Las decisiones de adecuación en el marco del Reglamento General de Protección de Datos

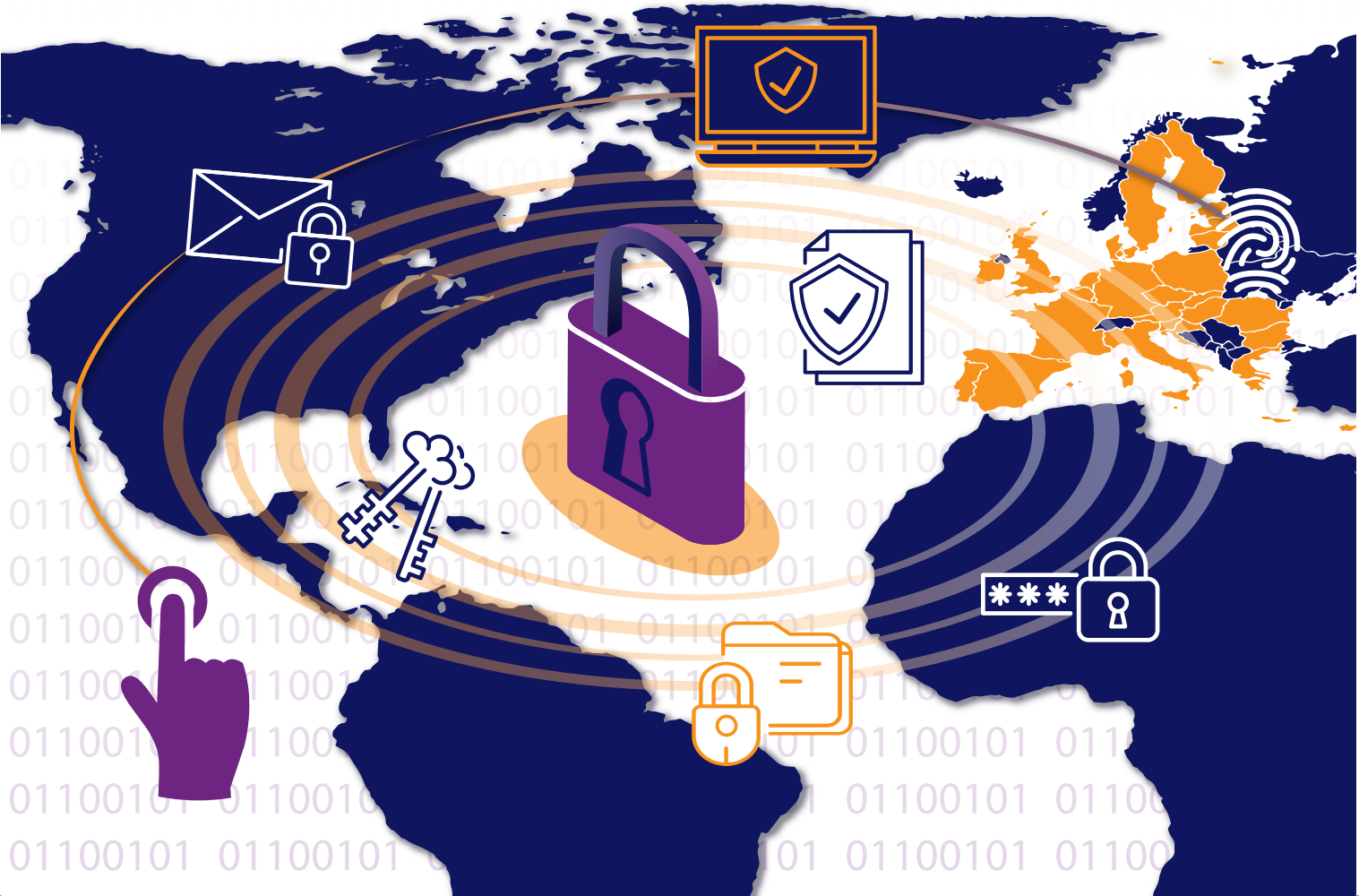
Nuevo régimen europeo de protección de datos personales: la adecuación de tercer país

31

Cuadernos de transparencia

inai
Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales

MAR ESPAÑA MARTÍ



DIRECTORIO

Las decisiones de adecuación en el marco del Reglamento General de Protección de Datos

PLENO DEL INAI

Blanca Lilia Ibarra Cadena
Comisionada Presidenta

Francisco Javier Acuña Llamas
Comisionado

Adrián Alcalá Méndez
Comisionado

Norma Julieta Del Río Venegas
Comisionada

Oscar Mauricio Guerra Ford
Comisionado

Rosendoevgueni Monterrey Chepov
Comisionado

Josefina Román Vergara
Comisionada

Comité editorial

Norma Julieta Del Río Venegas
Rosendoevgueni Monterrey Chepov
Josefina Román Vergara
Guillermo Miguel Cejudo Ramírez
Isabel Davara Fernández de Marcos
Pilar Ferreira García
Lilia María Vélez Iglesias

SECRETARIO TÉCNICO
Cristóbal Robles López

Las opiniones expresadas en esta publicación son responsabilidad exclusiva de los autores y no reflejan necesariamente las del INAI.

Derechos Reservados D.R.
Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales (INAI).
Insurgentes Sur No. 3211, colonia Insurgentes Cuicuilco, Alcaldía Coyoacán, C.P. 04530, Ciudad de México.

Diseño editorial y portada: Martha Rosalba Pérez Cravioto.
Primera edición digital, noviembre de 2021.
ISBN: 978-607-99164-6-6

Ejemplar de descarga gratuita.

31

Cuadernos de transparencia

ÍNDICE

LA AUTORA

MAR ESPAÑA MARTÍ

Es directora de la Agencia Española de Protección de Datos (AEPD) desde julio de 2015. Licenciada en Derecho por la Universidad Pontificia de Comillas, es funcionaria de carrera del Cuerpo Superior de Administraciones Civiles del Estado en la especialidad jurídica desde 1989. Tiene un máster de la Universidad de Alcalá en Protección Internacional de los Derechos Humanos y es experta en gestión en entidades sin ánimo de lucro. A lo largo de su carrera profesional ha trabajado en diferentes instituciones como el Defensor del Pueblo, el Instituto de la Mujer o la Junta de Comunidades de Castilla-La Mancha. Ha participado como profesora en másteres en la Universidad de Alcalá, la Universidad Rey Juan Carlos y el ICADE. También ha sido ponente en diversas jornadas nacionales e internacionales relacionadas con los derechos humanos y las nuevas tecnologías.

Semblanza tomada de la página web de la Agencia Española de Protección de Datos, la autoridad pública independiente que se encarga de velar la privacidad y la protección de datos de la ciudadanía: https://www.aepd.es/es/la-agencia/transparencia/informacion-de-caracter-institucional-organizativa-y-de-planificacion/organigrama-AEPD/la-directora/cv-mar-espana (24 de octubre de 2021).

PRESENTACIÓN

El Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos (INAI) se ha propuesto implementar una política editorial que promueva en la sociedad el conocimiento y el ejercicio de los derechos de nueva generación como es el derecho a la protección de datos personales. A través de los cuadernos de transparencia, el INAI busca tender puentes y crear redes de conocimiento útiles para acercar al gobierno con la sociedad civil, la academia y la sociedad en general con el fin de difundir, analizar, reflexionar y discutir los temas de relevancia que marca la agenda de la democracia moderna.

La generación de textos, como el que ahora nos ocupa, pretende vislumbrar un horizonte posible fuera de las fronteras del país, pero que nos involucra como una nación que sostiene intercambios culturales y económicos a nivel global. El comité editorial del INAI considera importante generar proyectos editoriales donde se analicen las experiencias internacionales relacionadas con la protección de datos personales, particularmente con la adecuación a la normativa que ha creado la Unión Europea en este derecho con el propósito de impulsar las mejores prácticas en la adecuación de dicha regulación.

En este ensayo, escrito por Mar España, directora de la Agencia Española de Protección de Datos, se resaltan los cambios en la normativa para la adecuación de tercer país al régimen europeo de protección de datos, desde la Directiva 95/46 al Reglamento General de Protección de Datos, y se refleja la evolución de las distintas disposiciones y criterios de adecuación en la Unión Europea.

