerrarse el sempiterno debate, según el cual, los datos personales pueden asimilarse a un derecho de propiedad susceptible de compraventa. En Europa sin embargo los datos se identifican con derechos humanos, los cuales nunca pueden ser objeto de transacciones. Probablemente la óptica europea tampoco llegue a servir para prohibir aquellas prácticas consistentes en remunerar el tiempo que las personas dedican a comunicar la información que interesa a los administradores de bases de datos. Pero esto prohíbe que la comunicación de datos sea considerada como la transferencia de un derecho de propiedad sobre ellos. Consecuentemente la transferencia a la Administración de datos personales no es puramente discrecional y no puede analizarse desde una perspectiva contractual. Puede imponerse como requisito de la comunidad para hacer posible la vida en común, en una lógica similar a la que está en la base de la tributación.

Con todo, el análisis más riguroso parece conducir, por tanto, a analizar los datos personales no en términos de derechos patrimoniales sino en términos de atributos de personalidad. Debe pues estimarse que, si bien el titular de los datos no es el autor de la información, en el sentido de formato, es el legítimo poseedor de sus elementos. Su vínculo con el individuo es demasiado estrecho para que no sea de otro modo. Cuando el sujeto de los datos es un sujeto de derecho, la información es un atributo de personalidad. Este carácter de atributo de personalidad implica que la comunicación de la información debe derivar o del consentimiento del interesado o de obligaciones legislativas o reglamentarias. Y más allá del debate doctrinario, todo el reto que atañe a la protección de los datos personales de los ciudadanos respecto a la e-Gobernanza consiste entonces en garantizar las condiciones suficientes para que las personas controlen estos datos, reconociendo su derecho real a determinar el uso que debe hacerse de los datos personales en posesión de las Administraciones. Es la puesta en práctica de la teoría de la autodeterminación informacional, por la cual el tribunal constitucional federal alemán proclamó el derecho del individuo a decidir sobre la comunicación y uso de la información relativa a su persona.

2.2. El debate acerca de los límites a los que debe sujetarse el principio de control de los datos personales en la implementación de la e-Gobernanza

El principio de control de los datos personales no puede ser absoluto, y toda pretensión encaminada hacia tal concepción ha de desestimarse como alejada de la realidad. En todo caso la potestad de supervisión habría de ejercerse, por lo que concierne a tan compleja zona de apreciación, en aquellos casos o situaciones en los que la decisión de comunicar o no determinados datos personales, de autorizar su transmisión de una Administración a otra puede dejarse ventajosamente a la iniciativa personal. En semejante zona de laxitud, correspondería a cada persona decidir libremente, según las ventajas que espera o los riesgos que teme, comunicar o no sus datos, lo que

IUS ET SCIENTIA • 2023
Vol. 9 • N° 1 • pp. 23-45
ISSN 2444-8478 • https://doi.org/10.12795/IESTSCIENTIA.2023.i01.03

incluye asimismo la opción de autorizar o no a la Administración que posee los datos que le conciernen para que los transmita a otra corporación pública, o inclusive a terceros ajenos al marco jurídico público. El principio de control de los datos personales no puede impedir la consecución de fines de interés público o que tengan carácter obligatorio: determinados procedimientos, formularios o recogidas de información por parte del Estado tienen carácter obligatorio. Y de otro tanto, la difusión incondicionada de datos estaría también limitada por las reglas genéricas que estarían de aplicar las oficinas generales supervisoras en la materia de protección de datos designadas por los Estados miembros, destinadas a proteger a las personas, en particular a las más vulnerables, contra la excesiva intromisión de los entes públicos respecto de los ciudadanos.

Desde luego el control sobre datos personales ha de ser un ámbito necesario, pero que debe enriquecerse y detallarse. Debemos considerar que, para salvaguardar la privacidad, todo sistema regulado de protección de datos debe obedecer a un doble enfoque: por un lado, un marco de "arriba hacia abajo", con esquemas de autorización proporcionada por los organismos supervisores específicos, destinados a la creación de archivos administrativos, y por otro lado, que se posibiliten derechos reconocidos a los usuarios para un control "de abajo hacia arriba", con el fin de verificar la licitud del tratamiento y la veracidad de los datos (derechos de acceso, comunicación, rectificación y oposición). En la práctica, es el primer enfoque el que mayoritariamente ha prevalecido. En efecto, el tratamiento de datos se examina rigurosamente en la fase de su creación, pero, y esto es quizás una muestra de confianza en este control, el ejercicio directo de sus derechos por parte de los usuarios se ha mantenido en gran medida teórico. Ello ha determinado pues que los derechos de acceso, comunicación y rectificación se hayan extendido como una potestad irrenunciable del ciudadano en cuanto a administrado telemático. Con el desarrollo de la Administración en línea, ha resultado posible enriquecer estos derechos de los ciudadanos, de modo que permitan un control real de los datos por parte de las personas. Dicho control ha venido significando para los usuarios un acceso real en línea a los sistemas que contienen datos sobre ellos, no solo para verificar su exactitud, sino también para obtener su comunicación en forma digital. Por ejemplo, tal como la cuestión está configurada actualmente, si el acceso y la comunicación por ejemplo de los expedientes de los titulados universitarios tiene como único fin comprobar su exactitud, un derecho de comunicación permitiría a este titulado obtener una copia digital de su título para adjuntar a su currículum. o registrarse en línea para una competencia administrativa. Es pues la operatividad creativa del ciudadano frente a las e-Administradores una fuente inagotable tanto de nuevos retos como de innovaciones relacionales entre unos y otros.

En consecuencia, se trata sólo de una transposición a la sociedad de la información de la práctica de comunicar documentos justificativos. Por lo tanto, si el objetivo ya es perceptible, quedan por definir los métodos de su implementación. Se trata de que este derecho de disposición de los datos, que por su naturaleza implica un consentimiento del interesado ejercido por éste, que aleja ya de toda idea

IUS ET SCIENTIA • 2023
Vol. 9 • N° 1 • pp. 23-45
ISSN 2444-8478 • https://doi.org/10.12795/IESTSCIENTIA.2023.i01.03

de coacción o de procedencia de consentimiento extorsionado propiciado desde los poderes públicos. Si se trata de una autorización otorgada a una Administración para que otra comunique información, semejante aquiescencia debe ser precisamente delimitada, revocable y ejercida bajo el control de organismos independientes en materia de protección de datos. Aun quedando muchas dudas irresueltas, resulta no obstante concebible que puedan surgir nuevos equilibrios que permitan un control real de las personas sobre sus datos los cuales, lejos de atenuar los controles existentes, pueden ser un cauce susceptible para que les sean reconocidos nuevos derechos.

Tampoco la e-Gobernanza debe pretender, ni puede tener como resultado, permitir a la Administración aumentar el nivel de control y vigilancia de los ciudadanos. El desarrollo de una potestad pública electrónica plena no debería tener por objeto recabar nuevas informaciones sobre los usuarios de manera continuada. El reto consiste, por el contrario, en dar acceso a los usuarios a los datos que les conciernen y que actualmente existen en los sistemas de información de las Administraciones. Todos estos servicios en ningún aumentar así el conocimiento que aquéllas tienen sobre el usuario. Por otro lado, tampoco es menos cierto que aumentan el conocimiento que el propio usuario tiene de lo que le preocupa respecto de la actividad que sobre él ejercen los poderes públicos, mejorando así su autonomía y su capacidad de acción.