Durante la 43 Asamblea Global para la Privacidad 2021 celebrada en octubre —de la cual México fue el país anfitrión— el Instituto Nacional de Acceso

a la Información (INAI) asumió la presidencia de la Asamblea Global de Privacidad (GPA) durante la cual refrendó su compromiso con la protección de datos personales y la privacidad a nivel internacional. Con su nuevo cargo, el INAI hizo un llamado a más de 130 autoridades de protección de datos de 80 países que integran este organismo para formar una alianza en defensa de las personas y, de este modo, otorgarles el poder necesario para hacer frente a los desafíos globales.

El tema del Cuaderno de Transparencia 31 está inserto en la discusión actual que se vincula directamente con los trabajos de dicha asamblea y con la creación de un marco normativo robusto, dinámico y compatible con los mejores estándares internacionales en favor de la protección y garantía de los derechos humanos. El estudio del concepto de adecuación del Reglamento General de Protección de Datos, las decisiones de la Comisión y directrices del Grupo de Trabajo del Artículo 29 o GT29 (ahora Comité Europeo de Protección de Datos) son de gran importancia para nuestro país, así como para el reconocimiento de los esfuerzos realizados por el INAI para la tutela efectiva del derecho humano a la protección de datos personales.

Este ensayo trata sobre las consideraciones, retos y desafíos para emitir una declaración de adecuación a un país tercero en el marco de la agenda de privacidad y protección de datos personales, lo cual se traduce en beneficios para las economías de las naciones que obtienen una determinación favorable, ya que tendrán la posibilidad de agilizar las transacciones que implican el tratamiento de datos personales; pero siempre poniendo en el centro a la persona, lo que implica hacer efectivas las medidas necesarias para proteger la privacidad, así como el uso apropiado y proporcional de sus datos.

El marco normativo europeo prevé que los datos solamente pueden ser transferidos desde la Unión Europea (UE) a un tercer país cuando existe la garantía suficiente de que los datos

van a ser protegidos con estándares equivalentes a los que se garantiza en los países miembros. Este texto permitirá al lector entender cómo está prevista en la normatividad de la comunidad europea la figura de "adecuación" y cómo debe procesarse.

La transferencia de datos personales es un tema presente en la agenda actual de varios gobiernos y su interés se ha acrecentado debido a la pandemia por covid-19 y sus implicaciones, como la adopción de nuevos servicios, la aceleración de los procesos de innovación e integración tecnológica y el intercambio de datos para la resolución de problemas. En ese sentido, el análisis de la normativa, sus procedimientos y prácticas en otros países —en este caso de la Unión Europea— es relevante porque puede impulsar mejoras y discusiones sobre los marcos y procedimientos nacionales.

Debido al aumento de la digitalización en los procesos de producción, la transferencia de datos entre Estados ha ido en aumento y es necesario que se establezcan medidas para garantizar la protección de la privacidad de las personas, por lo que se analizará el caso de la Unión Europea. Por eso, en el INAI consideramos que es de gran interés para las personas involucradas en la materia de datos personales, como legisladores, personal de órganos garantes y empresarios; pero también puede resultar atractivo para el público en general que desee acercarse a los temas relacionados con el establecimiento de estándares nacionales e internacionales en materia de protección de datos personales.

Comité editorial del INAI

1. INTRODUCCIÓN

EN 1995, LA UNIÓN EUROPEA ADOPTÓ LA DIRECTIVA DE PROTECCIÓN DE DATOS –CONOCIDA COMO LA DIRECTIVA 95/46/CE–, LA CUAL REGULABA EL PROCESAMIENTO DE DATOS PERSONALES DENTRO DE LA UNIÓN. LA NECESIDAD DE ADECUAR EL NIVEL DE PROTECCIÓN DE DATOS PERSONALES EN TRANSFERENCIAS INTERNACIONALES FUE UNA SOLUCIÓN TÍPICAMENTE EUROPEA, QUE YA SE ENCONTRABA EN ESTA DIRECTIVA.

Para entender el papel de las declaraciones de nivel adecuado de protección y de otros instrumentos de transferencia, de acuerdo con el derecho europeo, es preciso establecer que los datos solamente pueden ser transferidos desde la Unión Europea (UE) a un tercer país cuando existe la garantía suficiente de que los datos van a ser respetados.

Desde esa perspectiva, una declaración de adecuación supone reconocer que en otros países los datos personales tendrán una protección similar a la que reciben en la Unión Europea, por tanto, puede establecerse una libre circulación de datos desde cualquier Estado miembro de la Unión hacia otro país de forma paralela a como ocurriría con las transferencias de datos que se producen dentro de la UE.

Para alcanzar el reconocimiento de un nivel de protección equiparable al de la UE, es necesario que se valore a fondo la legislación del país solicitante y su aplicación.

Lo que se entiende como nivel adecuado de protección, los aspectos a considerar y el alcance de las propias decisiones de adecuación han evolucionado desde la regulación contenida en la antigua Directiva de Protección de Datos. Esta evolución fue consecuencia de las disposiciones del Reglamento General de Protección de Datos (RGPD) y de los criterios establecidos en la jurisprudencia del Tribunal de Justicia de la Unión Europea (TJUE).

Las decisiones de adecuación en el marco del Reglamento General de Protección de Datos

2. LAS DECISIONES DE ADECUACIÓN EN LA DIRECTIVA 95/46/CE

ESTE ENSAYO NO PRETENDE HACER UN ANÁLISIS HISTÓRICO DE LA FIGURA DE LA ADECUACIÓN. SIN EMBARGO, RESULTA INTERESANTE EXPLICAR SUS ORÍGENES EN LA YA SUPERADA DIRECTIVA, AUNQUE SEA DE FORMA MUY RESUMIDA, PARA LOGRAR UNA MEJOR PERCEPCIÓN DE LOS CAMBIOS PRODUCIDOS DESDE ENTONCES Y SU SIGNIFICADO.

En la Directiva, la declaración de adecuación se presentaba, al menos formalmente, como la única opción posible para realizar transferencias de datos a un país tercero.[1] La posibilidad de utilizar instrumentos para ofrecer garantías por parte de los exportadores se plantea como una opción sin perjuicio de la regla general de transferencia solo cuando existe una declaración de adecuación[2] y, de hecho, está regulada en un artículo distinto, encabezado por el título "Excepciones". Pese a ello, lo cierto es que el número de declaraciones de adecuación adoptadas sobre la base de la Directiva no fue particularmente elevado. No obstante, los otros instrumentos, que en principio se planteaban como excepciones son los que se han utilizado con mayor frecuencia y regularidad.

La posibilidad de declarar la existencia de un nivel adecuado de protección no estaba reservada en exclusiva a la Comisión, tal y como se desprende de la redacción de los apartados que tratan este tema. De hecho, algunas legislaciones —como sucedía con la ya derogada Ley de Protección de Datos española de 1999— contemplaban expresamente la posibilidad de que fuera la propia autoridad de protección de datos la que determinara la existencia de protección adecuada en el país de destino.[3] Aunque en la práctica fueron las decisiones de la Comisión en este ámbito las que se impusieron en la medida en que, siguiendo en este punto lo previsto por la Directiva, solo las declaraciones de adecuación vinculadas a través de una decisión de la Co-

misión podrían tener efecto en todos los Estados miembro de la Unión.[4]

Es también importante destacar que en la Directiva los criterios para concluir la existencia de un nivel adecuado de protección en un tercer país estaban esbozados de una forma bastante genérica, por referencia a la legislación interna, o a los compromisos internacionales suscritos por el país en cuestión, a los efectos de la protección de la vida privada o de los derechos fundamentales de las personas, aunque también es cierto que, en otro apartado del mismo artículo, se alude a las normas profesionales y las medidas de seguridad en vigor en dichos países.

Esta relativa parquedad de la Directiva, no solo en lo relativo a las decisiones de adecuación, sino, en general a todos los instrumentos para transferencias internacionales de datos personales, motivó la adopción por el ya extinto Grupo de Trabajo del Artículo 29 (GT29) de un documento de trabajo[5] en el que se identificaban algunos principios y contenidos de protección de datos, así como los requisitos procedimentales o de supervisión del cumplimiento, que se suponen condiciones mínimas para considerar el nivel de protección adecuado.

A continuación, haré dos últimos apuntes en relación con el contenido de la Directiva en este ámbito. El primero es que no se establecen los procedimientos concretos para la adopción de las decisiones de adecuación atribuidas a la Comisión,[6] es decir, no se hace alusión a cómo debe iniciarse el procedimiento, su duración o sus fases. Tampoco explicita la obligación de revisar regularmente estas decisiones de adecuación para comprobar si se siguen cumpliendo las condiciones.

El segundo es que la Directiva siempre habla de adecuación de terceros países. No se contempla formalmente la posibilidad de que la decisión afecte a un territorio o sector dentro de un país. Sin embargo, como ha sucedido con otros aspectos de las decisiones de adecuación, en la práctica sí se han registrado decisiones parciales. Por ejemplo, en el caso de Canadá, que tiene una decisión de adecuación desde 2002,[7] la declaración se limita al ámbito cubierto por la ley canadiense de protección de datos aplicable a entidades privadas (la Personal Information and Electronic Documents Act), mientras que no se extiende a las entidades públicas, que están sujetas a distinta norma de privacidad. En el mismo sentido, la

adecuación de Israel[8] alcanza solo a los tratamientos automatizados de datos, quedando excluidos los tratamientos manuales, dado que también quedan fuera de la aplicación de la normativa israelí que se consideró que ofrecía un nivel adecuado de protección.

Un ejemplo muy claro de decisión de adecuación sectorial es la que involucra las dos relativas a las transferencias a EEUU. La primera declaraba la adecuación del esquema conocido como "Puerto Seguro",[9] como su sucesora, de adecuación del "Escudo de Privacidad"[10] establecen que el nivel adecuado de protección se entiende referido a una serie de principios respecto de los cuales deben autocertificarse las empresas que se adhieren al esquema. En ambos casos, la declaración de adecuación tiene un alcance que podría considerarse sectorial y que afecta solo al sector de empresas adheridas a estos esquemas.

Las decisiones de adecuación en el marco del Reglamento General de Protección de Datos

3. EL NIVEL ADECUADO DE PROTECCIÓN EN EL RGPD

EL ENFOQUE DEL REGLAMENTO GENERAL DE PROTECCIÓN DE DATOS (RGPD) RESPECTO A LA ADECUACIÓN ES, EN LO FUNDAMENTAL, UNA CONTINUACIÓN DEL QUE MARCABA POR LA DIRECTIVA 95/46/CE, PERO, AL MISMO TIEMPO, PRESENTA ALGUNAS DIFERENCIAS SIGNIFICATIVAS.

La primera de ellas es que en el RGPD la declaración de la existencia de un nivel adecuado de protección no se presenta, al menos en términos sistemáticos, como la opción de elección para realizar transferencias internacionales.

En efecto, el artículo 44 del RGPD establece que solo podrán realizarse transferencias a un tercer país si se cumplen las condiciones previstas en el capítulo que este artículo encabeza (que es el relativo a las transferencias internacionales), añadiendo que, en todo caso, todas las disposiciones del capítulo se aplicarán a fin de asegurar que el nivel de protección de las personas físicas que el RGPD garantiza no se verá menoscabado por la transferencia.

Dicho en otros términos, de este artículo puede concluirse que el RGPD sitúa en pie de igualdad todos los instrumentos de transferencia, siempre que se den las condiciones para la utilización de cada uno de ellos, y, lo que quizás es más importante, exige que cualquiera de esos instrumentos asegure el nivel de protección garantizado por él.

No obstante, las decisiones de adecuación —por sus características particulares— siguen ocupando un lugar diferenciado dentro de los instrumentos de transferencia internacional. Por ejemplo, la Comisión, en su comunicación "Intercambio y protección de los datos personales en un mundo globalizado", hace notar que las decisiones de adecuación conllevan el establecimiento de un diálogo específico y de una estrecha cooperación con el tercer país interesado. Igualmente, subraya que las decisiones de adecuación son "la mejor manera de fomentar la confianza mu-

tua y garantizar la libre circulación de datos personales, favoreciendo así los intercambios comerciales que conllevan transferencias de datos personales al tercer país interesado".[11]

Por lo que hace a la regulación de las decisiones de adecuación, una primera novedad que presenta el Reglamento es que la declaración puede afectar a un país, a un territorio o a un sector específico dentro de ese país o a una organización internacional. El RGPD consagra formalmente lo que, como se ha indicado más arriba, ya venía sucediendo en la práctica, dotando a las decisiones de adecuación de una mayor flexibilidad.

Una novedad que, paradójicamente, no se encuentra en la parte dispositiva del RGPD, sino que hay que buscar en su considerando 104, es la determinación de lo que puede entenderse por nivel adecuado de protección.

CIUDADANOS EN TODO EL MUNDO ESTÁN CADA VEZ MÁS PREOCUPADOS POR SU PRIVACIDAD, COMO CONSECUENCIA DEL IMPACTO DE LAS NUEVAS TECNOLOGÍAS Y SU USO INTENSIVO DE DATOS PERSONALES.

Este concepto no estaba claramente definido en la anterior Directiva y, como se ha dicho, los criterios para la valoración del nivel de protección en el país de destino se apoyaban en buena medida en los principios y requisitos identificados por el GT29. En todo caso, lo cierto es que la noción de nivel adecuado, si buscamos los sinónimos en castellano de este adjetivo, tendería a asociarse con la existencia de un nivel apropiado, conveniente o suficiente. Se pensaría, por lo tanto, que para la Directiva no pareció necesario que ese nivel fuera equiparable de alguna forma al que los datos reciben en la Unión. Bastaría con que fuera "adecuado", lo que incluiría esos principios y requisitos que el GT29 recogía en su documento de trabajo, pero no en todos los casos otros contenidos de la propia Directiva que sí contribuirían a definir el nivel de protección otorgado a los datos dentro de la Unión.

El Tribunal de Justicia de la UE hizo una interpretación más exigente del concepto en su sentencia en el caso C362/14, conocida como Sentencia Schrems.[12] En ella, el Tribunal declaró inválida la decisión de la Comisión por la que se declaraba el nivel de protección adecuado del esquema de Puerto Seguro. Para llegar a esa conclusión, el Tribunal partió de que la noción de "nivel adecuado de protección" implicaba que el país que demanda la adecuación debe ofrecer una protección de las libertades y los derechos fundamentales "sustancialmente equivalente" a la que garantizaba en aquel momento la Directiva 95/46/CE. El Tribunal recono-

ció explícitamente que los medios de los que se sirviera el país en cuestión para conseguir el objetivo de protección no tienen que ser idénticos a los empleados en la Unión Europea. Sin embargo, esos medios deben resultar eficaces para alcanzar un nivel de protección "sustancialmente equivalente" al europeo. El Tribunal ha reiterado esta interpretación muy recientemente, en la Sentencia Schrems II, que declara inválida la decisión por la que se declara el nivel adecuado de protección del esquema de Puerto Seguro.

Como se ha indicado, el RGPD no emplea la expresión "nivel sustancialmente equivalente de protección" en ninguna de las disposiciones sobre instrumentos de transferencia y, en particular, en las que tratan las decisiones de adecuación, pero sí lo hace en el considerando 104, donde se afirma que "el tercer país debe ofrecer garantías que aseguren un nivel adecuado de protección equivalente en lo esencial al ofrecido en la Unión, (…)". Sin embargo, no cabe ignorar que la exigencia del artículo 44 sobre la necesidad de que los instrumentos de transferencia contenidos en el correspondiente capítulo del RGPD certifiquen que el nivel de protección garantizado por el Reglamento no se vea menoscabado apunta en la misma dirección que los términos "nivel de protección sustancialmente equivalente" acuñados por el TJUE.