Llegados a este punto cabe interrogarnos acerca de si podría hacerse plenamente operativo el principio según el cual todo acceso o modificación de datos personales relativos a un usuario en bases de datos públicas debe dar lugar a una notificación. La reforma de los sistemas de información permite hacer efectivo el derecho a la información. Los ciudadanos deben tener plena visibilidad de la gestión de la información que les concierne por parte de la Administración. De este modo, el ciudadano debería estar en condición de responder a cierta clase de preguntas cuando le asaltan ciertas dudas acerca del tratamiento de su intimidad y datos en el curso de la e-Gobernanza: ¿Quién consultó qué cosa? ¿Cuándo se hizo, y cuáles fueron los motivos para tal consulta? ¿Quién duplicó qué informaciones, cuándo y con qué propósito? ¿Quién modificó la información, en qué fecha, por qué razones y cuáles son las consecuencias dentro de la Administración competente y dentro de las Administraciones usuarias? La Administración tendría a renglón seguido la obligación de informar al ciudadano de estas modificaciones. Cabría plantearse que esta obligación de notificación reviste perfiles diferenciados según el grado de sensibilidad de los datos en cuestión, o incluso según el "ciclo de vida útil" de los datos. A decir verdad, ciertos datos se modifican con frecuencia mientras que otros están inactivos en los sistemas. de información. Es posible prever la obligación de notificar cada modificación. Esta notificación también puede ser mensual o anual. Entonces tomaría el carácter de una "evaluación informativa". Esta notificación permitiría ejercer el derecho de rectificación, si el usuario encuentra que la modificación ha inducido a error.

IUS ET SCIENTIA • 2023
Vol. 9 • N° 1 • pp. 23-45
ISSN 2444-8478 • https://doi.org/10.12795/IESTSCIENTIA.2023.i01.03

III. SUCINTA APROXIMACION A LOS SISTEMAS LEGALES COMPARADOS; CONTRASTE ENTRE ESTADOS UNIDOS Y LA UNIÓN EUROPEA

En los entornos tecnológicamente más avanzados y libres, como son Estados Unidos y la Unión Europea, las claves se plantean en términos del grado de complementariedad que debe existir entre la ley y la tecnología en la protección de la privacidad en el medio telemático. Se hace omisión de aquellos países carentes de un régimen libertades homologable, en los que (como sucede actualmente en la R. P. China), la privacidad ciudadana prácticamente no existe, siendo precisamente la tecnología el medio característicamente más empleado por el poder político para fiscalizar hasta límites intolerables áreas que deben quedar reservadas a la intimidad y libertades de los ciudadanos. Casi desde los inicios de las TIC muy pronto surgió la idea de que aquéllas, lejos de ser una vía de intromisión de los poderes hacia los ciudadanos (como también lo ha sido) podrían por el contrario ser la mejor defensa frente a la curiosidad de las fuerzas de orden público y demás poderes del Estado, así como de cara a los más poderosos agentes económicos. Fue por supuesto en los Estados Unidos, donde en ausencia de un marco verdaderamente protector, tomó forma esta perspectiva de protección a través de la tecnología. Esta acepción combina dos características sobresalientes de la civilización estadounidense cuales son la fe tanto en la tecnología como en la responsabilidad individual (todo el mundo tiene un derecho de autoprotección). En esta búsqueda de tecnologías de protección de la privacidad, sin duda resultaba necesario distinguir entre aquellas cuyo uso depende directamente del usuario (criptografía), aquellas otras que son implementadas por proveedores de servicios especializados (como son aquellos que ofrecen garantizar un sano anonimato que salvaguarde la intimidad de los usuarios de cara al mundo telemático), y finalmente aquellas que formarían parte de la arquitectura de redes y sistemas. Se buscaron así nuevos principios como los relacionados con consentimiento hacia la disposición de datos personales, pero basados no en la legislación, sino en tecnologías accesibles y manejables por los usuarios. Tal es el ejemplo del conocido como estándar P3P, que permite a los usuarios de internet reconocer automáticamente la política de protección de datos del sitio cuando se conectan a un sitio. De la protección "individual" o "de mercado" (encomendada a los proveedores de servicios), se habría pasado, con el citado P3P, a una forma de protección colectiva. Por lo tanto, al otro lado del Atlántico ha venido existiendo un interés creciente en la idea de que los principios de privacidad deben incorporarse a la arquitectura de los sistemas técnicos como un código de conducta cuyos modos de empleo han de estar en todo caso en los ciudadanos. Para los juristas estadounidenses que teorizan alrededor de este enfoque consistente en incorporar el derecho a la tecnología (la tecnología hace que el derecho sea exigible), corresponde al debate público y, en última instancia, a la autoridad política, establecer objetivos; será pues la labor de los ingenieros de programación y de las empresas para traducir estos objetivos en la operación de las redes.

El modo americano se tradujo en su momento en una fuerte tentación de optar por la concepción americana de protección individual (protegerse a sí mismo) frente

IUS ET SCIENTIA • 2023
Vol. 9 • N° 1 • pp. 23-45
ISSN 2444-8478 • https://doi.org/10.12795/IESTSCIENTIA.2023.i01.03

a la concepción europea de protección por el Derecho legislado y más estandarizado en lo que competía a la protección de datos en el medio telemático, inclusive en las relaciones entre las Administraciones y los ciudadanos. Por ejemplo, durante el debate en Alemania sobre la transposición de la Directiva de protección de datos de 1995, con internet cada vez más adentrado en la vida de los ciudadanos, la llamada escuela de la "modernización ofensiva" (a la que pertenecían los comisionados federales y estatales de protección de datos) pretendía propiciar una reforma sustancial de la legislación alemana, con vistas a mejorar la protección previstas actualmente en su legislación. Esta misma escuela reivindicó la libertad de la criptografía, alegando que cada vez será más responsabilidad de los ciudadanos protegerse mediante el uso de software de criptografía. Sin embargo, estas pulsiones parecen en Europa, al menos por el momento, ampliamente conjuradas o en declive. En concreto en lo que afecta a la UE, como super-Administración pública que ejerce sus competencias decisorias en el territorio de sus Estados miembros (de cara por supuesto a todas sus instancias administrativas y gubernativas, e inclusive con pretensiones de extender sus prerrogativas por lo que afecta al exterior, cuando son intereses de ciudadanos europeos los que resultan afectados) quedaba asumido que se debería contar con una normativa suficiente para tan trascendental misión, y hacerla cumplir de cara a las autoridades nacionales y, como no, respecto a sí misma. Ello ha sido el elemento originario de toda esa preocupación posterior, la cual habría constituido (en teoría) una prioridad irrenunciable para las autoridades tanto de la propia UE como de sus Estados miembros, matices estos que se preocupa en recalcar cierta doctrina especializada ya citada, no sin cierto escepticismo en cuanto a la coherencia entre intenciones iniciales y resultados efectivamente alcanzados (Brunet; 2019, p. 117).

IV. LÍNEAS RECTORAS DE LA NORMATIVA DE LA UNIÓN EUROPEA EN MATERIA DE PROTECCIÓN DE DATOS Y SU APLICACIÓN A LA ADMINISTRACIÓN ELECTRÓNICA

El estilo finalmente triunfador entre nosotros fue obviamente, el de origen netamente europeo, es decir, de confiar la tutela a procedimientos legales y con supervisión judicial en vez de que los administrados fueran ellos los que se autodefendiesen con instrumentos tecnológicos adecuados. Pero ello no quiere decir que el entramado legislativo en su aplicación a las relaciones con los e-administrados, estuviese carente de problemas concretos muy acuciantes, fruto precisamente de este prurito garantista. Cierto es que, desde el plano normativo desarrollado por las instituciones europeas, las cuestiones de la protección de datos revistieron, siempre en este estilo à *l'européenne*, un especial interés, a caballo de dos disposiciones trascendentales, que si bien no exclusivas del ámbito telemático, han deparado respecto de dicho entorno un trascendental impacto. Tales fueron inicialmente la Directiva de 1995 de Protección de Datos, la cual resultaría reemplazada por el vigente RPD. A tenor de lo acabado de afirmar, conviene partir del elemento central de la norma europea actual, esto es, del concepto de dato personal.

IUS ET SCIENTIA • 2023
Vol. 9 • N° 1 • pp. 23-45
ISSN 2444-8478 • https://doi.org/10.12795/IESTSCIENTIA.2023.i01.03

IUS ET SCIENTIA • 2023
Vol. 9 • Nº 1 • pp. 23-45
ISSN 2444-8478 • https://doi.org/10.12795/IESTSCIENTIA.2023.i01.03

De conformidad con el art. 4.1 del RPD, se define dato personal como cualquier información relativa a una persona física identificada o identificable (esto es, cada interesado); el citado instrumento especifica además que la persona física que puede ser identificada, directa o indirectamente, con especial referencia a un identificador como el nombre, un número, se considera identificable la identificación, los datos de ubicación, un identificador en línea o uno o más elementos característicos de su identidad física, fisiológica, genética, psíquica, económica, cultural o social. Cabe señalar que esta lista es meramente un ejemplo y no es exhaustiva. Además, se presta especial atención a los datos obtenidos mediante identificación tecnológica incluyendo la localización a través de la I.P. A ello hay que sumar el particular cuidado en relación con los datos genéticos, biométricos y de salud. Estos datos junto con los datos fiscales, judiciales o cualesquiera otro de índole pública generados en desde las diversas Administraciones se incluyen íntegramente en los datos personales particulares.

Un segundo concepto esencial es el de tratamiento de datos. El RPD define el concepto de tratamiento de cualquier operación o conjunto de operaciones, realizadas con o sin la ayuda de procesos automatizados y aplicadas a datos personales o conjuntos de datos personales, tales como la recolección, registro, organización, estructuración, almacenamiento, adaptación o modificación, extracción, consulta, uso, comunicación por transmisión, difusión o cualquier otra forma de puesta a disposición, comparación o interconexión, limitación, cancelación o destrucción. Fundamental es el concepto de elaboración de perfiles, que se define como cualquier forma de tratamiento automatizado de datos personales consistente en la utilización de dichos datos personales para evaluar determinados aspectos personales relativos a una persona física, en particular para analizar o predecir aspectos relativos al desempeño profesional, la situación económica, salud, preferencias personales, intereses, confiabilidad, comportamiento, ubicación o viaje de esa persona con entidad natural. A la luz de la definición anterior, una cadena de tiendas que adquiere información o realiza acciones para comprender mejor los intereses, preferencias, lugares frecuentados o posibilidades de gasto de una persona está realizando una actividad de elaboración de perfiles. A nadie le es extraño que las Administraciones son las primeras entidades que, con la excusa de mejor ajustar el buen gobierno y aplicar por ejemplo las mejores políticas presupuestarias, elaboran amplios y detallados perfiles estadísticos entre las diversas clases de administrados. Este aspecto es puesto de relieve de entrada en la Exposición de Motivos del RPD, la cual aborda la cuestión del interés público en lo concerniente al tratamiento de datos[1]. A mayor abundamiento, tal especificidad también es evidente en el tratamiento de datos sensibles. El principio de prohibición de tratamiento de tales datos, establecido en el art. 9.1 del RPD, encuentra muchas excepciones en el 9.2. Ya en el ámbito de la cooperación policial y judicial, donde el consentimiento de la persona tiende a ceder completamente el paso al único control de legalidad y proporcionalidad por parte de la autoridad pública (Gambardella; 2017, p. 63). En conclusión, la creación de un derecho de protección de datos para el tratamiento de los datos necesarios para el ejercicio de las prerrogativas del poder público podrá por tanto, fomentar la aparición de características específicas y reglas ajustadas. Por lo tanto, hay mucho en juego porque según

las normas jurídicas aplicables a los derechos concedidos a los particulares variarán. El riesgo de tal especificidad es entonces, al dejar de ser materia de derecho de la Unión y la conformidad que implica, excluir todo un régimen jurídico de protección de los derechos fundamentales (Gambardella; 2017, p. 65).

Por lo tanto, es una relación jurídico administrativa la que se construye con respecto al tratamiento de datos cuando hay por un lado poderes públicos y por otro administrados, matices que, como veremos posteriormente, la jurisprudencia comunitaria ha tenido la ocasión de precisar [2]. En dicho modo relacional de naturaleza pública el ciudadano figuraría como presunto titular de sus datos (aspecto que como veremos en su momento, no está ni tan claro ni tan asumido), mientras que cada Administración concernida quedaría como responsable del tratamiento de esos datos. Tal relación debería en principio basarse, de acuerdo con el RPD, con arreglo a un principio de consentimiento en el tratamiento, expresado por dicho ciudadano, dado que un aspecto crucial en el tratamiento de datos personales es, precisamente, el relativo al consentimiento para dicho tratamiento. Es por tanto necesario obtener el consentimiento de la persona para procesar sus datos. Si alguna entidad dispone de datos para los que no se ha prestado o solicitado previamente el consentimiento, será conveniente que contacte con el interesado y le pida dicha conformidad de forma expresa. En su art. 7.2 el RPD especifica a continuación que si el consentimiento del interesado se da en el marco de una declaración escrita que también se refiere a otras cuestiones, la solicitud de consentimiento se presenta de forma claramente diferenciable de los demás aspectos envueltos, de forma comprensible y de fácil acceso, utilizando un lenguaje sencillo y claro. Lo que sucede es que este aspecto suele cada vez más automatizarse por mecanismos de *click wrapping*, como el de aceptación de *cookies* del sitio, en los cuales se juega a menudo con el acto reflejo y no debidamente meditado por el usuario o administrado. Lo deseable tratándose de una relación jurídico-pública que ha de ser transparente sería que fuese imprescindible solicitar al usuario el consentimiento expreso para el tratamiento de datos en una pantalla específica del sitio web, posiblemente mediante la inserción de un botón independiente, sin confundirlo, ni insertarlo, con otros elementos diferentes. Si los datos han sido adquiridos previamente, solicitar de nuevo el consentimiento para el tratamiento. También será conveniente revisar la información facilitada al usuario sobre el uso de los datos ya que el responsable del tratamiento está obligado a indicar de forma clara y expresa para qué finalidades tratará los datos. En todo caso, y como contrapunto a lo acabado de afirmar, es también en la Exposición de Motivos del RPD donde hallamos menciones a ciertos casos o facetas particularmente sensibles con respecto de la actividad administrativa, en las cuales debe haber una óptica de salvaguardia del interés general frente al otro bien jurídicamente protegido de la intimidad, y por añadidura, del consentimiento prestado por parte de los sujetos particulares afectados [3].

El tratamiento de datos debe reportar una conciencia de responsabilidad para aquel que verifica el tratamiento, lo cual implica a su vez dos nociones, la del principio de responsabilidad en el tratamiento y la del titular de dicha responsabilidad, esto es, el responsable del tratamiento. La conformación del principio de responsabilidad constituye una de las novedades más importantes del RPD. Sobre la base de este principio,

IUS ET SCIENTIA • 2023
Vol. 9 • Nº 1 • pp. 23-45
ISSN 2444-8478 • https://doi.org/10.12795/IESTSCIENTIA.2023.i01.03

el controlador de datos, o la persona que adquiere los datos del usuario, implementa medidas técnicas y organizativas adecuadas para garantizar y poder demostrar que el procesamiento se lleva a cabo de conformidad con el instrumento normativo europeo que ahora nos ocupa (art. 24.1). También es la persona responsable de garantizar y comprobar el cumplimiento de los principios relativos al tratamiento de datos personales, establecidos en el art. 5.1 (por ejemplo, licitud, corrección y transparencia, imitación de finalidad, minimización de datos, etc.).