El Reglamento introduce también novedades respecto a los criterios de valoración para establecer la existencia de "nivel adecuado de protección", ampliando y detallando las previsiones que al respecto contenía la Directiva. Estas novedades se encuentran, principalmente, en lo relativo a las características del ordenamiento en el país de destino y al papel de la autoridad de supervisión.

El Reglamento va más allá de las referencias genéricas de la Directiva a la legislación interna y a las normas profesionales o medidas de seguridad en vigor e incluye entre los elementos que deben ser considerados "el Estado de Derecho, el respeto de los derechos humanos y las libertades fundamentales, la legislación pertinente, tanto general como sectorial, incluida la relativa a la seguridad pública, la defensa, la seguridad nacional y la legislación penal", o las normas sobre transferencias ulteriores de datos a otro tercer país u organización internacional.[13] Se añade, además, la necesidad de evaluar el reconocimiento a los interesados

cuyos datos se transfieren de derechos efectivos, exigibles y de vías de recurso administrativas o judiciales efectivas.

Esta consideración especial merece que en el mismo apartado se aluda al acceso de las autoridades públicas a los datos personales,[14] así como a la aplicación en la práctica de la legislación que se considera. Estas dos referencias no estaban incluidas en la propuesta inicial de la Comisión, pero se introdujeron posteriormente durante el procedimiento legislativo, en lo que podría considerarse un reflejo de la doctrina del TJUE en la Sentencia Schrems, donde las condiciones en que se producía el acceso de las autoridades norteamericanas a los datos transferidos fueron uno de los motivos en que se basó la anulación de la decisión de adecuación.[15]

EL RGPD ESTABLECE EXPRESAMENTE NO SOLO QUE DEBEN VALORARSE LA EXISTENCIA Y FUNCIONAMIENTO EFECTIVO DE UNA O VARIAS AUTORIDADES DE CONTROL INDEPENDIENTES, SINO TAMBIÉN QUE ESAS AUTORIDADES DEBEN DISPONER DE PODERES DE EJECUCIÓN ADECUADOS, ASÍ COMO PODERES PARA ASESORAR A LOS INTERESADOS Y COOPERAR CON LAS AUTORIDADES DE CONTROL DE LA UE Y DE LOS ESTADOS MIEMBROS

En lo tocante a la consideración del papel de autoridades de supervisión independientes, la novedad estriba, justamente, en su inclusión como requisito a valorar de cara a la decisión sobre la adecuación. En la Directiva no existía una previsión homóloga, ni tampoco se contenía en el Documento de Trabajo del GT29 que se ha citado anteriormente. De hecho, en éste se reconocía que estas autoridades no son (no eran en el momento en que se adoptó el documento) frecuentes fuera del entorno europeo y que, por ello, a los efectos de establecer la adecuación de la protección ofrecida sería necesario identificar los objetivos que persigue el marco institucional de protección de datos y comprobar si esos objetivos se consiguen a través de la variedad de los mecanismos judiciales o no judiciales empleados en los países terceros. En suma, el GT29 abogaba por un análisis material de la eficacia de los mecanismos de supervisión, sin exigir necesariamente que esos mecanismos incluyeran una autoridad de protección de datos independiente específicamente configurada como tal. Ese análisis, de acuerdo con el grupo de trabajo, debería centrarse en que los mecanismos proporcionaran un buen nivel de cumplimiento normativo, que ofrecieran apoyo a las personas en el ejercicio de sus derechos y vías de reacción apropiadas en caso de no cumplimiento.

Pese a ello, la existencia de una autoridad con un suficiente grado de autonomía o independencia, no necesariamente equiparable al exigido a las autoridades europeas, se ha ido consolidando en la práctica como uno de los requi-

sitos a tomar en consideración en los países candidatos a la adecuación.[16]

El Reglamento ha disipado cualquier duda al respecto, al establecer expresamente no solo que deben valorarse la existencia y funcionamiento efectivo de una o varias autoridades de control independientes, sino también que esas autoridades deben disponer de poderes de ejecución adecuados, así como poderes para asesorar a los interesados y cooperar con las autoridades de control de la Unión y de los Estados miembros. Lo previsto en la parte dispositiva del Reglamento se ve reforzado por el ya citado considerando 104, donde se señala que el tercer país debe garantizar "que haya un control verdaderamente independiente de la protección de datos y establecer mecanismos de cooperación con las autoridades de protección de datos de los Estados miembro".

Las consecuencias de esta especial atención que el Reglamento presta a la supervisión del cumplimiento de la normativa en el país tercero que aspira a la adecuación pueden observarse en la única decisión que hasta el momento se ha adoptado estando ya en aplicación el RGPD. Se trata de la decisión relativa a la adecuación de Japón, que dedica toda una sección de su introducción a la supervisión y control de la aplicación de la normativa y analiza en varios de sus considerandos la posición, funciones y poderes de la autoridad de supervisión de Japón.[17]

No obstante, el apartado tres del artículo 45 contiene una redacción que permitiría concluir que ese "control verdaderamente independiente" del que habla el considerando 104 podría adoptar formas no del todo idénticas a las de las autoridades de supervisión tal y como se entienden en Europa. En efecto, ese apartado señala que la decisión de ejecución de la Comisión especificará el ámbito territorial o sectorial de aplicación de la decisión y en su caso determinará la autoridad o autoridades de control a que se refiere el Reglamento. La interpretación literal de esta frase induce a pensar que puede haber casos en que no se determine en la decisión de adecuación cuál es la autoridad de supervisión, y la única forma de hacer compatible esa interpretación con la exigencia de un control independiente de supervisión es entender que esa exigencia se puede ver satisfecha también por formas menos concentradas o más difusas de control siempre que se garanticen los

requisitos de independencia y poderes ejecutivos adecuados.

El tercero de los aspectos que a tenor del RGPD deben considerarse al evaluar el nivel de protección existente en el país de destino es el de los compromisos internacionales asumidos por ese tercer país. Aunque esta referencia sí se encontraba en la Directiva, el tratamiento que hace de ella el RGPD es más amplio, dado que añade la participación en sistemas multilaterales o regionales, en particular los que tengan relación con la protección de datos. El Reglamento menciona específicamente en su considerando 105 un ejemplo de este tipo de marcos multilaterales, citando la adhesión al Convenio del Consejo de Europa de 1981.

El GT29 actualizó su documento de trabajo de 1998 sobre transferencias internacionales mediante varios títulos, uno de los cuales está dedicado a la determinación del nivel adecuado de protección y profundiza en la interpretación que debe darse a algunos de los elementos contenidos en el RGPD.[18]

En este documento, el grupo de trabajo señala que, a la luz de las previsiones del Reglamento, la valoración del nivel de protección debe tener tanto en cuenta el contenido de la legislación que puede afectar al modo en que se procesan los datos en el país candidato como los medios para garantizar su aplicación. En ese sentido, ambos elementos deben reunir unos requisitos mínimos que se derivarían de la Carta Europea de Derechos Fundamentales y del RGPD, dado que el objetivo es que el nivel de protección sea "esencialmente equivalente" al ofrecido en la Unión Europea.

El GT29 identifica los siguientes contenidos de la legislación aplicable, que reproducen, en buena medida, el núcleo de los principios y derechos de los interesados establecidos en el RGPD:

- Conceptos. En el país candidato deben existir conceptos o principios básicos en materia de protección de datos. No tienen que ser idénticos a los empleados por el RGPD, pero sí deben reflejarlos y ser consistentes con ellos.
- Fundamentos del tratamiento lícito y leal para fines legítimos. Deben establecerse de forma clara las bases que permiten legitimar el tratamiento de datos personales.
- Principio de limitación de finalidad.
- Principio de calidad de los datos y proporcionalidad.
- Principio de retención de datos por

periodos no superiores a lo necesario para los fines para los que los datos son tratados.
- Principio de seguridad y confidencialidad.
- Principio de transparencia.
- Derecho de acceso, rectificación, supresión y oposición.
- Restricción de transferencias ulteriores. Aunque este no es realmente un principio o derecho, es un aspecto esencial en la declaración de la adecuación. El Reglamento exige que los datos sean transferidos solo cuando se pueda asegurar la continuidad en la protección de que disfrutan en la UE. Si posteriormente los datos son enviados desde el país de destino a otro que no ofrece las garantías suficientes, se desvirtúa ese objetivo de protección. Por lo tanto, las transferencias ulteriores solo deberían producirse para fines específicos, con la suficiente base jurídica y en la medida en que se ofrezcan garantías de que se mantiene un nivel de protección adecuado en el tercer país.

Junto a estos principios básicos, el GT29 enumera, a modo de ejemplos, y repitiendo lo que ya se incluía en el Documento de Trabajo WP12, otros contenidos adicionales que deberían encontrarse en la normativa aplicable en el país de destino. Entre ellos se encuentran la existencia de salvaguardas específicas similares a las previstas por el RGPD cuando se traten datos de los considerados "sensibles",[19] la existencia de un derecho de oposición para los tratamientos con fines de mercadotecnia directa o la limitación de los supuestos en que pueden adoptarse decisiones basadas únicamente en el tratamiento automatizado de los datos que produzcan efectos legales o que afecten de forma significativa a los interesados.

Estos elementos se citan tan solo como ejemplos, por lo que no se excluye que otros aspectos no mencionados específicamente pudieran tener que ser objeto de evaluación, en particular si por su configuración en la legislación del país de destino pueden influir en el nivel de protección que se garantiza.

Como se ha indicado, las Referencias destacan la necesidad de valorar tanto los contenidos de la legislación aplicable como los medios para garantizar su eficaz aplicación. Por ello, se incluye en ellas un apartado dedicado a los mecanismos relativos al procedimiento e implementación de las normas.

Este apartado sí que presenta diferencias significativas con el correspondiente en el documento de trabajo WP12. Por una parte, se añade una referencia específica a la existencia de autoridades de control independientes, en línea con la ya comentada introducción de este requisito en el RGPD. Se mantienen, ampliados, los puntos relativos a la necesidad de que el sistema garantice un nivel de cumplimiento suficiente de la normativa, con una mención expresa al papel que en este sentido pueden jugar las sanciones y los sistemas de verificación directa por parte de las autoridades, así como un apartado sobre el apoyo a los interesados en el ejercicio de sus derechos y la existencia de mecanismos de reclamación e indemnización adecuados.

NO SE TRATA DE QUE LA LEGISLACIÓN DEL PAÍS TERCERO DEBA REPRODUCIR MIMÉTICAMENTE EL REGLAMENTO EUROPEO, SINO MÁS BIEN DE QUE SU SISTEMA EN CONJUNTO ESTÉ ORIENTADO A LA APROXIMACIÓN PROACTIVA PROPIA DE LA *ACCOUNTABILITY*

A los anteriores se añade un apartado que refleja también muy directamente el enfoque del RGPD. Se trata de la necesidad de que el marco de protección de datos en el tercer país incluya obligaciones de responsabilidad activa para quienes tratan los datos personales. Aunque las Referencias citan como ejemplo algunas de las medidas de cumplimiento previstas por el RGPD. Conviene aclarar, una vez más, que no se trata de que la legislación del país tercero deba reproducir miméticamente el Reglamento europeo, sino más bien de que su sistema en conjunto esté orientado a la aproximación proactiva propia de la *accountability*[20] y de que esa orientación no se quede en un plano meramente declarativo, sino que se traduzca en un conjunto de obligaciones adecuadas y se lleven a la práctica.

Las Referencias incluyen un nuevo capítulo, que no está presente en el documento de trabajo de 1998, sobre las garantías esenciales en países terceros para el acceso a los datos por parte de los servicios de seguridad e inteligencia con el fin de limitar las injerencias en los derechos fundamentales.

Como ya se ha mencionado, la Sentencia Schrems invalidó la decisión de Puerto Seguro precisamente porque el TJUE consideró que no contenía ninguna constancia de que existieran en EEUU reglas destinadas a limitar las injerencias de las autoridades de ese país en los derechos fundamentales de las personas, cuyos datos se transfieren con fines, en principio, legítimos, como la seguridad nacional.

La posición del Tribunal se basa en la Carta Europea de Derechos Fundamentales, que permite limitaciones en el ejercicio de los derechos y libertades

que reconoce solo si son necesarias y proporcionadas para alcanzar objetivos de interés general reconocidos por el derecho de la Unión.[21]

A partir de esta previsión, debe entenderse que será posible la injerencia que supone el acceso de autoridades policiales o de seguridad nacional en el país tercero a los datos transferidos siempre que ese acceso se produzca en unas condiciones compatibles con los criterios fijados por la Carta, una situación que el TJUE entendía que no se daba en el caso de EEUU en el marco de la aplicación del esquema de Puerto Seguro.

La importancia de este análisis del Tribunal se refleja en el RGPD, donde, como se ha señalado, hay una mención expresa de que esta cuestión debe ser tenida en cuenta en la evaluación de la adecuación y también en las Referencias del GT29, que le dedican un capítulo.

En ese capítulo, el GT29 se remite a su dictamen en el grupo de trabajo 237 (WP237)[22] y señala que en cualquier caso los países terceros o receptores tienen que respetar cuatro garantías esenciales a la hora de regular el acceso a los datos transferidos tanto para fines de seguridad nacional como policiales. Estas cuatro garantías, que el grupo de trabajo desarrolló a partir de lo dispuesto en la Carta como de la jurisprudencia de los tribunales europeos, son las siguientes:

1. El tratamiento que supone el acceso y utilización de los datos debe basarse en normas claras, precisas y accesibles (base jurídica).
2. Se deben demostrar la necesidad y la proporcionalidad respecto a los objetivos legítimos perseguidos.
3. El tratamiento debe estar sujeto a una supervisión independiente.
4. Las personas deben disponer de vías de acción efectivas con fines de seguridad nacional.

Las Referencias del GT29, refrendadas por el Comité Europeo, tienen una gran importancia en el contexto de los procesos de adecuación. Por una parte, porque contribuyen a precisar la interpretación que puede darse a algunos de los elementos que, según el RGPD, deben considerarse a la hora de determinar la adecuación de un país tercero. Por otra, porque son la guía que sigue el propio Comité a la hora de preparar sus dictámenes a la Comisión sobre nivel de adecuación en países terceros.[23]

4. PROCEDIMIENTO PARA LA DECLARACIÓN DE ADECUACIÓN EN EL RGPD

EL REGLAMENTO DESCRIBE EL PROCESO DE ADOPCIÓN DE UNA DECISIÓN DE ADECUACIÓN CON ALGO MÁS DE PRECISIÓN QUE LA DIRECTIVA 95/46/CE.

En primer lugar, el Reglamento establece claramente que las declaraciones de adecuación corresponden exclusivamente a la Comisión Europea. Por otro lado, y en esto sigue la misma pauta que la Directiva, remite el procedimiento de adopción de la decisión a lo previsto en el Reglamento 182/2011, que establece las modalidades de control por parte de los Estados miembro en el ejercicio de competencias de ejecución por parte de la Comisión.[24]

En síntesis, el Reglamento establece la necesidad de que la Comisión someta a un comité compuesto por representantes de los Estados miembro las propuestas de actos de ejecución para que sigan un procedimiento de consulta o un examen (dependiendo de la materia sobre la que verse el acto de ejecución). Existen numerosos comités para los distintos ámbitos de actuación de la Unión Europea. En el marco del procedimiento de examen, que sería el que se aplica a las propuestas de decisión de adecuación, estos comités pueden emitir dictámenes favorables, desfavorables o no emitirlos. El Reglamento 182/2011 también establece las consecuencias y opciones para la Comisión, en caso de que no se realice un dictamen o sea desfavorable. En definitiva, este procedimiento supone que los Estados miembros tienen una intervención directa en el proceso de adopción de las decisiones de adecuación.