Por su parte el art. 4.7 del RPD define al responsable o encargado del tratamiento como cualquier persona física o jurídica, autoridad pública, servicio u otro organismo que, individualmente o junto con otros, determine los fines y medios del tratamiento de datos personales; cuando los fines y medios de dicho tratamiento estén determinados por el Derecho de la Unión o de los Estados miembros, el responsable del tratamiento o los criterios específicos aplicables a su designación podrán ser establecidos por el Derecho de la Unión o de los Estados miembros. El RPD apoya al controlador de datos, al procesador de datos o a la persona física o jurídica, autoridad pública, servicio u otro organismo que procese datos personales en nombre del procesador de datos, así como también establece la posibilidad, siempre con el debido control, que se puedan estipular acuerdos puntuales y específicos en relación con el tratamiento de datos entre cada controlador de datos (la empresa o entidad pública titular del tratamiento) que pretenda externalizar el tratamiento de datos personales, y el encargado del tratamiento (el proveedor de servicios externalizados, ya sea un *outsourcer* tradicional o un proveedor de servicios en la nube). A mayor abundamiento, el art. 28.3, del RPD establece que el contrato vinculante para el responsable del tratamiento debe prever en particular: a)- la obligación de tratar los datos únicamente de acuerdo con las instrucciones a las que el responsable deba atenerse (y que deberán estar debidamente documentadas y recibidas por aquél), incluso en caso de transferencia de datos fuera de la Unión Europea; b)- la obligación de garantizar que las personas físicas autorizadas para realizar las actividades de tratamiento estén sujetas a obligaciones de confidencialidad, asumidas contractualmente o establecidas por la ley; c)- la obligación de tomar las medidas requeridas de conformidad con el art. 32 del RPD, es decir, las medidas técnicas y organizativas de protección de los datos que se consideren adecuadas para garantizar un nivel de seguridad adecuado al riesgo inherente al tratamiento [4].

Completa el cuadro de personaje implicados en el correcto tratamiento de los datos el Delegado de Protección de Datos o D.P.O., como agente especialmente designado por el responsable del tratamiento para desempeñar funciones específicas en clave de correcto empleo y gestión de los datos. El D.P. O. constituye una figura, parcialmente novedosa y propensa a deparar no poca confusión tras la adopción del RPD [5]. La empresa (y por analogía, el servicio público competente) deberá dotarle de estructuras, medios técnicos y económicos y equipos proporcionales a su cometido. Las funciones del D.P.O. están previstos en los artículos 37 y 39 del RPD y entre los más relevantes se encuentra el deber de informar y asesorar al Responsable del tratamiento y a sus empleados respecto de la legislación de la Unión y de los Estados individuales sobre la materia, verificar la implementación de la citada normativa, actuar como punto de contacto tanto hacia la Autoridad de

IUS ET SCIENTIA • 2023
Vol. 9 • Nº 1 • pp. 23-45
ISSN 2444-8478 • https://doi.org/10.12795/IESTSCIENTIA.2023.i01.03

IUS ET SCIENTIA • 2023
Vol. 9 • N° 1 • pp. 23-45
ISSN 2444-8478 • https://doi.org/10.12795/IESTSCIENTIA.2023.i01.03

Privacidad como hacia los usuarios, comunicar su opinión en relación con la evaluación de impacto en la protección de datos. Además, sin estar dentro de las funciones de regulación, puede tener encomendado el registro de las actividades de tratamiento.

V. ANALISIS SISTEMÁTICO DE LA JURISPRUDENCIA DEL TRIBUNAL DE JUSTICIA DE LA UE EN LA MATERIA

Lo interesante es que al respecto disponemos de expresiones en las dos clases de modalidades de cuestiones prejudiciales que existen en el contexto del Derecho europeo, tanto en su variante interpretativa, como con relación a su modalidad de apreciación de validez, y que afectan, según las fechas, tanto a la derogada Directiva de 1995 como al vigente RPD de 2016. Las jurisprudencias anteriores son por lo general aprovechables en el contexto actual, pese a la diferente naturaleza normativa que presentan una y otra expresión del Derecho derivado. A este respecto cierta doctrina reivindica el papel del Juez comunitario como verdadero garante constitucional de los derechos de los administrados frente a las entidades públicas en lo que atañe a la protección de datos con arreglo a la normativa de la UE (Peyrou; 2015, p. 213), elemento que se reivindica como una expresión de un nuevo concepto de seguridad jurídica ligada a las NN TT (Tambou; 2020, p. 43).

Las cuestiones prejudiciales interpretativas responden a una doble problemática, de tal modo:

a) Tenemos desde un extremo casos en los que los particulares que ven limitadas por las Administraciones públicas competentes sus solicitudes de que les sean facilitados sus propios datos personales de los que aquéllas son depositarias. La idea central de todos estos pronunciamientos es que las limitaciones interpuestas por las Administraciones son admisibles, siempre que medie la debida proporcionalidad, nunca con carácter absoluto (criterio a la postre éste jurídicamente indeterminado y que el TJUE dirige al Juez nacional de reenvío) estando presentes ejemplos que afectan tanto a la Directiva[6] como al Reglamento[7]. Destaca en este contexto el refuerzo de la idea, según la cual la I.P. constituye un dato personal de primer orden emn cuanto a los imperativos de su tratamiento informático mediatizado judicialmente (Péronne/ Daoud; 2017, P. 120).
b) Como contraste, hallamos algún ejemplo disperso deparado por algún particular que se opone a las imposiciones que les remiten las autoridades nacionales de facilitar datos personales de terceros, teniendo como elemento dirimente al RPD. Vuelve aquí a imperar un consejo de proporcionalidad dirigido al Juez nacional encargado de entender de la causa[8].

No menos interesantes son los ejemplos recaídos en la variante, mucho menos frecuente de la apreciación de validez, en donde determinadas disposiciones de la propia Unión Europea son puestas en entredicho, para después ser destinadas a ser inaplicadas como inválidas, tras su contraste con respecto de la normativa de protección de

datos. Llaman en el contexto electrónico que afecta a las relaciones dos supuestos especialmente llamativos, que se suceden en contextos tanto internos [9] como externos a la propia UE, pero que afectan a ésta y que, por el devenir del tiempo conciernen tanto a la Directiva de 1995 como al actual RPD. Es aquí donde encuentran su ubicación los complejos avatares de las jurisprudencias Schrems I y II del TJUE, sobre la que tan abundantemente se ha escrito poniendo de relieve sus contradicciones y carencias a cargo de la doctrina tanto internacional (Castests-Renard; 2016, p. 88), como española (Uría Gavilán; 2016, p. 261) [10].

Conclusiones

Con la normalización del fenómeno de la Administración electrónica a múltiple nivel, también conocida como e-Gobernanza, las corporaciones de Derecho público han hecho soportar a los usuarios una nueva forma de complejidad administrativa, como así nuevos deberes en cuanto al tratamiento de sus datos, tanto personales como de terceros. El requisito de privacidad está lejos de ser la causa única o central de la complejidad administrativa construida alrededor de una cierta cultura administrativa basada en la desconfianza, que trata a los usuarios como posibles estafadores, y lleva a exigirles montones de documentos y certificados para justificar su situación. El surgimiento de las TIC, debido a que facilitan considerablemente el intercambio de información que hasta ahora era difícil y costoso de organizar, propicia un caldo de cultivo de colisión entre la eficiencia en la gestión, la seguridad colectiva y el mantenimiento de la privacidad e intimidad del ciudadano mismo. Y si bien queda demostrado que no procede considerar a los ciudadanos como propietarios, en el sentido romanista del término, de sus datos telemáticos en lo que atañe al entorno telemático, tampoco deja de ser admisible que, en correlativa muestra de pedagogía o ejemplo, también las Administraciones públicas deben poner su parte para facilitar una imagen respetuosa y responsable con esos mismos datos, en su rol de tratantes de los datos de los Administrados.