Lo mismo sucede con el Comité Europeo de Protección de Datos (CEPD). Su participación no está prevista en el artículo dedicado a las decisiones de adecuación, sino en el artículo 70, donde se enumeran las funciones del Comité. En este artículo se establece que el CEPD facilitará a la Comisión un dictamen para evaluar la adecuación

del nivel de protección en un tercer país. Este dictamen se proporcionará para determinar la existencia de nivel adecuado y para constatar que un país ha dejado de ofrecer ese nivel de protección. Aunque el artículo 70 tan solo dispone que el Comité "facilitará" el dictamen, sin pronunciarse sobre el carácter preceptivo o no de solicitarlo, el considerando 105 del Reglamento es taxativo. Es decir que no admite discusión o réplica, al establecer que "la Comisión debe consultar al Comité al evaluar el nivel de protección existente en terceros países u organizaciones internacionales".

El Reglamento, como ya ocurría en la Directiva, no indica cómo se debe iniciar el proceso de adecuación. Sin embargo, en la práctica existieron varias opciones posibles. Lo más habitual era que el país interesado en obtener la adecuación se dirigiera a la Comisión para manifestar su interés y, de esta forma iniciar el proceso.

Sin embargo, puede haber otras posibilidades. Por ejemplo, el Reglamento General de Protección de Datos (RGPD) en su comunicado "Intercambio y protección de datos personales en un mundo globalizado", la Comisión parece inclinarse por una gestión más activa de los procesos de adecuación y señala una serie de prioridades para "determinar los terceros países con los que conviene entablar un diálogo sobre la adecuación".[25] Esas prioridades se basan en criterios como el alcance de las relaciones comerciales presentes o posibles entre el país en cuestión y la UE, la magnitud de los flujos de los datos personales con origen en la UE —que reflejaría la existencia de relaciones más intensas con el país tercero— o el hecho de que un país tercero sea pionero en materia de protección de datos en su región y pueda servir como modelo.

No obstante, la Comisión también señala que acogerá favorablemente las manifestaciones de interés de otros países que busquen la cooperación en la materia, aceptando así implícitamente la pervivencia del enfoque más tradicional en el que es el país interesado el que toma la iniciativa para conseguir la adecuación.

El Reglamento no formaliza el proceso de adecuación como tal, más allá de prever las intervenciones del CEPD y del comité de representantes de los Estados miembros. A grandes rasgos, este proceso incluye los informes previos sobre la situación en el país tercero

candidato que la Comisión realiza por sí misma o encomienda a entidades especializadas, el dictamen del Comité Europeo de Protección de Datos sobre la propuesta de decisión, el dictamen del comité de representantes de los Estados miembros y la adopción de la decisión por el colegio de comisarios.

Dependiendo de las condiciones existentes en el país solicitante, a lo largo de todo el proceso se producen también negociaciones con la Comisión para que haga las modificaciones necesarias con el objetivo de resolver aspectos que pudieran resultar negativos a la hora de garantizar el nivel de protección exigido.

Si la legislación en el país solicitante presenta contenidos y mecanismos de aplicación "sustancialmente equivalentes" a los de la UE, estas negociaciones pueden reducirse al mínimo. Esto puede suceder —y de hecho ha sucedido en el pasado— cuando el país interesado ha adoptado normas de protección de datos o ha modificado la legislación existente que se aplicó con antelación o en los primeros pasos del proceso de determinación de la adecuación.

En otros casos, las negociaciones pueden ser más extensas y complejas, pudiendo llegar hasta las últimas etapas del proceso de adopción de la decisión final.[26]

Estas negociaciones de la Comisión con el país tercero estaban ya expuestas en la Directiva de 1995 y se han replicado en el RGPD, aunque en ambos textos esta intervención parece limitarse a los casos en que a un país tercero se le ha retirado la adecuación por haber dejado de garantizar un nivel de protección adecuado.

Efectivamente, el Reglamento prevé que cuando la información disponible indique que ya no se proporciona el nivel de protección adecuado, la Comisión procederá según corresponda al caso a derogar, suspender o modificar su decisión de adecuación. Estas medidas requieren también los dictámenes del CEPD y del comité de representantes de los Estados miembros.

El Reglamento también prevé expresamente, igual que la Directiva, que esa decisión negativa debe ir seguida (el RGPD emplea el verbo "establecerá") de consultas con el país afectado con vistas a remediar la situación que dio lugar a la retirada o modificación de la declaración de adecuación.

En el pasado esa previsión se ha aplicado, por extensión, a los casos en que las carencias en el marco normativo

del tercer país se constataban en el propio proceso de declaración de adecuación. En la actualidad, esa interpretación sigue vigente, como demuestra el ejemplo de Japón.

La última novedad de cierto alcance que presenta el Reglamento en esta materia es la previsión de que toda decisión de adecuación incluya un mecanismo de revisión periódica de al menos cada cuatro años, de la propia decisión, de forma que se puedan tener en cuenta cambios en las condiciones del país tercero. Esta obligación debe entenderse como un mínimo que, dependiendo de cada caso, puede reforzarse para establecer revisiones más frecuentes en casos concretos. Así sucedió en el caso del Escudo de Privacidad, donde se preveían revisiones anuales o, más recientemente, en el de Japón, en el que la primera revisión tendrá lugar en los próximos meses, a los dos años de entrada en vigor de la decisión. La Comisión y el comité de representantes de los Estados miembros valorará a la luz de sus resultados si se mantiene la periodicidad bianual para futuras revisiones o si se aplica el plazo previsto por el RGPD.

5. PERSPECTIVAS FUTURAS DE LA ADECUACIÓN

EL REGLAMENTO GENERAL DE PROTECCIÓN DE DATOS HA AMPLIADO EL CATÁLOGO DE INSTRUMENTOS QUE PERMITEN TRANSFERIR DATOS PERSONALES DESDE LA UNIÓN EUROPEA A PAÍSES TERCEROS, SIEMPRE CON EL OBJETIVO DE QUE LA PROTECCIÓN QUE LOS DATOS RECIBEN EN LA UNIÓN EN VIRTUD DEL DERECHO EUROPEO DE PROTECCIÓN DE DATOS NO SE VEA MERMADA A RAÍZ DE LA TRANSFERENCIA Y POSTERIOR UTILIZACIÓN DE LOS DATOS.

En concreto, el artículo 46 del RGPD incluye entre los instrumentos mediante los que los exportadores (que pueden ser responsables o encargados de tratamiento) pueden ofrecer garantías suficientes de que se mantendrá el nivel de protección algunas novedades que no se contemplaban en la Directiva. Entre ellas destacan los acuerdos jurídicamente vinculantes entre autoridades u organismos públicos, las nuevas cláusulas contractuales tipo adoptadas por la Comisión o por las autoridades de supervisión nacionales, los códigos de conducta o esquemas de certificación y las "normas corporativas vinculantes" (BCR, por sus siglas en inglés), que pueden referirse a grupos empresariales o a uniones de empresas.[27]

Ante esta pluralidad de opciones para encuadrar las transferencias internacionales cabe plantearse cuál puede ser el futuro de las decisiones de adecuación.

En el pasado, se han destacado algunas de las aparentes debilidades de este mecanismo de transferencia, señalándose en particular el largo tiempo que puede suponer obtener una declaración de adecuación, la exigencia de los requisitos a cumplir para conseguir esa declaración o la aparente inconsistencia en la lista de países declarados adecuados, muy reducida y en la que faltan algunos de los principales destinos de los datos europeos.[28] También se ha criticado el supuesto interés de la Unión Europea en extender su modelo de protección de datos a través de estas decisiones de adecuación.

Sin embargo, existen diversos factores que pueden contribuir a que el sistema de adecuación mantenga su valor en el futuro como un mecanismo para facilitar los flujos transfronterizos de datos.

La Comisión explica algunos de estos factores en su comunicación "Intercambio y protección de los datos personales en un mundo globalizado". En donde explica que las demandas para una eficaz protección de datos personales no se limitan, como ocurría en el pasado, a Europa. Los ciudadanos en todo el mundo están cada vez más preocupados por su privacidad, posiblemente como consecuencia del impacto de las nuevas tecnologías y su uso intensivo de datos personales. Esa creciente preocupación se traduce en la rápida aprobación de normas sobre protección de datos y privacidad en todas las regiones del mundo. La comunicación cita diversos estudios que señalan que más de cien países ya han introducido o modificado sus normas.

Al mismo tiempo, la Comisión señala que, si bien la protección de datos no es una materia negociable en acuerdos comerciales internacionales, el respeto a la privacidad constituye un requisito para permitir los flujos comerciales en un mundo globalizado en que esos flujos precisan en la mayoría de los casos de intercambios de datos personales.

En ese contexto, la Comisión reconoce que las decisiones de adecuación son "la mejor manera de fomentar la confianza mutua y garantizar la libre circulación de datos personales, favoreciendo así los intercambios comerciales que conllevan transferencias de datos personales al tercer país interesado".

Por ello, la Comisión define una estrategia que podríamos considerar proactiva en materia de decisiones de adecuación, la cual busca fomentar su empleo de acuerdo con las prioridades que ya se mencionaron anteriormente en este artículo. Entre esas prioridades, la Comisión incluye expresamente, "dependiendo de los progresos que logren en la modernización de sus leyes de protección de datos", a los "países de América Latina, sobre todo los pertenecientes a Mercosur".[29]

Más allá de la voluntad expresada por la Comisión, se ha producido muy recientemente un desarrollo cuyo impacto sobre el uso de las decisiones de adecuación no puede todavía valorarse pero que es posible que sea significativo.

Se trata de la segunda sentencia del Tribunal de Justicia de la Unión

CUANDO LA LEGISLACIÓN DE UN PAÍS IMPIDA AL IMPORTADOR CUMPLIR CON SUS OBLIGACIONES, EL EXPORTADOR DEBE OFRECER GARANTÍAS SUPLEMENTARIAS QUE PERMITAN RESOLVER LA SITUACIÓN Y ASEGURAR EL NIVEL DE PROTECCIÓN ADECUADO. SI NO PUEDE HACERLO, DEBE SUSPENDER LA TRANSFERENCIA O, SI PRETENDE CONTINUAR CON ELLA, INFORMAR A LA AUTORIDAD DE SUPERVISIÓN.

Europea conocida como Schrems II, en la que se confirma la validez de la decisión de la Comisión por la que se adoptan las cláusulas contractuales tipo (CCT) para las transferencias internacionales y se declara no válida la decisión que declara la adecuación del Escudo de Privacidad.[30]

En esta sentencia, el TJUE reafirma su doctrina en la primera sentencia Schrems, sobre el Puerto Seguro respecto a la noción de "nivel de protección esencialmente equivalente" como en lo tocante a las garantías que deben establecerse para que el acceso de las autoridades públicas a los datos transferidos se produzca en términos compatibles con el derecho europeo. Es decir, el Tribunal mantiene el estándar riguroso que definió en Schrems I para la declaración de adecuación.

Pero a los efectos que aquí nos interesan es incluso más relevante que el Tribunal, al tiempo que valida las CCT de la Comisión, expresa su interpretación de que las garantías que se ofrecen mediante esas cláusulas (y, en general, mediante cualquier instrumento de transferencia) deben asegurar también un nivel de protección esencialmente equivalente al existente en la Unión.

El TJUE señala que corresponde al exportador, auxiliado por el importador, determinar si la legislación del país de destino contiene elementos que impidan al importador cumplir con sus obligaciones de acuerdo con las cláusulas. Esto puede suceder en la medida en que las cláusulas no pueden oponerse a las autoridades públicas en el tercer país, dado que se trata de obligaciones entre partes privadas que, por sí mismas, no vinculan a las autoridades.

Cuando la legislación de un país impida al importador cumplir con sus obligaciones, el exportador debe ofrecer garantías suplementarias que permitan resolver la situación y asegurar el nivel de protección adecuado. Si no puede hacerlo, debe suspender la transferencia o, si pretende continuar con ella, informar a la autoridad de supervisión.

En conclusión, el Tribunal exige que el uso de cada instrumento de transferencia hacia un país determinado debe ir precedido de una especie de evaluación de adecuación de la legislación vigente en ese país y de su aplicación práctica desde la perspectiva de cuáles puedan ser sus consecuencias en el terreno de la protección de los datos transferidos. En ese sentido, un aspecto que destaca a la vista de la jurisprudencia del Tri-

Y LA PREGUNTA QUE CABRÍA HACERSE ES HASTA QUÉ PUNTO ESTA NUEVA SITUACIÓN PODRÍA DESINCENTIVAR EL USO DE LOS NUEVOS INSTRUMENTOS DE TRANSFERENCIA DISTINTOS DE LA ADECUACIÓN QUE CONTEMPLA EL RGPD EN BENEFICIO DE UN ENFOQUE MÁS GLOBAL QUE PERMITA A TODOS LOS IMPORTADORES DE UN PAÍS O A UN TERRITORIO O SECTOR DE ESE PAÍS, RECIBIR DE FORMA FLUIDA LOS DATOS ENVIADOS DESDE LA UNIÓN EUROPEA.

bunal es el de los accesos por parte de las autoridades con fines de seguridad nacional o *law enforcement*.

Y la pregunta que cabría hacerse es hasta qué punto esta nueva situación podría desincentivar el uso de los nuevos instrumentos de transferencia distintos de la adecuación que contempla el RGPD en beneficio de un enfoque más global que permita a todos los importadores de un país o a un territorio o sector de ese país, recibir de forma fluida los datos enviados desde la Unión Europea.

En los últimos años, este mecanismo se ha incluido en algunas de las normas de protección de datos adoptadas por países no miembros de la UE. Un buen ejemplo al respecto puede ser el de Japón, que incluye el instrumento de la declaración de adecuación en su legislación y que, de hecho, ha sido el primero que declara la adecuación, de acuerdo con su normativa de la protección, del nivel de protección ofrecido por los países miembros de la UE, simultáneamente a la declaración adoptada en esa región.

Diversos factores respaldan que la declaración de adecuación de un país tercero o receptor, o más precisamente que la existencia de un "nivel sustancialmente equivalente de protección" puede seguir teniendo un espacio propio como medio para facilitar los flujos de datos desde la Unión Europea a otras naciones o regiones, incluso con un mayor alcance que el que ha tenido hasta ahora.

NOTAS

1 Art. 25.1 "Los Estados miembros dispondrán que la transferencia a un país tercero de datos personales que sean objeto de tratamiento o destinados a ser objeto de tratamiento con posterioridad a su transferencia, únicamente pueda efectuarse cuando, (…), el país tercero de que se trate garantice un nivel de protección adecuado".

2. Art. 26.2 "Sin perjuicio de lo dispuesto en el apartado 1, los Estados miembros podrán autorizar una transferencia o una serie de transferencias de datos personales a un tercer país que no garantice un nivel de protección adecuado con arreglo al apartado 2 del artículo 25, cuando el responsable del tratamiento ofrezca garantías suficientes respecto de la protección de la vida privada, de los derechos y libertades fundamentales de las personas, (…)".

3. Ley Orgánica 15/99, del 13 de diciembre, de Protección de Datos de Carácter Personal. Art. 33.2. "2. El carácter adecuado del nivel de protección que ofrece el país de destino se evaluará por la Agencia de Protección de Datos atendiendo a todas las circunstancias que concurran en la transferencia o categoría de transferencia de datos. (…)".

4. Art. 26.6 "La Comisión podrá hacer constar, de conformidad con el procedimiento previsto en el apartado 2 del artículo 31, que un país tercero garantiza un nivel de protección adecuado de conformidad con el apartado 2 del presente artículo, (…). Los Estados miembros adoptarán las medidas necesarias para ajustarse a la decisión de la Comisión".

5. "Transfers of personal data to third countries: Applying Articles 25 and 26 of the EU data protection directive". Adopted by the Working Party on 24 July 1998.

6. No obstante, sí se incluye una referencia a que la adopción de estas decisiones deberá contar con la participación del comité previsto en su artículo 31, en el que están representados los Estados miembros, así como la necesidad de buscar la opinión del Grupo de Trabajo del Artículo 29, tal y como se establece en el artículo 30.1.b.