Resulta notoria la tarea de determinar los roles que incumben a las diversas Administraciones públicas nacionales de los Estados miembros de la UE, y que con un plus de exigencia serían contemplables desde el actual RPD. En este ámbito, la presencia de una más que incipiente o inicial jurisprudencia por parte del TJUE (que como hemos podido apreciar, oscila desde la idea de equilibrio y proporcionalidad en las cuestiones prejudiciales interpretativas, hasta un alto grado de exigencia en aquellas otras cuestiones prejudiciales en apreciación de validez, que llegan al extremo de anular inclusive Decisiones de la UE), constituye una vez más un elemento consustancial y necesario a este trascendental entorno, que comparte todos los rasgos y elementos característicos del engranaje jurídico comunitario. Siempre con este trasfondo proteccionista de la normativa europea hacia el administrado, si se quiere podemos transigir con que un nuevo pacto, a renegociar, estaría basado en la confianza de la Administración en los usuarios. La llamada E-Gobernanza también podría, en base a su conocimiento de situaciones personales, informar a los usuarios de los derechos que pueden ejercer. Todos estos

IUS ET SCIENTIA • 2023
Vol. 9 • N° 1 • pp. 23-45
ISSN 2444-8478 • https://doi.org/10.12795/IESTSCIENTIA.2023.i01.03

deseos deben ponerse a la luz de la compleja casuística analizada en los asuntos jurisprudenciales, contando con que el paradigma deparado por la legalidad ya no es de factura nacional, ni siquiera transponiendo en normas nacionales una Directiva como sucedía con la antigua norma de esta especie de 1995, sino que ahora contamos con un instrumento completo y obligatorio en todos sus elementos, el RPD.

1. Concretamente leemos en el Considerando 111: "Se debe establecer la posibilidad de realizar transferencias en determinadas circunstancias, de mediar el consentimiento explícito del interesado, si la transferencia es ocasional y necesaria en relación con un contrato o una reclamación, independientemente de tratarse de un procedimiento judicial o un procedimiento administrativo o extrajudicial, incluidos los procedimientos ante organismos reguladores. También se debe establecer la posibilidad de realizar transferencias cuando así lo requieran razones importantes de interés público establecidas por el Derecho de la Unión o de los Estados miembros, o cuando la transferencia se haga a partir de un registro establecido por ley y se destine a consulta por el público o por personas que tengan un interés legítimo. En este último caso la transferencia no debe afectar a la totalidad de los datos personales o de las categorías de datos incluidos en el registro y, cuando el registro esté destinado a su consulta por personas que tengan un interés legítimo, la transferencia solo debe efectuarse a petición de dichas personas o, si estas van a ser las destinatarias, teniendo plenamente en cuenta los intereses y los derechos fundamentales del interesado".

2. STJUE de 9 de julio de 2022 recaída en el As 272/19, VQ contra Estado de Hesse.

3. Leemos en el Considerando 112: "Dichas excepciones deben aplicarse en particular a las transferencias de datos requeridas y necesarias por razones importantes de interés público, por ejemplo en caso de intercambios internacionales de datos entre autoridades en el ámbito de la competencia, Administraciones fiscales o aduaneras, entre autoridades de supervisión financiera, entre servicios competentes en materia de seguridad social o de sanidad pública, por ejemplo en caso contactos destinados a localizar enfermedades contagiosas o para reducir y/o eliminar el dopaje en el deporte. La transferencia de datos personales también debe considerarse lícita en caso de que sea necesaria para proteger un interés esencial para los intereses vitales del interesado o de otra persona, incluida la integridad física o la vida, si el interesado no está en condiciones de dar su consentimiento. En ausencia de una decisión de adecuación, el Derecho de la Unión o de los Estados miembros puede limitar expresamente, por razones importantes de interés público, la transferencia de categorías específicas de datos a un tercer país o a una organización internacional. Los Estados miembros deben notificar esas disposiciones a la Comisión. Puede considerarse necesaria, por una razón importante de interés público o por ser de interés vital para el interesado, toda transferencia a una organización internacional humanitaria de datos personales de un interesado que no tenga capacidad física o jurídica para dar su consentimiento, con el fin de desempeñar un cometido basado en las Convenciones de Ginebra o de conformarse al Derecho internacional humanitario aplicable en caso de conflictos armados".

4 Teniendo en cuenta la naturaleza del tratamiento y la información de que dispone, la obligación de asistir al titular consiste: a)- en garantizar la protección de datos a través de medidas técnicas y organizativas apropiadas, de conformidad con el art. 32 del RPD; b)- en la notificación a la Autoridad de cualquier violación de datos (violaciones de datos) que se haya producido, de conformidad con el art. 33 del RPD; c)- en la comunicación a los interesados de las violaciones de datos que se hayan producido, en los casos previstos por el art. 34 del Reglamento; d)- en la realización de la evaluación de impacto exigida por el art. 35 del RPD; y e)- en consultar a la Autoridad, si la evaluación de impacto realizada indica que el tratamiento presentaría un alto riesgo en ausencia de medidas tomadas por el controlador de datos para mitigar el riesgo. Asimismo, el responsable del tratamiento tiene las siguientes obligaciones: primera, cancelar o devolver los datos, a elección del titular, en el momento de la terminación de la relación, salvo que la ley imponga obligaciones específicas de conservación; segunda, poner a disposición del titular toda la información necesaria para demostrar el cumplimiento

IUS ET SCIENTIA • 2023
Vol. 9 • Nº 1 • pp. 23-45
ISSN 2444-8478 • https://doi.org/10.12795/IESTSCIENTIA.2023.i01.03

de las obligaciones establecidas en esta lista; y tercera, permitir al titular la realización de auditorías, directamente o a través de terceros designados al efecto.

5. Configurado en los arts. 37 y siguientes, su traslación al contexto público plantea amplios interrogantes, y eso que en esta normativa comunitaria se prevé la obligatoriedad del D.P.O. en una serie de casos, concretamente: primero, para todas las Administraciones públicas, incluidas las empresas privadas que realicen funciones publicitarias o ejerzan poderes públicos; y segundo, para todas las empresas que realicen un seguimiento regular y sistemático de datos a gran escala (geolocalización con fines estadísticos, análisis de consumo y preferencias, análisis de datos para publicidad dirigida) para quienes procesan datos relacionados con delitos y condenas penales. Cabe señalar que la lista no pretende ser exhaustiva y por tanto debe ser la empresa individual la que evalúe la conveniencia, en función de su tipo de actividad, de nombrar al D.P.O. No obstante, la designación de un D.P.O. sin duda puede constituir una medida importante para demostrar la adecuación y el cumplimiento del responsable del tratamiento en relación con las disposiciones del RPD. A diferencia del responsable del tratamiento y del encargado del tratamiento, el Delegado de Protección de Datos no puede ser una persona jurídica debiendo, necesariamente, siendo una persona natural, además debe reunir los siguientes requisitos; 1º)- poseer un conocimiento adecuado de la legislación y las prácticas de gestión de datos personales; 2º)- desempeñar sus funciones con total independencia y en ausencia de conflictos de intereses; y 3º)- para trabajar para el propietario o gerente o sobre la base de un contrato de servicios.

6. En primer término, y como precedente más remoto a nuestro entender de cuestión prejudicial interpretativa de la Directiva de 1995 en los contextos de litigios en materia de datos personales entre una Administración y un ciudadano, la hallamos la STJUE de 7 de mayo de 2009 Rijkeboer, As 553/07. Aquí el problema versa sobre las limitaciones en el periodo temporal respecto del cual el particular puede reclamar información sobre sus datos personales a la Administración. Sucedía que el interesado, con motivo de un traslado de domicilio, solicitó una relación de todas las comunicaciones a terceros de información relativa a él procedente de la base de datos de padrón municipal, efectuadas durante los dos años anteriores a su petición, y que versaban acerca de su domicilio antiguo. Unas comunicaciones, debe entenderse, que se realizaron por vía telemática. Sin embargo, la Entidad municipal limitaba dicha información a un año. El TJUE entendió que, si bien era competencia nacional, conforme a la Directiva, fijar un plazo suficiente, una normativa que limitaba la conservación de la información sobre los destinatarios al período de un año, limitando correlativamente el acceso a dicha información, si bien los datos se conservan durante mucho más tiempo, no constituía un justo equilibrio entre el interés tutelado y la obligación de mantener la intimidad de los sujetos que habían recibido dicha información. Según el TJUE el campo de aplicación de la entonces vigente Directiva 95/46 resultaba ser muy amplio, de manera que el concepto en sí de dato personal en lo que atañe a su tratamiento por los poderes públicos es muy diverso, y en cualquier caso cuando aquéllos son responsables del tratamiento su desempeño no puede resultar imposible o suponer un esfuerzo desproporcionado (Considerandos 59 a 61).

Un segundo ejemplo de análoga naturaleza lo tenemos en la STJUE de 12 de diciembre de 2013, en As 486/12. En ella vemos que un individuo identificado como X pretendía consultar su domicilio a efecto de notificaciones respecto a multas de tráfico, y veía limitado su derecho por una exigencia de cobro al respecto exigida por la Administración. Considerando la informatización que impera en toda la tramitación de las sanciones derivadas por infracciones de tráfico, un ciudadano multado quiere recurrir para no pagar la infracción aduciendo la posibilidad de que se le haya notificado a una dirección no actualizada o errónea. Con ese objeto solicitó al municipio donde residía la comunicación de sus datos de carácter personal de los años 2008 y 2009, en especial sus sucesivas direcciones y así fundamentar su recurso. Pero el Ayuntamiento reclamaba una tasa de 12,80 euros por suministrar dicha información. Es lo que el interesado intentó recurrir sin éxito ante el orden jurisdiccional administrativo neerlandés. En idéntica línea a la de la proporcionalidad el TJUE indica que la Directiva que no se opone a la percepción de gastos por la comunicación de datos de carácter personal por una autoridad pública. Eso sí, el importe de tales gastos no debe exceder el coste de la comunicación de dichos datos, siendo tarea del tribunal nacional competente realizar las verificaciones necesarias a tal efecto.

IUS ET SCIENTIA • 2023
Vol. 9 • Nº 1 • pp. 23-45
ISSN 2444-8478 • https://doi.org/10.12795/IESTSCIENTIA.2023.i01.03

IUS ET SCIENTIA • 2023
Vol. 9 • Nº 1 • pp. 23-45
ISSN 2444-8478 • https://doi.org/10.12795/IESTSCIENTIA.2023.i01.03

Una tercera muestra que versa acerca de la interpretación de la Directiva de 1995 es la deparada por la STJUE Breyer de 2016 As 582/14. Aquí lo cuestionado es el procedimiento de recopilación sistemática por parte de las Autoridades alemanas de las IP de consulta de páginas de organismos federales por parte de los particulares con fines de seguridad. Ante ello el Sr. Breyer presentó, ante los órganos jurisdiccionales de lo contencioso-administrativo alemanes, un recurso con el objeto de que se prohibiera a la República Federal de Alemania conservar o permitir que terceros conservasen, al final de las sesiones de consulta de sitios accesibles al público de medios en línea de organismos federales alemanes, la dirección IP del sistema principal de acceso del Sr. Breyer, en la medida en que dicha conservación no fuera necesaria, en caso de fallo, para el restablecimiento de la difusión de esos medios. La jurisdicción nacional plantea si una dirección IP registrada por un prestador de servicios o de medios en línea en relación con un acceso a su sitio de internet constituye para éste un dato personal desde el momento en que un tercero (en este caso, un proveedor de acceso) disponga de los datos adicionales que permiten identificar al interesado, a lo que el TJUE respondió afirmativamente. Quedaba por averiguar pues las limitaciones a las que había que someter dicha actividad. Se entendió que la Directiva se oponía a una normativa de un Estado miembro con arreglo a la cual un prestador de servicios de medios en línea sólo podría recoger y utilizar datos personales de un usuario de esos servicios sin mediar el consentimiento de éste, cuando dichas recogida y utilización, entendiéndose necesarias para posibilitar y facturar el uso concreto de dichos servicios por ese usuario, fuesen más allá del objetivo de garantizar el funcionamiento general de esos mismos servicios.

7. Encontramos aquí la solitaria muestra que encarna la STJUE de 9 de julio de 2020 que en el As 272/19 enfrentaba al individuo designado como VQ al Estado de Hesse. Acontece que la Comisión de peticiones del Parlamento de un Estado Federado alemán, que se niega a suministrar las informaciones que posee de un determinado ciudadano, se la considera responsable del tratamiento, incluido el tratamiento informático por sus aplicaciones propias/ Además se define la noción de Autoridad pública a efectos del Reglamento, incluyendo a un organismo como la Comisión de Peticiones. En efecto, tras presentar una petición a la Comisión de peticiones del Parlamento del Estado Federado de Hesse, VQ solicitó a dicha Comisión, basándose en el artículo 15 del RPD, el acceso a los datos de carácter personal que le afectaban, y que consiguientemente quedaban registrados por dicha Comisión en el marco del tratamiento de su petición. El presidente del Parlamento del Estado Federado de Hesse decidió rechazar esa solicitud debido a que el procedimiento de petición constituye una función parlamentaria y que dicho Parlamento no está comprendido en el ámbito de aplicación del RPD. El 22 de marzo de 2013, VQ interpuso recurso ante el *Verwaltungsgerich*t Wiesbaden (Tribunal de lo Contencioso-Administrativo de Wiesbaden. El TJUE estima que el Reglamento 2016/679 no recoge definición alguna del concepto de "autoridad pública". Según el *Verwaltungsgericht*, a esa expresión se le puede otorgar una acepción funcional o una acepción institucional. Con arreglo a la primera de esas acepciones, serían autoridades públicas "todas las autoridades públicas que ejerzan funciones de Administración pública, incluido, por tanto, el Parlamento del Estado Federado de Hesse cuando lleve a cabo tales funciones. En tal línea la Comisión de peticiones del mencionado Parlamento es un organismo autónomo, y por tanto una autoridad pública, en el sentido institucional". Así las cosas, y con las consideraciones de autoridad pública expresadas por la jurisdicción contenciosa germana de reenvío, el TJUE responde que el art. 4.7 del RPD debía interpretarse, "en la medida en que una comisión de peticiones del Parlamento de un Estado federado de un Estado miembro determina, sola o junto con otros, los fines y los medios del tratamiento, esa comisión debe calificarse de responsable del tratamiento a efectos de dicha disposición, de modo que el tratamiento de datos personales efectuado por la mencionada comisión está comprendido en el ámbito de aplicación de dicho Reglamento, en particular de su art. 15".

8. En concreto se trataba de una obligatoriedad de remisión a Hacienda del número de bastidor de los vehículos que se vendían en un portal de internet gestionado por una empresa. En efecto, SS es un proveedor de servicios de publicación de anuncios en internet con domicilio social en Letonia. La Administración tributaria letona remitió a SS una solicitud de información en la que instaba a la citada sociedad a renovar el acceso de que disponía dicha Administración tributaria a los números de bastidor de los vehículos anunciados en el portal de Internet de la sociedad mencionada y a los números de teléfono de los vendedores y a facilitarle información sobre los anuncios publicados en la sección relativa a los turismos del referido portal durante cierto período comprendido entre los me-

ses de julio y agosto de 2018. La información que debía remitir el requerido consistían en la marca, el modelo, el número de bastidor y el precio del vehículo, así como el número de teléfono del vendedor. Tal conjunto de informaciones debía facilitarse por vía electrónica, en un formato que permitiera filtrar o seleccionar los datos. Al considerar que la solicitud de información de la Administración tributaria letona no era conforme con los principios de proporcionalidad y de minimización de datos personales, establecidos en el RPD, SS presentó un recurso en vía administrativa contra dicha solicitud ante el director general en funciones de la Administración tributaria letona. En sucesivas fases la cuestión llega a máximo tribunal de lo contencioso administrativo letón, el cual consideraba no discutible que la ejecución de la solicitud de información controvertida estuviese intrínsecamente vinculada a un tratamiento de datos personales, ni que la Administración tributaria letona tuviese derecho a obtener la información a disposición de un proveedor de servicios de publicación de anuncios en Internet, por cuanto resultase necesaria para la ejecución de medidas específicas en materia de recaudación de impuestos. El problema versaba en realidad sobre la cantidad y el tipo de información que podía solicitar la Administración tributaria letona, sobre su carácter limitado o ilimitado, y sobre la cuestión de si la obligación de información a la que estaba sujeta la empresa requerida debía conocer asimismo una limitación en el tiempo. El TJUE entiende que la recogida, por parte de la Administración tributaria de un Estado miembro, de información que implique una cantidad considerable de datos personales de manos de un operador económico está sujeta a los requisitos de dicho Reglamento, en particular a los enunciados en su art.5.1, las cuales sólo pueden ser obviadas si la Administración en cuestión tiene respaldo legislativo expreso. Consideradas todas estas cuestiones, por motivos de salvaguarda de la soberanía fiscal, se proclama que "nada se opone a que la Administración tributaria de un Estado miembro exija a un proveedor de servicios de publicación de anuncios en internet que le facilite información relativa a los contribuyentes que hayan publicado anuncios en alguna de las secciones de su portal de internet siempre que, en particular, tales datos sean necesarios a la luz de los fines específicos para los que se recaban y que el período de recogida no exceda del estrictamente necesario para alcanzar el objetivo de interés general perseguido".

9. La muestra interna, tocante a la Directiva del 1995, viene representada por la STJUE de 9 de noviembre de 2010, que en los As Acum. 92/09 y 93/09 opusieron a Volker y otros al Estado Federado de Hesse. Resultaba aquí que en estos asuntos agrupados por el TJUE, y relativos a la PAC, ciertas empresas agrícolas alemanas interesadas contestaban como inadecuada la práctica, según la cual, se les obligaba a firmar y reconocer para percibir las ayudas, a instancias de la *Bundesanstalt* (Administración Federal competente) que habían sido informadas de que en virtud de los Reglamento 1290/2005 y 259/2008 era obligatorio publicar los datos de los beneficiarios de fondos procedentes de FEAGA y FEADER, concretando los importes recibidos por cada beneficiario. Por lo que leemos en el relato fáctico, "dichos datos se colgaban en el sitio web de la *Bundesanstalt*, donde se ponían a disposición del público los nombres de los beneficiarios de ayudas del FEAGA y del FEADER, la localidad en la que están establecidos o en la que residen y el código postal de dicha localidad, así como los importes anuales percibidos" Y por añadidura dicho sitio web disponía de una función de búsqueda. Los interesados consideraban que dicha publicidad de datos contradecía los estándares de protección de la entonces vigente Directiva de 1995. El problema es que dicha obligación procedía de otras normas europeas, lo que planteaba su colisión e incompatibilidad en el contexto típico de la cuestión prejudicial de invalidez. El TJUE acuerda declarar que los referidos Reglamentos son inválidos en la medida en que obligan, por lo que respecta a las personas físicas beneficiarias de ayudas del FEAGA y del FEADER, a publicar datos de carácter personal de todos los beneficiarios, sin establecer distinciones en función de criterios pertinentes, tales como los períodos durante los cuales dichas personas han percibido estas ayudas, su frecuencia o, incluso, el tipo y magnitud de las mismas. Pero el alcance de esta invalidación no tiene efectos retroactivos. Se declara que la invalidez de los referidos Reglamentos no permite impugnar los efectos de las publicaciones de las listas de beneficiarios de ayudas del FEAGA y del FEADER llevadas a cabo por las autoridades nacionales, en virtud de dichas disposiciones, en el período anterior a la fecha de pronunciamiento de la presente sentencia. Y en idéntica línea, para el período antes de la sentencia, se excluye por tanto imponer al encargado de la protección de los datos personales la obligación de llevar el registro contemplado en esta disposición con anterioridad a la realización de un tratamiento de datos personales.

IUS ET SCIENTIA • 2023
Vol. 9 • Nº 1 • pp. 23-45
ISSN 2444-8478 • https://doi.org/10.12795/IESTSCIENTIA.2023.i01.03

10. Hablamos de las STJUES respectivamente de 6 de octubre de 2015 As 362/14 y de 16 de julio de 2020 As 311/18, correspondientes a los conocidos como casos Schrems I y II, los cuales conocen el tránsito, como norma de referencia para anular ciertas Decisiones de la Comisión, de la Directiva de 1995 al Reglamento de 2016 en materia de protección de datos. Ambos casos han determinado una prolija literatura, pues en ella entraban en colisión los modos de protección de datos personales de los ciudadanos de cara a las Administraciones públicas que imperan en la UE en un lado y en EE UU por otro.

Ya en el primer asunto, el TJUE declaró la invalidez de la Decisión 2000/520 sobre los principios de puerto seguro, mediante la cual la Comisión Europea estimaba que las transferencias de datos personales entre la Unión Europea y los Estados Unidos tenían un nivel de protección adecuado. Los motivos esenciales son no respeto del contenido esencial de derechos fundamentales consagrados en la Carta Europea de Derechos Fundamentales (en concreto sus art. 7 y art. 47), mientras que por añadidura desproveería a las autoridades nacionales del poder de evaluar la solicitud de una persona que cuestiona la compatibilidad de esa Decisión con aquellos derechos. Aparte, es la Directiva de protección de datos de 1995 entonces en vigor la otra norma esencial manejada por el TJUE en este otro ejemplo de cuestión prejudicial de apreciación de validez.

El contexto de la materia (resumido en los considerandos 27 y 28 de la STJUE Schrems I) eran que, al estar "toda persona residente en el territorio de la Unión que desee utilizar Facebook obligada a concluir en el momento de su inscripción un contrato con Facebook Ireland, filial de Facebook Inc., domiciliada ésta última en Estados Unidos (…) traía por consecuencia que los datos personales de los usuarios de Facebook Ireland residentes en el territorio de la Unión se transfieren en todo o en parte a servidores pertenecientes a Facebook Inc, situados en el territorio de Estados Unidos, donde son objeto de tratamiento". En 2013 el Sr. Schrems, nacional austriaco residente en Austria, es usuario de la red Facebook desde 2008 presentó ante el comisario irlandés de protección de datos (pues es en ese Estado miembro donde está la filial europea de la red social) "una reclamación en la que le solicitaba en sustancia que ejerciera sus competencias estatutarias, prohibiendo a Facebook Ireland transferir sus datos personales a Estados Unidos", siendo lo aducido que "que el Derecho y las prácticas en vigor en este último país no garantizaban una protección suficiente de los datos personales conservados en su territorio contra las actividades de vigilancia practicadas en él por las autoridades públicas". En el caso Schrems I se considera que la normativa de la Comisión controvertida, la Decisión 2000/520, cotejada con arreglo a la Directiva 95/46, y todo ello en consideración a la adecuación de la protección conferida por los principios de puerto seguro para la protección de la vida privada y las correspondientes preguntas más frecuentes (que fueron publicadas por el Departamento de Comercio de Estados Unidos de América, y por la que la Comisión Europea constató que dicho tercer país garantiza un nivel de protección adecuado), no impediría en ningún caso que una autoridad de control de un Estado miembro pudiese examinar, y en su caso acoger favorablemente, la solicitud de una persona relativa a la protección de sus derechos y libertades frente al tratamiento de los datos personales que van a conocer en un país tercero (EE UU), para así denegar en consecuencia la transferencia a aquél de tales datos personales. Ello llevó a la declaración de invalidez de la Decisión 2000/520, la cual habría de quedan inaplicada en el caso de especie.

El asunto conoció una secuela en el pronunciamiento Schrems II, en donde resultaron cuestionadas otras Decisiones diversas a las del caso anterior, pero de la misma naturaleza en su condescendencia al envío a las autoridades norteamericanas de datos de ciudadanos europeos desde la sede irlandesa de Facebook. En concreto, el TJUE sostuvo que otras Decisiones, conocidas como CPT, son válidas en principio, pero puede requerir garantías adicionales para garantizar un nivel de protección sustancialmente equivalente pero no idéntico al de la UE. Es posible que un importador de datos fuera de la UE no pueda hacer mucho, si es que puede hacer algo, para proteger los datos transferidos de los programas de vigilancia del gobierno, pero cualquier protección contractual que se pueda agregar puede ayudar tanto al exportador como al importador de datos a documentar sus esfuerzos para cumplir con un entorno legal incierto, en caso de que una autoridad reguladora de la UE cuestione una transferencia en particular y/o en caso de disputa. El TJUE declaró específicamente que, en los casos apropiados, un importador de datos de EE. UU. podría tomar diversos posicionamientos, así: declarar que no tiene motivos para creer que las personas afectadas por la transferencia de datos desde la UE están sujetos a los programas de vigilancia del gobierno de EE. UU.; declarar que no tiene

IUS ET SCIENTIA • 2023
Vol. 9 • Nº 1 • pp. 23-45
ISSN 2444-8478 • https://doi.org/10.12795/IESTSCIENTIA.2023.i01.03

motivos para creer que su legislación nacional le impediría cumplir con sus obligaciones en virtud de las CPT modificadas; comprometerse a implementar medidas técnicas y organizativas adicionales para garantizar la seguridad de los datos (como el uso de cifrado o el conocido como modo de transmisión VPN); comprometerse a verificar e informar al exportador de datos de la UE sobre la existencia de leyes locales que puedan comprometer la seguridad de los datos; comprometerse a informar inmediatamente al exportador de datos de la UE si tiene conocimiento de cualquier modificación de la legislación o normativa susceptible de tener consecuencias negativas sobre las garantías y obligaciones ofrecidas por las CPT, modificadas; o si se ve obligado a revelar datos personales a las autoridades gubernamentales, se comprometen a notificar al exportador de datos de la UE su incumplimiento de las CPT modificadas.

Se consideró en esta segunda ocasión, aplicando el RDP ya en vigor, que "está comprendida dentro de su ámbito de aplicación una transferencia de datos personales realizada con fines comerciales por un operador económico establecido en un Estado miembro a otro operador económico establecido en un país tercero, a pesar de que, en el transcurso de esa transferencia o tras ella, esos datos puedan ser tratados por las autoridades del país tercero en cuestión con fines de seguridad nacional, defensa y seguridad del Estado". Debe así garantizarse que "los derechos de las personas cuyos datos personales se transfieren a un país tercero sobre la base de cláusulas tipo de protección de datos gozan de un nivel de protección sustancialmente equivalente al garantizado dentro de la Unión Europea por el referido Reglamento, interpretado a la luz de la Carta de los Derechos Fundamentales de la Unión Europea. A tal efecto, la evaluación del nivel de protección garantizado en el contexto de una transferencia de esas características debe, en particular, tomar en consideración tanto las estipulaciones contractuales acordadas entre el responsable o el encargado del tratamiento establecidos en la Unión Europea y el destinatario de la transferencia establecido en el país tercero de que se trate como, por lo que atañe a un eventual acceso de las autoridades públicas de ese país tercero a los datos personales de ese modo transferidos, los elementos pertinentes del sistema jurídico de dicho país". En la medida que las Decisiones de la Comisión que garantizan suficiente o insuficientemente dichos requerimientos de estándar europeo en la transferencia a un país tercero, como EE UU, así resultan unas validadas y otras declaradas inválidas por el TJUE.

BIBLIOGRAFÍA

ANDRIEU, E. (2000) Internet et la protection des données personnelles, *Legicom* 2000, núm. 21-22. Recuperado el 22 de diciembre de 2022 de https://www.cairn.info/revue-legicom-2000-1-page-155.htm

BRUNET E. (2016), Règlement général sur la protection des données à caractère personnel – Genèse de la réforme et présentation globale*, Récueil Dalloz* París. pp. 567 y sigs.

BRUNET, E. (2019), Les mécanismes de coopération des autorités de contrôle au sein de l'Union européenne et le Comité européen de la protection des données, *Revue de Droit International d'Assas* 2019, núm 2, pp. 117- 128. Recuperado el 22 de diciembre de 2022 de https://www.u-paris2. fr/sites/default/files/document/cv_publications/rdia_ndeg2_2019.pdf

CASTETS-RENARD, C. (2016) Invalidation du *Safe Harbor* par la CJUE: tempête sur la protection des données personnelles aux États-Unis, *Recueil Dalloz*. Paris, pp. 88 y sigs.

GAMBARDELLA, S. (2017) La protection des données sensibles à l'ère du numérique: regard sur le droit de l'Union Européenne, en KARLSSON-TALEB A., DE DAVID BEAUREGARD-BERTHIER O. *Protection des données personnelles et sécurité nationale: quelles garanties juridiques dans l'utilisation du numérique*, 1ère édition, Bruylant, Bruselas, pp. 56-134.

GUADAMUZ A. (2000), Habeas Data vs. the European Data Protection Directive, *The Journal of Information, Law and Technology*, Conventry, Reino Unido, Recuperado el 22 de diciembre de 2022 de https://warwick.ac.uk/fac/soc/law/elj/jilt/2000_2/guadamuz/

IUS ET SCIENTIA • 2023
Vol. 9 • Nº 1 • pp. 23-45
ISSN 2444-8478 • https://doi.org/10.12795/IESTSCIENTIA.2023.i01.03

PÉRONNE G. y DAOUD, E. (2017) L'adresse IP est bien une donnée à caractère personnel, *Recueil Dalloz* Paris, pp. 120 y sigs.

PEYROU, S. (2015) La protection des données à caractère personnel: un droit désormais constitutionnalisé et garanti par la CJUE, en *La protection des droits fondamentaux dans l'Union européenne*, dir. R. Tinière et C. Vial, Bruylant, Bruselas.

TAMBOU, O. (2020) *Manuel de droit européen de la protection des données à caractère personnel*, Bruylant, Bruselas.

URIA GAVILAN, E. (2016) Derechos fundamentales *versus* vigilancia masiva Comentario a la sentencia del Tribunal de Justicia (Gran Sala) de 6 de octubre de 2015 en el asunto C-362/14 Schrems, *Revista Electrónica de Estudios Internacionales (REEI)*, Madrid pp. 261-282, Recuperado el 22 de diciembre de 2022 de https://www.cepc.gob.es/sites/default/files/2021-12/37636elisauriagavilanrdce53.pdf

Documentos

La protection des données à caractère personnel dans l'Union européenne: le rôle des autorités nationales chargées de la protection des données Renforcement de l'architecture des droits fondamentaux au sein de l'UE, Edición de 2012. Recuperado el 22 de diciembre de 2022 de https://fra.europa.eu/sites/default/files/tk3109265frc_fr_web.pdf

Manual de legislación europea en materia de protección de datos, Edición de 2018. Recuperado el 22 de diciembre de 2022 de https://fra.europa.eu/sites/default/files/fra_uploads/fra-coe-edps-2018-handbook-data-protection_es.pdf.

IUS ET SCIENTIA • 2023
Vol. 9 • N° 1 • pp. 23-45
ISSN 2444-8478 • https://doi.org/10.12795/IESTSCIENTIA.2023.i01.03