7. Decisión 2002/2/CE de la Comisión, de 20 de diciembre de 2001. Disponible en https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:32002D0002&from=ES

8. Decisión 2011/61/UE de la Comisión, de 31 de enero de 2011. Disponible en https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:32011D0061&from=ES
9. Decisión 2000/520/CE de la Comisión, de 26 de julio de 2000. Disponible en https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:32000D0520&from=RO
10. Decisión de Ejecución (UE) 2016/1250 de la Comisión, de 12 de julio de 2016. Disponible en https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:32016D1250&from=es. Declarada no válida por el Tribunal de Justicia de la Unión Europea en la Sentencia C-311/18, Schrems II.
11. Comunicación de la Comisión «Intercambio y protección de los datos personales en un mundo globalizado», COM. (2017) 7 final, p. 10. Disponible en https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:52017DC0007&from=ES
12. Sentencia TJUE de 6 de octubre de 2015, *Maximiliam Schrems c. Data Protection Commissioner* (C-362/14) http://curia.europa.eu/juris/document/document.jsf?docid=169195&doclang=ES. En relación con este punto, es particularmente ilustrativo el fundamento 73, en el que el Tribunal señala que "es verdad que el término "adecuado" que figura en el artículo 25, apartado 6, de la Directiva 95/46 significa que no cabe exigir que un tercer país garantice un nivel de protección idéntico al garantizado en el ordenamiento jurídico de la Unión. Sin embargo, como ha manifestado el abogado general en el punto 141 de sus conclusiones, debe entenderse la expresión "nivel de protección adecuado" en el sentido de que exige que ese tercer país garantice efectivamente, por su legislación interna o sus compromisos internacionales, un nivel de protección de las libertades y derechos fundamentales sustancialmente equivalente al garantizado en la Unión por la Directiva 95/46, entendida a la luz de la Carta. En efecto, a falta de esa exigencia el objetivo mencionado en el anterior apartado de la presente sentencia se frustraría. Además, el elevado nivel de protección garantizado por la Directiva 95/46 entendida a la luz de la Carta se podría eludir fácilmente con transferencias de datos personales desde la Unión a terceros países para su tratamiento en éstos".
13. RGPD, artículo 45.2.a

14. Sobre este punto pueden consultarse las orientaciones proporcionadas por el GT29 en su documento de trabajo 01/2016 sobre "justificación de injerencias en los derechos fundamentales a la privacidad y la protección de datos a través de medidas de vigilancia a la hora de transferir datos personales (garantías esenciales europeas)", WP 237, 13 de abril de 2016 (disponible en https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2016/wp237_en.pdf), que ha sido posteriormente ampliado por el Comité Europeo de Protección de Datos a través de sus "Recommendations 02/2020 on the European Essential Guarantees for surveillance measures", adoptadas el 10 de noviembre de 2020, disponible solo en inglés en https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_recommendations_202002_europeanessentialguaranteessurveillance_en.pdf

15. Ver Sentencia Schrems, citada, fundamentos de derecho 88 y ss., entre otros.

16. Puede comprobarse esta evolución comparando, por ejemplo, el considerando 14 de la decisión de la Comisión (2003/490/CE), sobre adecuación de Argentina (disponible en https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:32003D0490&from=ES), con el considerando 10 de la Decisión de Ejecución de la Comisión (2012/484/UE) (disponible en https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:32012D0484&from=ES), sobre adecuación de Uruguay, o con el considerando 11 de la Decisión de Ejecución de la Comisión (2013/65/UE), sobre adecuación de Nueva Zelanda (disponible en https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:32013D0065&from=ES).

17. Ver Decisión de Ejecución (UE) 2019/419 de la Comisión, sección 4, considerandos 95 a 102 (disponible en https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:32019D0419&from=EN).

18. "Referencias sobre adecuación", revisado y aprobado el 6 de febrero de 2018, WP254, disponible en https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=614108 . Aunque el documento fue adoptado formalmente por el GT29, fue posteriormente refrendado por el CEPD en su primera reunión de mayo de 2018.

19. Artículos 9 y 10 del RGPD.

20. Nota de la edición: de acuerdo con Andreas Schedler, la traducción más común y la más cercana es *rendición de cuentas. En Cuaderno de Transparencia 03 ¿Qué es la rendición de cuentas?,* p. 10. INAI. 2015.

21. Carta de los Derechos Fundamentales de la Unión Europea, artículo 51. Disponible en https://www.europarl.europa.eu/charter/pdf/text_es.pdf

22. "Justificación de injerencias en los derechos fundamentales a la privacidad y la protección de datos a través de medidas de vigilancia a la hora de transferir datos personales (garantías esenciales europeas), y "Recommendations 02/2020 on the European Essential Guarantees for surveillance measures", citados en nota 14.

23. Ver la manifestación expresa que se contiene en el "Dictamen 28/2018 sobre el Proyecto de Decisión de Ejecución de la Comisión Europea sobre la protección adecuada de los datos personales en Japón", p. 5. disponible en https://edpb.europa.eu/sites/edpb/files/files/file1/2018-12-05-opinion_2018-28_art.70_ja_es.pdf

24. Disponible en: https://www.google.com/search?q=taxativo&rlz=1C1CHBF_esMX834MX834&oq=taxativo&aqs=chrome..69i57j0i512l4j0i10i512j0i512l4.3001j1j15&sourceid=chrome&ie=UTF-8#:~:text=Que%20no%20admite%20discusi%C3%B3n%20o%20que%20corta%20cualquier%20posibilidad%20de%20r%C3%A9plica

25. Comunicación de la Comisión "Intercambio y protección de los datos personales en un mundo globalizado", citada en la nota 14.

26. Puede consultarse, por ejemplo, el ya citado Dictamen 28/2018 sobre el Proyecto de Decisión de Ejecución de la Comisión Europea sobre la protección adecuada de los datos personales en Japón, pp. 4 a 5 y 8 a 11, donde se hace referencia tanto a las conversaciones entre la Comisión y las autoridades japonesas en relación con determinados aspectos considerados en el proyecto de decisión como al diálogo entre el propio Comité y la Comisión, que condujo a que la Comisión modificara hasta en dos ocasiones su propuesta de decisión. En ese mismo dictamen se alude también a que en el caso de Japón la evaluación tiene características particulares, dado que es preciso valorar tanto la legislación aplicable como normas suplementarias adoptadas en el proceso de adecuación.

27. Las BCR existían con anterioridad al RGPD, pero no tenían un respaldo formal en la normativa europea, dado que se desarrollaron, principalmente, como resultado de los trabajos del GT29.

28. En esta lista encontramos a Andorra, Argentina, Canadá, Guernsey, Isla de Man, Islas Feroe, Israel, Jersey, Nueva Zelanda, Suiza, Uruguay y muy recientemente el Escudo de Privacidad con EEUU. Japón ha sido el último país en sumarse.

29. Comunicación, p. 9.

30. Sentencia en el caso (C.311/2018), Maximiliam Schrems c. Data Protection Commissioner. Disponible en: http://curia.europa.eu/juris/document/document.jsf?text=&docid=228677&pageIndex=0&doclang=ES&mode=req&dir=&occ=first&part=1&cid=9841532

Las decisiones de adecuación en el marco del Reglamento General de Protección de Datos. Nuevo régimen europeo de protección de datos personales: la adecuación de tercer país,
primera edición digital, 29 de noviembre de 2021.

Edición a cargo de:
Dirección General de Promoción y Vinculación con la Sociedad.

Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales

© Instituto Nacional de Transparencia,
Acceso a la Información y Protección de Datos Personales (INAI)
Insurgentes Sur 3211, colonia Insurgentes Cuicuilco,
Alcaldía Coyoacán, C. P. 04530,
Ciudad de México.
Primera edición digital, noviembre de 2021.
Hecho en México / *Made in Mexico*

Infórmate:

Ingresa a

www.inai.org.mx

Acude al Centro de Atención a la Sociedad [CAS]
Insurgentes Sur 3211,
Colonia Insurgentes Cuicuilco,
Alcaldía Coyoacán, C. P. 04530,
Ciudad de México.
Llama sin costo al

800 835 4324

inai

Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales