COMISIÓN EUROPEA
DIRECCIÓN GENERAL XV
Mercado Interior y Servicios Financieros
Libre Circulación de la Información, Derecho de Sociedades e Información Financiera
Libre Circulación de la Información, protección de datos y sus aspectos internacionales

DG XV D/5025/98
WP 12

Grupo de Trabajo sobre la protección de las personas físicas en lo que respecta al tratamiento de datos personales

Documento de Trabajo

Transferencias de datos personales a terceros países: aplicación de los artículos 25 y 26 de la Directiva sobre protección de datos de la UE

Aprobado por el Grupo de Trabajo el 24 de julio de 1998

[versión española corregida]

Índice

Introducción

El objetivo de este documento consiste en reunir el trabajo previamente realizado por el Grupo de Trabajo de los Comisarios para la Protección de Datos de la UE, creado al amparo del artículo 29 de la Directiva sobre protección de datos[1], en un conjunto de reflexiones más exhaustivo sobre todas las cuestiones centrales planteadas en las transferencias de datos personales a terceros países en el contexto de la aplicación de la Directiva sobre protección de datos de la UE (95/46/CE). La estructura de este documento se ajusta al sistema utilizado en las transferencias internacionales de datos personales expuesto en los artículos 25 y 26 de la directiva. (Se ha incluido el texto de estos artículos en el Anexo 2)

El apartado 1 del artículo 25 establece el principio por el cual los Estados miembros sólo podrán permitir una transferencia si los terceros países en cuestión aseguran un nivel adecuado de protección. El apartado 2 declara que el "carácter adecuado" deberá evaluarse caso por caso "atendiendo a todas las circunstancias que concurran en una transferencia o en una categoría de transferencias de datos". El apartado 6 dispone que la Comisión podrá declarar que ciertos países ofrecen una protección adecuada. **El capítulo uno** de este documento trata la cuestión central de la protección adecuada. Su objetivo es explicar lo que se entiende por "adecuada" y esboza un marco de cómo debe evaluarse el carácter adecuado de la protección en un caso concreto.

La aplicación de este enfoque se trata más detalladamente en los capítulos dos y tres. **El capítulo dos** se ocupa de las transferencias a países que han ratificado el Convenio 108 del Consejo de Europa, mientras que **el capítulo tres** evalúa las cuestiones que rodean las transferencias en las cuales la protección de datos personales se facilita principal o completamente mediante mecanismos de autorregulación y no por normas de Derecho.

A falta de una protección adecuada entendida según el artículo 25.2, la Directiva también contempla en el artículo 26.2 la posibilidad de medidas *ad hoc*, sobre todo de tipo contractual, que podrían dar lugar al establecimiento de garantías adecuadas sobre cuya base podrían realizarse las transferencias en cuestión. En **el capítulo cuatro** de este documento se examina en qué circunstancias las soluciones contractuales *ad hoc* pueden ser apropiadas y se mencionan algunas recomendaciones sobre la forma y el contenido posibles de dichas soluciones.

El capítulo cinco se ocupa de la tercera y última situación contemplada en la directiva: los grupos limitados de casos contenidos en el artículo 26.1 que incluyen efectivamente una excepción al requisito de "protección adecuada". Se examina el alcance exacto de

[1] Véase **WP 4 (5020/97)** "Primeras orientaciones sobre las transferencias de datos personales a países terceros - Posibles formas de evaluar su adecuación", un documento de debate adoptado por el Grupo de Trabajo el 26 de junio 1997;
Documento de trabajo del **WP 7 (5057/97)**: "Evaluación de la autorregulación industrial: ¿en qué casos realiza una contribución significativa al nivel de protección de datos en un país tercero?", adoptado por el Grupo de Trabajo el 14 de enero de 1998;
Documento de trabajo del **WP 9 (5005/98)**: "Conclusiones preliminares sobre la utilización de disposiciones contractuales en caso de transferencia de datos personales a terceros países", adoptado por el Grupo de Trabajo el 22 de abril de 1998.

estas excepciones, con ejemplos ilustrativos de los tipos de casos abarcables, junto con los que no parecen serlo.

Por último, **el capítulo seis** contiene algunos comentarios sobre cuestiones de procedimiento que surgen al juzgar el carácter adecuado (o inadecuado) de la protección y sobre la consecución de un enfoque coherente de estas cuestiones a escala comunitaria.

El anexo 1 comprende una serie de estudios ilustrativos que pretenden demostrar cómo puede aplicarse en la práctica el enfoque expuesto en este documento.

CAPÍTULO UNO: EVALUAR SI LA PROTECCIÓN ES ADECUADA

1) ¿Qué debe entenderse por "protección adecuada"?

El objetivo de la protección de datos es ofrecer protección a las personas cuyos datos son objeto de tratamiento. Normalmente, dicho objetivo se logra combinando los derechos del interesado y las obligaciones de quienes tratan los datos o controlan dicho tratamiento. Las obligaciones y los derechos establecidos en la Directiva 95/46/CE se basan en aquellos dispuestos en el Convenio nº 108 (1981) del Consejo de Europa, que a su vez no son diferentes de los incluidos en las directrices de la OCDE (1980) o en las directrices de la ONU (1990). Por eso, parece que existe un alto grado de consenso en relación con el contenido de las normas de protección de datos que traspasa los límites del espacio ocupado por los quince estados de la Comunidad.

Sin embargo, las normas de protección de datos sólo contribuyen a la protección de las personas físicas si efectivamente se cumplen en la práctica. Por ello es necesario considerar no sólo el contenido de las normas aplicables a los datos personales transferidos a un tercer país, sino también el sistema utilizado para asegurar la eficacia de dichas normas. En Europa, históricamente ha habido una tendencia a plasmar en el Derecho las normas de protección de datos, lo que ha permitido sancionar el incumplimiento y conceder a las personas físicas un derecho de reparación. Además, estas legislaciones han incluido en general otras normas de procedimiento como el establecimiento de autoridades de control con funciones de seguimiento e investigación de denuncias. Estos aspectos relativos al procedimiento están plasmados en la Directiva 95/46/CE, con sus disposiciones sobre responsabilidades, sanciones, recursos, autoridades de control y notificaciones. Fuera del ámbito comunitario es menos común encontrar estos medios de procedimiento para asegurar el cumplimiento de las normas de protección de datos. Los signatarios del Convenio 108 deben incorporar los principios de la protección de datos en su legislación, pero no se requieren mecanismos complementarios tales como una autoridad de control. Las directrices de la OCDE sólo exigen que “se tengan en cuenta” en la legislación nacional y no prevén procedimientos para garantizar que las directrices resulten en una protección efectiva de las personas físicas. Por otro lado, las últimas directrices de la ONU sí incluyen disposiciones de control y sanciones, lo que refleja una creciente sensibilización a nivel mundial sobre la necesidad de aplicar debidamente las normas de protección de datos.

En este contexto, es evidente que todo análisis significativo de la protección adecuada debe comprender los dos elementos básicos: el contenido de las normas aplicables y los medios para asegurar su aplicación eficaz.

Tomando la Directiva 95/46/CE como punto de partida, y teniendo en cuenta las disposiciones de otros textos internacionales sobre la protección de datos, debería ser posible lograr un “núcleo” de principios de “contenido” de protección de datos y de requisitos “de procedimiento/de aplicación”, cuyo cumplimiento pudiera considerarse un requisito mínimo para juzgar adecuada la protección. Esta lista mínima no debería ser inamovible. En algunos casos será necesario ampliar la lista, mientras que en otros incluso sea posible reducirla. El grado de riesgo que la transferencia supone para el

interesado será un factor importante para determinar los requisitos concretos de un caso determinado. A pesar de esta condición, la compilación de una lista básica de condiciones mínimas es un punto de partida útil para cualquier análisis.

i) Principios de contenido

Se sugiere la inclusión de los siguientes principios básicos:

1) **Principio de limitación de objetivos** - los datos deben tratarse con un objetivo específico y posteriormente utilizarse o transferirse únicamente en cuanto ello no sea incompatible con el objetivo de la transferencia. Las únicas excepciones a esta norma serían las necesarias en una sociedad democrática por una de las razones expuestas en el artículo 13 de la Directiva.[2]

2) **Principio de proporcionalidad y de calidad de los datos -** los datos deben ser exactos y, cuando sea necesario, estar actualizados. Los datos deben ser adecuados, pertinentes y no excesivos con relación al objetivo para el que se transfieren o para el que se tratan posteriormente.

3) **Principio de transparencia -** debe informarse a los interesados acerca del objetivo del tratamiento y de la identidad del responsable del tratamiento en el tercer país, y de cualquier otro elemento necesario para garantizar un trato leal. Las únicas excepciones permitidas deben corresponder a los artículos 11.2[3] y 13 de la Directiva.

4) **Principio de seguridad -** el responsable del tratamiento debe adoptar medidas técnicas y organizativas adecuadas a los riesgos que presenta el tratamiento. Toda persona que actúe bajo la autoridad del responsable del tratamiento, incluido el encargado del tratamiento, no debe tratar los datos salvo por instrucción del responsable del tratamiento.

5) **Derechos de acceso, rectificación y oposición -** el interesado debe tener derecho a obtener una copia de todos los datos a él relativos, y derecho a rectificar aquellos datos que resulten ser inexactos. En determinadas situaciones, el interesado también debe poder oponerse al tratamiento de los datos a él relativos. Las únicas excepciones a estos derechos deben estar en línea con el artículo 13 de la Directiva.

6) Restricciones respecto a transferencias sucesivas a otros terceros países - únicamente deben permitirse transferencias sucesivas de datos personales del tercer país de destino a otro tercer país en el caso de que este último país garantice asimismo un nivel de protección adecuado. Las únicas excepciones permitidas deben estar en

[2] El artículo 13 permite una limitación al 'principio de los objetivos' cuando tal limitación constituya una medida necesaria para la salvaguardia de la seguridad del Estado, la defensa, la seguridad pública, la prevención, la investigación, la detección y la represión de infracciones penales o de las infracciones de la deontología en las profesiones reglamentadas, un interés económico y financiero importante, o la protección del interesado o de los derechos y libertades de otras personas.

[3] El artículo 11.2 estipula que cuando los datos no han sido recabados del propio interesado, la información no se facilitará al interesado si resulta imposible, si exige esfuerzos desproporcionados o si el registro o la comunicación de los datos están expresamente exigidos por ley.

línea con el artículo 26.1 de la directiva (estas excepciones se examinan en el capítulo cinco.)

A continuación figuran ejemplos de principios adicionales que deben aplicarse a tipos específicos de tratamiento:

1) **Datos sensibles -** cuando se trate de categorías de datos "sensibles" (las incluidas en el artículo 8 de la Directiva[4]), deberán establecerse protecciones adicionales, tales como la exigencia de que el interesado otorgue su consentimiento explícito para el tratamiento.

2) **Mercadotecnia directa -** en el caso de que el objetivo de la transferencia de datos sea la mercadotecnia directa, el interesado deberá tener en cualquier momento la posibilidad de negarse a que sus datos sean utilizados con dicho propósito.

3) **Decisión individual automatizada -** cuando el objetivo de la transferencia sea la adopción de una decisión automatizada en el sentido del artículo 15 de la Directiva, el interesado deberá tener derecho a conocer la lógica aplicada a dicha decisión, y deberán adoptarse otras medidas para proteger el interés legítimo de la persona.

ii) Mecanismos del procedimiento/de aplicación

En Europa existe un amplio consenso sobre la necesidad de plasmar los principios de la protección de datos en la legislación. También es amplio el consenso en que un sistema de "supervisión externa" en forma de una autoridad independiente es una característica necesaria de un sistema de cumplimiento de la protección de datos. Sin embargo, en otras partes del mundo no siempre se encuentran estas características.

Con el fin de sentar las bases para evaluar el carácter adecuado de la protección ofrecida, es necesario distinguir los objetivos de un sistema normativo de protección de datos, y sobre esta base juzgar la variedad de diferentes mecanismos de procedimiento judiciales y no judiciales utilizados en terceros países.

Los objetivos de un sistema de protección de datos son básicamente tres:

1) Ofrecer un **nivel satisfactorio de cumplimiento** de las normas. (Ningún sistema puede garantizar el 100 % de cumplimiento, pero algunos son mejores que otros). Un buen sistema se caracteriza, en general, por el hecho de que los responsables del tratamiento conocen muy bien sus obligaciones y los interesados conocen muy bien sus derechos y medios para ejercerlos. La existencia de sanciones efectivas y disuasorias es importante a la hora de garantizar la observancia de las normas, al igual que lo son, como es natural, los sistemas de verificación directa por las autoridades, los auditores o los servicios de la Administración encargados específicamente de la protección de datos.

[4] Datos que releven el origen racial o étnico, las opiniones políticas, las convicciones religiosas o filosóficas, la pertenencia a sindicatos, datos relativos a la salud o a la sexualidad, así como datos relativos a infracciones, condenas penales o medidas de seguridad.

2) Ofrecer **apoyo y asistencia a los interesados** en el ejercicio de sus derechos. El interesado debe tener la posibilidad de hacer valer sus derechos con rapidez y eficacia, y sin costes excesivos. Para ello es necesario que haya algún tipo de mecanismo institucional que permita investigar las denuncias de forma independiente.

3) Ofrecer **vías adecuadas de recurso** a quienes resulten perjudicados en el caso de que no se observen las normas. Éste es un elemento clave que debe incluir un sistema que ofrezca la posibilidad de obtener una resolución judicial o arbitral y, en su caso, indemnizaciones y sanciones.

CAPÍTULO DOS: APLICACIÓN DEL ENFOQUE A LOS PAÍSES QUE HAN RATIFICADO EL CONVENIO 108 DEL CONSEJO DE EUROPA

El Convenio 108 es el único instrumento internacional existente con poder vinculante en el área de la protección de datos, aparte de la Directiva. La mayoría de los signatarios del Convenio también son Estados miembros de la Unión Europea (actualmente cuenta con la ratificación de los 15) o países, como Noruega e Islandia, donde en cualquier caso la Directiva es vinculante en virtud del acuerdo del Espacio Económico Europeo. Sin embargo, Eslovenia, Hungría y Suiza también han ratificado el Convenio, y es posible que otros terceros países lo hagan en el futuro, en particular porque el Convenio también está abierto a países no pertenecientes al Consejo de Europa. Por tanto, examinar si es posible considerar que los países que han ratificado el Convenio ofrecen un nivel adecuado de protección en el sentido del artículo 25 de la Directiva, es interesante no sólo por motivos académicos.

Como punto de partida, es útil examinar el propio texto del Convenio a la luz del esbozo teórico de la "protección adecuada" expuesta en el capítulo uno de este documento.

Respecto al contenido de los principios básicos, puede decirse que el Convenio incluye las cinco primeras de las seis "condiciones mínimas"[5]. El Convenio también incluye el requisito de una protección adecuada para los datos sensibles, la cual será requisito de adecuación cuando se trate de tales datos.

Un elemento ausente en el Convenio, desde el punto de vista del contenido de sus normas sustantivas, son las restricciones a las transferencias a países no signatarios del Convenio. Esta carencia supone el riesgo de que un país signatario del Convenio 108 pueda utilizarse como "escala" en una transferencia de datos de la Comunidad a otro tercer país con niveles de protección absolutamente insuficientes.

El segundo aspecto de la "protección adecuada" se refiere a los mecanismos de procedimiento instaurados para asegurar que los principios básicos resulten eficaces. El Convenio exige que sus principios se plasmen en legislaciones nacionales y que se establezcan sanciones y remedios apropiados en caso de violación de estos principios. Estas medidas deberían bastar para garantizar un nivel razonable de cumplimiento de las normas y una reparación adecuada para los interesados en caso de incumplimiento de las normas (objetivos 1) y 3) de un sistema de cumplimiento de la protección de datos). No obstante, el Convenio no obliga a las partes contratantes a establecer mecanismos institucionales que permitan la investigación independiente de las quejas, aunque en general los países que lo han ratificado así lo han hecho en la práctica. Esto es un punto flaco porque, sin estos mecanismos institucionales, no se garantiza el apoyo y la asistencia prestados a las personas cuyos datos son objeto de tratamiento en el ejercicio de sus derechos (objetivo 2).

[5] Pueden surgir algunas dudas respecto del 'principio de transparencia'. El artículo 8.a) del Convenio quizá no se corresponda con el deber *activo* de facilitar información, que es la esencia de los artículos 10 y 11 de la Directiva. Además, el Convenio no incluye ningún derecho específico de "exclusión voluntaria" cuando se utilizan los datos con fines de mercadotecnia directa, ni ninguna disposición sobre decisiones individuales automatizadas (elaboración de perfiles).

Este breve análisis parece indicar que es posible permitir la mayoría de las transferencias de datos personales a países que han ratificado el Convenio 108 al amparo del artículo 25.1 de la Directiva a condición de que

- el país en cuestión también disponga de mecanismos adecuados para garantizar el cumplimiento, ayudar a las personas físicas y facilitar la reparación (como, por ejemplo, una autoridad de control independiente dotada de las competencias apropiadas); y
- el país en cuestión sea el destino final de la transferencia y no un país intermediario a través del cual transitan los datos, excepto cuando las transferencias sucesivas se dirigen de nuevo a la UE o a otro destino que ofrezca una protección adecuada [6].

Evidentemente, este es un examen bastante simplificado y superficial del Convenio. Los casos específicos de las transferencias de datos a los países signatarios del Convenio pueden plantear nuevos problemas que no se han tratado en este documento.

[6] Actualmente se está revisando el Convenio 108, un proceso que puede dar lugar a modificaciones que aborden estas y otras dificultades.

CAPÍTULO TRES: APLICACIÓN DEL ENFOQUE A LA AUTORREGULACIÓN INDUSTRIAL

Introducción

El artículo 25.2 de la Directiva sobre protección de datos (95/46/CE) establece que el nivel de protección que ofrece un tercer país se evaluará atendiendo a *todas las circunstancias* que concurran en una transferencia o en una categoría de transferencias de datos. Se hace referencia específica no sólo a las normas de Derecho, sino también a "las normas profesionales y las medidas de seguridad en vigor en dichos países."

El texto de la Directiva exige por lo tanto que se tengan en cuenta las normas no jurídicas que puedan existir en el tercer país en cuestión, siempre que estas normas *se cumplan*. En este contexto debe evaluarse la función de la autorregulación industrial.

¿Qué es la autorregulación?

El término "autorregulación" puede significar cosas distintas para diferentes personas. A efectos del presente documento, deberá entenderse por código de autorregulación (u otro instrumento) cualquier conjunto de normas de protección de datos aplicable a una pluralidad de responsables del tratamiento que pertenezcan a la misma profesión o al mismo sector industrial, cuyo contenido haya sido determinado fundamentalmente por los miembros del sector industrial o profesión en cuestión.

Esta es una definición amplia que abarcaría desde un código de protección de datos voluntario elaborado por una pequeña asociación industrial con pocos miembros, hasta los detallados códigos de ética profesional aplicables a profesiones enteras, tales como médicos y banqueros, que a menudo tienen una fuerza cuasi judicial.

¿Es el organismo responsable del código representativo del sector?

Tal como sostendrá este capítulo, un importante criterio para juzgar el valor de un código es su fuerza ejecutiva. En este contexto, la cuestión de si la asociación u organismo responsable del código representa a todos los operadores del sector o únicamente a un pequeño porcentaje de éstos tiene probablemente menos importancia que la fuerza de la asociación en cuanto a su capacidad para imponer sanciones a sus miembros por incumplimiento del código, por ejemplo. No obstante, existen diversas razones secundarias que hacen que los códigos aplicables a todo un sector industrial o a toda una profesión sean instrumentos de protección más útiles que los elaborados por pequeñas agrupaciones de empresas dentro de un sector industrial. En primer lugar figura el hecho de que un sector industrial fragmentado y caracterizado por diversas asociaciones rivales, cada una con su propio código de protección de datos, resulta confuso para el consumidor. La coexistencia de varios códigos diferentes crea un panorama opaco para las personas cuyos datos son objeto de tratamiento. En segundo lugar, especialmente en sectores tales como la mercadotecnia directa, donde es práctica corriente transferir los datos personales entre diferentes empresas del mismo sector, pueden surgir situaciones en que la empresa que transmita datos personales no esté sujeta al mismo código de protección de datos que la empresa receptora. Esto supone una gran fuente de ambigüedad en cuanto a la naturaleza de las normas aplicables, y

también puede dificultar en gran medida la investigación y resolución de las denuncias de los interesados.

Evaluación de la autorregulación - el enfoque más adecuado

Dada la gran variedad de instrumentos que entran dentro del concepto de autorregulación, está claro que existe una necesidad de diferenciar entre las diversas formas de autorregulación por su impacto real en el nivel de la protección de datos aplicable cuando se transfieran datos personales a un tercer país.

El punto de partida para la evaluación de cualquier conjunto específico de normas sobre protección de datos (tengan éstas categoría de autorregulación o de norma legal) debe ser el enfoque general establecido en el capítulo uno de este documento. La piedra angular de este enfoque es el examen no sólo del contenido del instrumento (deberá contener una serie de principios básicos) sino también de su eficacia para lograr:

- un buen nivel de cumplimiento general,
- apoyo y ayuda a las personas cuyos datos sean objeto de tratamiento,
- una reparación adecuada (incluida la compensación, cuando corresponda).

Evaluación del contenido de un instrumento de autorregulación

Esta es una tarea relativamente sencilla. Se trata de garantizar que estén presentes los "principios de contenido" expuestos en el capítulo uno. Es una evaluación objetiva. Se trata de ver cuál es el contenido del código, y no de cómo se elaboró. El hecho de que un sector industrial o profesión haya desempeñado una función primordial en el desarrollo del contenido de un código no es relevante por sí mismo, aunque evidentemente, si en su desarrollo se han tenido en cuenta las opiniones de las personas cuyos datos son objeto de tratamiento y de las organizaciones de consumidores, es más probable que el código refleje fielmente los principios básicos necesarios para la protección de datos.

La transparencia del código es un elemento crucial; en particular, el código debería redactarse en lenguaje sencillo y ofrecer ejemplos concretos que ilustren sus disposiciones.

Además, el código debería prohibir la transferencia de datos a empresas que no pertenezcan al sector y que no se rijan por el código, a menos que se prevean otras protecciones adecuadas.

Evaluación de la eficacia de un instrumento de autorregulación

La evaluación de la eficacia de un código o instrumento concreto de autorregulación es un ejercicio más difícil, que exige la comprensión de los métodos y formas para garantizar la adhesión al código y para resolver los problemas de incumplimiento. Es necesario que se cumplan los tres criterios funcionales de eficacia de la protección para considerar que un código de autorregulación proporciona una protección adecuada.

Un buen nivel de cumplimiento general

Típicamente, un código profesional o industrial será desarrollado por un organismo representativo del sector industrial o profesión en cuestión, y se aplicará a los miembros de dicho organismo representativo específico. El nivel de cumplimiento del código dependerá del grado de conocimiento de la existencia del código y su contenido por parte de sus miembros, de las medidas que se adopten para garantizar la transparencia del código a los consumidores con el fin de permitir a las fuerzas del mercado realizar una contribución eficaz, de la existencia de un sistema de control externo (tal como la exigencia de una auditoría de su cumplimiento a intervalos periódicos) y, quizá lo más importante, de la naturaleza y la aplicación de las sanciones en caso de incumplimiento.

Por tanto, son importantes las siguientes preguntas:

- ¿Qué medidas adopta el organismo representativo para asegurarse de que sus miembros conocen el código?
- ¿Exige el organismo representativo a sus miembros pruebas de que aplican las disposiciones del código? ¿Con qué frecuencia?
- ¿Presentan dichas pruebas las propias empresas o proceden de una fuente exterior (tal como un auditor acreditado)?
- ¿Investiga el organismo representativo las supuestas o presuntas violaciones del código?
- ¿Es el cumplimiento del código una condición para formar parte del organismo representativo o es dicho cumplimiento meramente "voluntario"?
- En caso de que un miembro viole el código, ¿con qué tipos de sanciones disciplinarias cuenta el organismo representativo (expulsión u otras)?
- ¿Es posible para una persona o empresa continuar trabajando en la profesión o sector industrial concreto después de haber sido expulsado del organismo representativo?
- ¿Puede hacerse cumplir el código de otras maneras, por ejemplo en los tribunales o en un tribunal especializado? Los códigos profesionales tienen fuerza legal en algunos países. En algunas circunstancias, también puede ser posible recurrir a las leyes generales relativas a prácticas comerciales correctas o incluso de competencia para conseguir el cumplimiento de los códigos de conducta de los sectores industriales.

Al examinar los tipos de sanciones existentes, es importante distinguir entre una sanción "reparadora" que, en caso de incumplimiento, únicamente exige al responsable del tratamiento la modificación de sus prácticas con el fin de adecuarlas a lo establecido en el código, y una sanción que vaya más lejos, castigando al responsable por su incumplimiento. Sólo esta segunda categoría de sanción "punitiva" tiene repercusión en el comportamiento futuro de los responsables del tratamiento al proporcionar un incentivo para que se cumpla sistemáticamente el código.

La falta de sanciones auténticamente disuasorias y punitivas es, por lo tanto, una carencia importante en un código. Sin dichas sanciones, es difícil entender cómo puede lograrse un nivel satisfactorio de cumplimiento general, a no ser que se establezca un sistema riguroso de control exterior (como una autoridad pública o privada

competente para intervenir en caso de incumplimiento del código, o una exigencia obligatoria de realizar auditorías externas a intervalos periódicos).

Apoyo y ayuda a las personas cuyos datos sean objeto de tratamiento

Un requisito esencial para un sistema de protección de datos adecuado y eficaz es que no se abandone a las personas que se enfrentan a un problema relativo a sus datos personales, sino que se les proporcione un apoyo institucional que permita resolver sus dificultades. Este apoyo institucional debería, idealmente, ser imparcial, independiente y poseer los poderes necesarios para investigar cualquier denuncia de un interesado. A este respecto, las preguntas que deben formularse respecto de la autorregulación son las siguientes:

- ¿Existe un sistema que permita la investigación de las denuncias de los interesados?
- ¿Cómo se da a conocer a los interesados este sistema y las decisiones adoptadas en cada caso concreto?
- ¿Supone el sistema costes para el interesado?
- ¿Quién realiza la investigación? ¿Tiene los poderes necesarios?
- ¿Quién juzga sobre una supuesta violación del código? ¿Es independiente e imparcial?

La imparcialidad del árbitro o juez sobre una supuesta violación de un código es un punto clave. Claramente, dicha persona u organismo deberá ser independiente respecto al responsable del tratamiento. No obstante, esto por sí mismo no basta para garantizar la imparcialidad. Idealmente, el árbitro debería asimismo ser ajeno a la profesión o sector en cuestión, dado que los miembros de una misma profesión o sector tienen una clara comunidad de intereses con el responsable del tratamiento que supuestamente haya infringido el código. A falta de esto, la neutralidad del órgano de decisión podría garantizarse incluyendo a representantes de los consumidores (en igual número) junto a los representantes del sector.

Reparación adecuada

Probada la infracción del código de autorregulación, deberá existir un recurso para el interesado. Este recurso deberá solucionar el problema (por ejemplo, corregir o suprimir datos incorrectos, o garantizar que cese el tratamiento con objetivos incompatibles) y, si se ha producido un perjuicio al interesado, prever el pago de una compensación adecuada. Hay que tener en cuenta que "perjuicio" en el sentido de la Directiva sobre protección de datos incluye no sólo el daño físico y la pérdida financiera, sino también cualquier daño psicológico o moral que se cause (llamado "distress" en el Derecho del Reino Unido y de EEUU).

Muchas de las cuestiones relativas a las sanciones que se han enumerado en la sección "Un buen nivel de cumplimiento general" son pertinentes aquí. Tal y como se ha explicado anteriormente, las sanciones tienen una doble función: castigar al infractor (y fomentar así el cumplimiento de las normas por parte del infractor y de los demás), y remediar una violación de las normas. Nos ocuparemos ahora de la segunda función. Por lo tanto, podrían plantearse también las siguientes preguntas:

- ¿Es posible comprobar si un miembro que haya violado el código, ha modificado después sus prácticas y solucionado el problema?
- ¿Pueden los interesados obtener compensación en virtud del código, y en caso afirmativo, de qué manera?
- ¿Equivale la violación del código a una ruptura de contrato, o es susceptible de sanción en virtud del Derecho público (por ejemplo, protección de los consumidores, competencia desleal), y puede la jurisdicción competente conceder indemnización por daños y perjuicios sobre dicha base?

Conclusiones

- La autorregulación debería evaluarse utilizando el enfoque funcional y objetivo establecido en el capítulo uno.
- Para que un instrumento de autorregulación pueda considerarse un elemento válido de "protección adecuada", debe ser vinculante para todos los miembros a quienes se transfieran los datos personales y proporcionar una protección adecuada si los datos se transfieren a terceros.
- El instrumento debe ser transparente e incluir el contenido básico de los principios esenciales de la protección de datos.
- El instrumento debe tener mecanismos que garanticen de forma eficaz un nivel satisfactorio de cumplimiento general. Una forma de lograrlo es el establecimiento de un sistema de sanciones disuasorias y punitivas. Otro sistema son las auditorías externas obligatorias.
- El instrumento debe proporcionar apoyo y ayuda a los interesados que se enfrenten a un problema relativo al tratamiento de sus datos personales. Por ello, debe existir un órgano independiente, imparcial y de fácil acceso que acoja las denuncias de los interesados y resuelva sobre las violaciones del código.
- El instrumento deberá garantizar una reparación adecuada en caso de incumplimiento. Los interesados deberán poder obtener una reparación de su problema y una compensación adecuada.

CAPÍTULO CUATRO: LA FUNCIÓN DE LAS DISPOSICIONES CONTRACTUALES

1. Introducción

La Directiva sobre protección de datos (95/46/EC) establece en su artículo 25.1 el principio de que sólo deben efectuarse transferencias de datos personales a terceros países si el país considerado ofrece un nivel de protección adecuado. El objetivo de este capítulo es estudiar la posibilidad de excepción al principio de "protección adecuada" del artículo 25 establecida en el artículo 26.2. Esta última disposición permite a un Estado miembro autorizar una transferencia o un conjunto de transferencias a un tercer país que no garantice una protección adecuada "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, así como respecto al ejercicio de los respectivos derechos". Esta disposición especifica, asimismo, que "dichas garantías podrán derivarse, en particular, de cláusulas contractuales". Además, el artículo 26.4 faculta a la Comisión para declarar, de conformidad con el procedimiento previsto en el artículo 31, que determinadas cláusulas contractuales tipo ofrecen garantías suficientes a efectos de lo dispuesto en el artículo 26.2.

La idea de utilizar un contrato para regular las transferencias internacionales de datos personales no proviene, evidentemente, de la Directiva. Ya en 1992, el Consejo de Europa, la Cámara de Comercio Internacional y la Comisión Europea iniciaron conjuntamente un estudio del tema.[7] Más recientemente, un número creciente de expertos y analistas, inspirados quizá por la referencia explícita de la Directiva, han comentado el uso de contratos en estudios y artículos. Los contratos también han seguido utilizándose en el "mundo real" con el objeto de resolver los problemas de protección planteados por la exportación de datos personales desde algunos Estados miembros de la UE. En Francia, se viene haciendo un uso extenso de ellos desde finales de la década de los ochenta. En Alemania, el reciente caso de la "Bahncard", en el que estaba implicado Citibank, recibió una considerable publicidad.[8]

2. Utilización de contratos en las transmisiones de datos intracomunitarias

Antes de examinar los requisitos que deben cumplir las cláusulas contractuales en el contexto de la transmisión de datos a terceros países, es importante aclarar la diferencia existente entre la situación de los países no comunitarios y la que prevalece dentro de la Comunidad. En este último caso, el contrato es el mecanismo utilizado

[7] *Model Contract to Ensure Equivalent Data Protection in the Context of Transborder Data Flows, with Explanatory Memorandum* [Contrato tipo para garantizar un nivel equivalente de protección de los datos en caso de transferencia transfronteriza de datos, con exposición de motivos], estudio realizado conjuntamente por el Consejo de Europa, la Comisión de las Comunidades Europeas y la Cámara de Comercio Internacional, Estrasburgo, 2 de noviembre de 1992.

[8] Véase la presentación de este caso realizada por Alexander Dix ante la Conferencia Internacional de Comisarios para la protección de los datos y la intimidad, septiembre de 1996, Ottawa.

para definir y regular el reparto de responsabilidades en materia de protección de datos, cuando en el tratamiento de los datos en cuestión interviene más de una entidad. De acuerdo con la Directiva, una entidad, el "responsable del tratamiento", debe asumir la responsabilidad principal del cumplimiento de los principios sustantivos de protección de datos. La segunda entidad, el "encargado del tratamiento", sólo es responsable de la seguridad de los datos. Una entidad se considera responsable del tratamiento si está capacitada para decidir sobre la finalidad y los medios del mismo, en tanto que el encargado del tratamiento es simplemente el organismo que presta materialmente el correspondiente servicio. La relación entre ambos se rige por lo dispuesto en el artículo 17.3 de la Directiva, en el que se establece lo siguiente:

> *La realización de tratamientos por encargo deberá estar regulada por un contrato u otro acto jurídico que vincule al encargado del tratamiento con el responsable del tratamiento, y que disponga, en particular:*
>
> - *que el encargado del tratamiento sólo actúa siguiendo instrucciones del responsable del tratamiento*
>
> - *que las obligaciones del apartado 1 (las normas sustantivas sobre seguridad de los datos), tal como las define la legislación del Estado miembro en el que esté establecido el encargado, incumben también a éste.*

Se desarrolla así el principio general enunciado en el artículo 16, con arreglo al cual toda persona que esté bajo la autoridad del responsable del tratamiento, incluido el encargado del tratamiento, deberá abstenerse de procesar datos personales salvo cuando reciba instrucciones del responsable (o cuando lo exija la ley).

En caso de transferencia de datos a terceros países, también intervendrá, en general, más de una entidad. En este caso, se establece una relación entre la entidad que transfiere los datos (el "remitente") y la que los recibe en el otro país (el "receptor"). En tal contexto, una de las finalidades del contrato debe seguir siendo la de determinar el reparto de responsabilidades entre ambas partes en lo que atañe a la protección de datos. No obstante, el contrato no debe limitarse a ello: ha de ofrecer garantías adicionales para los interesados, por el hecho de que el receptor del país no comunitario no está sujeto a una serie de normas obligatorias de protección de datos que proporcionen garantías adecuadas.

3. Objetivo de una solución contractual

En el contexto de las transferencias a terceros países el contrato es, por consiguiente, un medio que permite al responsable del tratamiento ofrecer garantías adecuadas al transmitir datos fuera de la Comunidad (y, por tanto, fuera del ámbito de aplicación de la Directiva y, de hecho, del marco general del Derecho comunitario[9]), a un país en el

[9] El ejercicio del derecho a la protección de los datos personales se ve facilitado, dentro de la Comunidad, por el marco jurídico general, en el que se incluye, por ejemplo, el Acuerdo de Estrasburgo (1997) sobre la transmisión de solicitudes de asistencia jurídica.

que el nivel general de protección no sea suficiente. Para que una cláusula contractual pueda cumplir esta función, debe compensar de manera satisfactoria la ausencia de una protección general adecuada mediante inclusión de los elementos esenciales de la misma que no existen en una situación determinada.

4. Requisitos específicos de una solución contractual

El punto de partida para analizar el significado de la expresión "garantías suficientes" utilizada en el artículo 26.2 es el concepto de "protección adecuada", que ya se desarrolló con cierto detenimiento en el capítulo uno. Éste consiste en una serie de principios básicos para la protección de datos, junto con ciertas condiciones necesarias para asegurar su eficacia.

i) Normas sustantivas de protección de datos

El primer requisito de una solución contractual es, pues, que obligue a las partes de la transferencia a garantizar que se aplique íntegramente el conjunto de principios básicos de protección de datos, desarrollado en el capítulo uno, al tratamiento de los datos transferidos al país no comunitario. Dichos principios básicos son los siguientes:

- principio de limitación de objetivos
- principio de proporcionalidad y de calidad de los datos
- principio de transparencia
- principio de seguridad
- derecho de acceso, rectificación y oposición
- restricciones respecto a transferencias sucesivas a personas ajenas al contrato[10]

Además, en determinados casos deben aplicarse los principios complementarios relativos a los datos sensibles, a la mercadotecnia directa y a las decisiones automatizadas.

El contrato debe estipular minuciosamente la forma en que el receptor de los datos transferidos ha de aplicar los anteriores principios (es decir, deben especificarse los fines de la transferencia, las categorías de los datos, el plazo límite de conservación, las medidas de seguridad, etc.). En circunstancias distintas, por ejemplo cuando exista en el tercer país considerado una ley general de protección de datos similar a la Directiva, es probable que existan otros mecanismos por los que se precise la forma en la que se aplican, en la práctica, las normas sobre protección de datos (códigos de conducta, notificación, función consultiva de la autoridad supervisora). En el caso de un contrato esto no es así. Por tanto, en el supuesto de que la transferencia se base en un contrato, los detalles son imprescindibles.

[10] No deberían permitirse posteriores transferencias de datos personales del remitente a un tercero, a menos que se encuentre un medio de obligar contractualmente a este tercero, proporcionando la misma protección de datos a los interesados.

ii) Efectividad de las normas sustantivas

El capítulo uno fija tres criterios para evaluar la efectividad de un sistema de protección de datos. Estos criterios son la capacidad del sistema para:

- ofrecer un **nivel satisfactorio de cumplimiento** de las normas
- facilitar **apoyo y asistencia a los interesados** en el ejercicio de sus derechos
- y, como elemento clave, proporcionar **vías adecuadas de recurso** a quienes resulten perjudicados en el caso de que no se observen las normas.

Al evaluar la efectividad de una solución contractual, deben aplicarse los mismos criterios. Esto, como es natural, resulta complicado, pero no imposible. Para ello es necesario hallar medios que permitan suplir la falta de mecanismos de supervisión y aplicación, y ofrecer a los interesados, que pueden no ser partes del contrato, apoyo y asistencia y, en última instancia, vías de recurso.

Cada uno de estos aspectos debe examinarse detenidamente. Para facilitar el análisis, se han tomado invirtiendo el orden de los mismos.

Vías de recurso a disposición de los interesados

Ofrecer a una persona un recurso legal (es decir, el derecho a exigir que un árbitro independiente se pronuncie sobre su denuncia y a recibir, si procede, una indemnización), por medio de un contrato entre el "remitente" de los datos y su "receptor", no es cosa fácil. Será, en gran parte, determinante el tipo de normativa contractual elegida como legislación nacional aplicable al contrato. Cabe suponer que, en general, la legislación aplicable será la del Estado miembro en el que esté establecido el remitente. La normativa contractual de algunos Estados miembros permite reconocer derechos a terceros, en tanto que, en otros Estados miembros, esto no es posible.

Como regla general, cuanto más limitadas sean las posibilidades del receptor de elegir los fines, los medios y las condiciones con los cuales puede procesar los datos, mayor será la seguridad jurídica para los interesados. Teniendo en cuenta que nos estamos refiriendo a casos en los que la protección general es inadecuada, la solución óptima consistiría en que el contrato impidiera que el receptor disponga de una autonomía de decisión con respecto a los datos transferidos o a la manera en que se procesarán posteriormente. El receptor vendrá obligado a seguir exclusivamente las instrucciones del remitente y, aun cuando los datos se hayan transferido materialmente fuera de la UE, la capacidad para tomar decisiones con respecto a los mismos seguirá correspondiendo a la entidad establecida en la Comunidad que haya efectuado la transferencia. El remitente seguirá siendo así el responsable del tratamiento, en tanto que el receptor será un simple subcontratista del tratamiento. En tales circunstancias, dado que los datos estarán bajo el control de una entidad establecida en un Estado miembro de la UE, el tratamiento realizado en el tercer país seguirá estando sujeto a la normativa de dicho Estado miembro[11], y además el responsable del tratamiento

[11] En virtud del artículo 4.1.a) de la Directiva 95/46/EC.

continuará respondiendo, en virtud de la legislación de ese Estado, de los daños causados como consecuencia de un tratamiento ilegal de los datos.[12]

Este tipo de solución no dista mucho de la adoptada en el "Acuerdo Interterritorial", por el que se resolvió el caso "Bahncard" de Citibank mencionado con anterioridad. En este caso, el acuerdo contractual fijó pormenorizadamente las condiciones de tratamiento de los datos, en particular las relacionadas con la seguridad de los mismos, excluyendo cualquier otro uso por el receptor. De esta forma, el tratamiento de datos efectuado en el tercer país quedó sujeto a la legislación alemana y se garantizó a los interesados un recurso legal[13].

Como es lógico, habrá casos en los que esta solución no será válida. Es posible que el receptor de los datos no preste simplemente un servicio de tratamiento al responsable radicado en la UE. De hecho, puede, por ejemplo, haber alquilado o comprado los datos para utilizarlos en su propio beneficio y con fines propios. En tales circunstancias, el receptor necesitará libertad para procesar los datos como desee y se convertirá así de pleno derecho en "responsable del tratamiento".

Ante una situación semejante, no es posible confiar en la aplicabilidad automática y continua de la legislación de un Estado miembro y en la permanente responsabilidad por daños del remitente de los datos. Deben idearse otros mecanismos más complejos para ofrecer al interesado un recurso legal adecuado. Como ya se ha mencionado antes, algunos ordenamientos jurídicos permiten conferir derechos a terceros en un contrato, lo cual podría servir para establecer derechos en favor de los interesados en un contrato abierto y público entre el remitente y el receptor. La situación del interesado mejoraría aún más si, dentro del contrato, las partes se comprometieran a someterse a un arbitraje vinculante en el supuesto de que el interesado impugnara su observancia de las disposiciones. Algunos códigos sectoriales autorreguladores incluyen tales mecanismos de arbitraje, por lo que cabe pensar en utilizar los contratos en conjunción con dichos códigos.

Otra posibilidad es que el remitente, por ejemplo en el momento en que obtenga inicialmente los datos del interesado, celebre un contrato independiente con éste en el que se estipule que el remitente responderá de cualesquiera daños y perjuicios que se deriven del incumplimiento, por parte del receptor de los datos, del conjunto de principios básicos acordados para la protección de los datos. De esta forma, el interesado dispondrá de una vía de recurso frente al remitente por las faltas cometidas por el receptor. Correspondería entonces al remitente iniciar una acción contra el receptor por ruptura de contrato, para recuperar las posibles indemnizaciones por daños y perjuicios que se hubiera visto obligado a pagar al interesado.

Esta compleja solución tridireccional es posiblemente más factible de lo que pueda parecer. El contrato con el interesado podría formar parte de las condiciones generales

[12] Véase el artículo 23 de la Directiva 95/46/EC.

[13] No obstante, como la normativa vigente cuando se planteó este caso era anterior a la Directiva, no era automáticamente aplicable a todos los tratamientos de datos que estuviesen bajo el control de un responsable establecido en Alemania. El recurso legal de que disfrutaban los interesados se basaba, en realidad, en la posibilidad que ofrece la legislación alemana sobre contratos de reconocer derechos a terceros.

con arreglo a las cuales un banco o una agencia de viajes, por ejemplo, presta sus servicios a la clientela. Además, tiene la ventaja de ser transparente: el interesado puede así tener pleno conocimiento de los derechos de que disfruta.

Por último, como alternativa al contrato con el interesado, cabría también pensar en la posibilidad de que los Estados miembros adoptasen disposiciones legales por las que se atribuyera a los responsables del tratamiento que transfirieran datos fuera de la Comunidad la responsabilidad continuada por los perjuicios causados como consecuencia de los actos del receptor de la transferencia.

Apoyo y asistencia a los interesados

Una de las mayores dificultades a las que se enfrentan las personas cuyos datos son transferidos a un país extranjero radica en su incapacidad para determinar la raíz de su problema concreto, y, por tanto, en su imposibilidad de juzgar si se han aplicado correctamente las normas sobre protección de datos o si existen motivos para entablar una acción judicial.[14] Por ello, una protección adecuada supone la existencia de algún tipo de mecanismo institucional que haga posible un examen independiente de las denuncias.

Los poderes de control e investigación de la autoridad supervisora de un Estado miembro se limitan al tratamiento de datos efectuado en el territorio de este último.[15] Si los datos se transfieren a otro Estado miembro, el sistema de asistencia mutua entre autoridades de supervisión garantizará que se estudie debidamente la denuncia presentada por una persona en el Estado miembro. Si se transfieren a un tercer país, en la mayor parte de los casos no habrá tal garantía. La pregunta que debemos plantearnos es, pues, qué tipo de mecanismos compensatorios cabría idear en el supuesto de que la transferencia de datos se basara en un contrato.

Una posibilidad sería exigir sencillamente una cláusula contractual que confiriera a la autoridad supervisora del Estado miembro en el que estuviera establecido el remitente de los datos el derecho de inspeccionar el tratamiento realizado por el encargado del mismo en el tercer país. En la práctica, y siempre que se considere oportuno, esta inspección podría efectuarla un agente (por ejemplo, una empresa de auditoría especializada) designado por dicha autoridad. Ahora bien, uno de los problemas que entraña este planteamiento es que la autoridad supervisora no suele ser[16] parte en el contrato, por lo que, en algunos países, le resultaría imposible invocar tal cláusula para tener acceso al tratamiento. Otra posibilidad es que el receptor de los datos en el tercer país se comprometa jurídica y directamente con la autoridad supervisora del Estado miembro afectado a autorizar el acceso de la misma o de un agente designado cuando existan sospechas de que se han incumplido los principios de la protección de datos.

[14] Aun cuando una persona disfrute de determinados derechos en virtud de un contrato, con frecuencia será incapaz de determinar si se ha incumplido el contrato y, en su caso, quién es el responsable. De ahí que sea necesario un procedimiento de investigación, al margen de los procedimientos formales ante los tribunales civiles.

[15] Véase el artículo 28.1 de la Directiva 95/46/EC

[16] La delegación francesa opina que puede haber situaciones en las que la autoridad supervisora sea parte en el contrato.

Dentro de esta cláusula, podría exigirse también que las partes en la transferencia informaran a la autoridad supervisora de cualesquiera quejas recibidas de los interesados. De seguirse este planteamiento, la existencia del citado compromiso sería una condición previa para que pudiera autorizarse la transferencia de los datos.

Sea cual sea la solución elegida, es difícil determinar con certeza si resulta oportuno, práctico, o incluso viable desde el punto de vista de los recursos disponibles, que una autoridad supervisora de un Estado miembro de la UE asuma la responsabilidad de examinar e inspeccionar el tratamiento de los datos efectuado en un tercer país.

Nivel satisfactorio de cumplimiento

Aun cuando el interesado no presente una queja concreta ni tope con dificultades particulares, es necesario poder confiar en que las partes del contrato se atienen realmente a sus cláusulas. El inconveniente de la solución contractual radica en la dificultad de imponer sanciones por incumplimiento suficientemente serias como para producir el efecto disuasorio necesario para crear tal clima de confianza. Incluso en aquellos casos en que siga ejerciéndose un control efectivo sobre los datos desde dentro de la Comunidad, el receptor de la transferencia puede no estar sujeto directamente a ninguna penalización si procesa los datos sin atenerse a lo dispuesto en el contrato. Por el contrario, la responsabilidad recaería en el remitente de los datos establecido en la Comunidad, el cual tendría entonces que entablar una acción legal independiente contra el receptor, para resarcirse de sus posibles pérdidas. Esta forma de responsabilidad indirecta podría no ser suficiente para inducir al receptor a cumplir el contrato al pie de la letra.

En tales circunstancias, es probable que, en la mayor parte de los casos, la solución contractual deba completarse, al menos, con la posibilidad de llevar a cabo de algún modo una verificación externa de las actividades de tratamiento del receptor, como por ejemplo una auditoría efectuada por un organismo de normalización o una empresa especializada.

5. El problema de la legislación aplicable

Una de las dificultades específicas que plantea el enfoque contractual es la posibilidad de que las normas jurídicas generales del tercer país de que se trate obliguen al receptor de la transferencia, en determinadas circunstancias, a comunicar los datos personales a las autoridades (policiales, judiciales o fiscales, por ejemplo) y de que tales requisitos legales prevalezcan sobre todo contrato firmado por el encargado del tratamiento.[17] En lo que respecta a los encargados del tratamiento en la Comunidad, esta posibilidad se contempla en el artículo 16 de la Directiva, con arreglo al cual éstos únicamente pueden procesar datos siguiendo las instrucciones del responsable del tratamiento, *salvo en virtud de un imperativo legal*. No obstante, de acuerdo con la

[17] El alcance de las facultades con que cuentan los poderes públicos para exigir la comunicación de información es también un aspecto importante a la hora de evaluar, de forma más general, la idoneidad de la protección ofrecida en un tercer país.

Directiva, estas notificaciones de datos (que, por su naturaleza, persiguen fines incompatibles con los previstos al recabar los datos) deben limitarse a lo imprescindible para atender a los imperativos de orden público de las sociedades democráticas, enunciados en el artículo 13.1 de la Directiva (véase la nota a pie de página nº 2). El artículo 6 del Tratado de Amsterdam garantiza también la salvaguarda de los derechos fundamentales establecidos en el Convenio Europeo para la Protección de los Derechos Humanos y de las Libertades Fundamentales. En terceros países, es posible que no siempre existan tales restricciones sobre la capacidad de los poderes públicos para exigir de las empresas y otros organismos que operen en su territorio la comunicación de datos personales.

Esta dificultad no es fácil de superar. Demuestra sencillamente las limitaciones de la solución contractual. En algunos casos, un contrato es un instrumento demasiado frágil como para ofrecer garantías suficientes en relación con la protección de datos, y no deberían autorizarse las transferencias de datos a determinados países.

6. Consideraciones de carácter práctico de cara a la utilización de contratos

El anterior análisis demuestra la necesidad de que los contratos contengan cláusulas pormenorizadas y debidamente adaptadas a la transferencia de datos de que se trate. Esta necesidad de fijar minuciosamente la finalidad y las condiciones concretas del tratamiento al que se someterán los datos transferidos no excluye la posibilidad de desarrollar un modelo de contrato tipo, pero supone que todo contrato basado en el mismo se adecúe a las circunstancias particulares del caso.

El análisis realizado indica también que existen serias dificultades de orden práctico para llevar a cabo investigaciones en relación con el incumplimiento de un contrato cuando el tratamiento se efectúa fuera de la UE y cuando el país en cuestión no dispone de ningún tipo de organismo de supervisión. Si se unen ambas consideraciones, podemos concluir que habrá situaciones en las que una solución contractual resulte adecuada, y otras en las que quizá un contrato no pueda ofrecer "garantías suficientes".

Dada la necesidad de que el contrato se adapte rigurosamente a las particularidades de la transferencia, esta solución resultará especialmente adecuada en el caso de transferencias de datos similares y repetitivas. Los problemas relacionados con la supervisión suponen que la solución contractual será más eficaz cuando las partes del contrato sean grandes operadores que estén ya sometidos a inspección y regulación públicas[18]. Las grandes redes internacionales, como las utilizadas para las transacciones con tarjetas de crédito y las reservas en líneas aéreas, presentan ambas características, por lo que, en este caso, los contratos pueden resultar de la máxima eficacia. En tales circunstancias podrían, incluso, completarse con convenios multilaterales que ofrezcan una mayor seguridad jurídica.

Del mismo modo, cuando las partes de la transferencia sean filiales o miembros del

[18] En el caso "Bahncard" de Citibank, la autoridad competente en materia de protección de datos de Berlín colaboró con las autoridades de supervisión bancaria estadounidenses.

mismo grupo de empresas, es probable que aumenten considerablemente las posibilidades de investigar un incumplimiento de contrato, dada la fuerte vinculación existente entre el receptor en el tercer país y la entidad establecida en la Comunidad. Otro caso en el que convendría claramente desarrollar soluciones contractuales es, por tanto, el de las transferencias efectuadas dentro de una misma empresa.

Principales conclusiones y recomendaciones

- En la Comunidad se utilizan contratos para determinar el reparto de responsabilidades en materia de protección de datos entre el responsable del tratamiento y el subcontratista encargado de llevarlo a cabo. Cuando se utilice un contrato en relación con transferencias de datos a terceros países, éste debe abarcar mucho más: ha de ofrecer a la persona a la que se refieran los datos salvaguardas adicionales, puesto que el receptor establecido en el tercer país no está sujeto a una serie de normas obligatorias para garantizar un nivel de protección adecuado.
- Para evaluar la idoneidad de las salvaguardas ofrecidas por una solución contractual debe partirse de la misma base que para evaluar el nivel general de protección en un tercer país. Una solución contractual debe contener todos los principios básicos para la protección de datos y ofrecer los medios necesarios para que pueda velarse por su observancia.
- El contrato debe fijar minuciosamente la finalidad, los medios y las condiciones del tratamiento de los datos transferidos, así como la forma en que se aplicarán los principios básicos de protección de datos. Los contratos que limitan la posibilidad de que el receptor de los datos los procese por cuenta propia de forma autónoma ofrecen una mayor seguridad jurídica. Por consiguiente, en la medida de lo posible, el contrato debería servir para atribuir al remitente de los datos el poder decisorio sobre el tratamiento efectuado en el tercer país.
- Si el receptor disfruta de cierta autonomía en relación con el tratamiento de los datos transferidos, la situación es más compleja y es posible que un simple contrato entre las partes de la transferencia no siempre permita a las personas a las que se refieren los datos ejercer sus derechos. Puede resultar necesario un mecanismo por el cual el remitente establecido en la Comunidad conserve la responsabilidad por los daños que pudieran derivarse del tratamiento llevado a cabo en el tercer país.
- El contrato debería excluir expresamente la posibilidad de que los datos sean transmitidos posteriormente por el receptor a organismos u organizaciones no vinculados por el contrato, a menos que pueda obligarse a terceros, mediante disposiciones contractuales, a respetar los mismos principios de protección de datos.
- La confianza en el respeto de tales principios, una vez efectuada la transferencia, mejoraría si el cumplimiento de los mismos por parte del receptor quedase sujeto a una verificación externa, de la que podría encargarse, por ejemplo, una empresa de auditoría especializada o un organismo de normalización o certificación.
- En el supuesto de que la persona a la que se refieren los datos se encuentre con algún problema, como consecuencia, en su caso, del incumplimiento de las cláusulas sobre protección de datos contenidas en el contrato, resulta, en general, difícil asegurarse de que la queja del interesado se investiga convenientemente.

Las autoridades supervisoras de los Estados miembros experimentarán dificultades de orden práctico a la hora de llevar a cabo tales indagaciones.

- Las soluciones contractuales resultan probablemente más adecuadas para las grandes redes internacionales (tarjetas de crédito, reservas de billetes de avión), que se caracterizan por un elevado volumen de transferencias de datos similares y repetitivas, y por la existencia de un número relativamente reducido de grandes empresas que operan en sectores ya sujetos a supervisión y regulación públicas. Otro caso en el que la utilización de contratos presenta un potencial considerable es el de las transferencias de datos entre distintas sucursales o empresas del mismo grupo.
- Los países en los que las prerrogativas con las que cuentan los poderes públicos para acceder a la información son más amplias de lo que autorizan las normas sobre protección de los derechos humanos aceptadas en el ámbito internacional, no constituyen un destino seguro para las transferencias basadas en cláusulas contractuales.

CAPÍTULO CINCO: EXCEPCIONES AL REQUISITO DE ADECUACIÓN

El artículo 26.1 de la Directiva enuncia un número limitado de situaciones en las que se puede aplicar una excepción al requisito de "adecuación" de las transferencias a terceros países. Estas excepciones, muy circunscritas, se refieren en su mayoría a casos en los que los riesgos para el interesado son relativamente escasos o en los que otros intereses (intereses públicos o del propio interesado) prevalecen sobre los derechos de intimidad del interesado. Como excepciones a un principio general, deben interpretarse restrictivamente. Además, los Estados miembros pueden estipular en la legislación nacional que las excepciones no se apliquen en determinados casos. Este puede ser el caso, por ejemplo, cuando sea necesario proteger a grupos de personas especialmente vulnerables, como los trabajadores o los pacientes.

La primera de estas excepciones abarca casos en los que el interesado ha dado su consentimiento *inequívocamente* a la transferencia prevista. Es importante tener en cuenta que el consentimiento, de acuerdo con la definición del artículo 2.h de la Directiva, debe ser libre, específico e informado. El requisito de información es especialmente relevante porque exige que el interesado esté debidamente informado del riesgo concreto que supone el hecho de que sus datos se transfieran a un país que carece de la protección adecuada. Si no se facilita esta información, dicha excepción no será aplicable. Puesto que el consentimiento debe ser inequívoco, cualquier duda sobre su obtención anularía la aplicabilidad de la excepción. Esto podría significar que en muchas situaciones en que el consentimiento se da por sobreentendido (por ejemplo, porque la persona ha sido informada de una transferencia y no se ha opuesto), la excepción no resultaría aplicable. Sin embargo, la excepción será útil cuando el remitente esté en contacto directo con el interesado y sea posible facilitar sin problemas la información necesaria y obtener un consentimiento inequívoco. Normalmente, éste será el caso en transferencias emprendidas en el contexto de, por ejemplo, la suscripción de seguros.

Las excepciones segunda y tercera abarcan transferencias *necesarias* para la ejecución de un contrato entre el interesado y el responsable del tratamiento (o para la ejecución de medidas precontractuales adoptadas a petición del interesado) o para la celebración o ejecución de un contrato celebrado *en interés del interesado* entre el responsable del tratamiento y un tercero. Aparentemente, estas excepciones son potencialmente bastante amplias, pero, al igual que las excepciones cuarta y quinta comentadas a continuación, es probable que su aplicación en la práctica se vea limitada por la "prueba de necesidad": todos los datos transferidos deben ser necesarios para la ejecución del contrato. Así, si se transfieren datos complementarios que no son esenciales o si el objetivo de la transferencia no es la ejecución del contrato sino otro (mercadotecnia de seguimiento, por ejemplo) se invalidará la excepción. Respecto de las situaciones precontractuales, esta excepción sólo abarca situaciones iniciadas por el interesado (como una solicitud de información sobre un servicio particular) y no las que derivan de propuestas de mercadotecnia planteadas por el responsable del tratamiento.

A pesar de estas salvedades, las excepciones segunda y tercera tienen bastante peso. Es probable que sean aplicables con frecuencia, por ejemplo, en las transferencias necesarias para reservar un billete de avión de un pasajero, o en transferencias de datos

personales necesarios para la transacción de un banco internacional o de un pago con tarjeta de crédito. De hecho, la excepción de contratos "en interés del interesado" (artículo 26.1.c) abarca específicamente la transferencia de datos relativos a los beneficiarios de los pagos bancarios, quienes, aunque sean interesados, es posible que a menudo no sean parte de un contrato celebrado con el responsable del tratamiento que realiza la transferencia.

La cuarta excepción tiene dos vertientes. La primera engloba las transferencias necesarias o legalmente exigidas por un interés público importante. Este aspecto puede abarcar ciertas transferencias limitadas entre administraciones públicas, aunque hay que tener cuidado de no interpretar esta disposición en sentido muy amplio. Para justificar una transferencia no basta con alegar un interés público, debe ser un interés público *importante*. El considerando 58 declara que, normalmente, se incluirán los datos transferidos entre administraciones fiscales o aduaneras, o entre servicios competentes en materia de seguridad social. Es posible que también las transferencias entre organismos supervisores de los servicios financieros se beneficien de la excepción. La segunda vertiente se refiere a las transferencias que tienen lugar en el contexto de litigios o procedimientos judiciales internacionales, concretamente transferencias necesarias para el reconocimiento, ejercicio o defensa de derechos legales.

La quinta excepción se refiere a las transferencias necesarias para proteger los intereses vitales del interesado. Un ejemplo evidente sería la transferencia urgente de datos médicos a un tercer país, en el caso de un turista que, habiendo recibido anteriormente tratamiento médico en la UE, haya sufrido un accidente o haya enfermado gravemente. Sin embargo, es preciso tener en cuenta que el considerando 31 de la Directiva interpreta con bastante concreción el "interés vital" como un interés "esencial para la vida del interesado". Esta interpretación normalmente excluye, por ejemplo, los intereses financieros, de propiedades o familiares.

La excepción sexta y última se refiere a las transferencias realizadas desde registros que por la ley se han destinado a la consulta pública, si se cumplen las condiciones de consulta en cada caso particular. La intención de esta excepción es que cuando un registro de un Estado miembro esté disponible para consulta pública o por personas que demuestren un interés legítimo, el hecho de que la persona con derecho a consultar el registro se encuentre en un tercer país y que la consulta conlleve el hecho de una transferencia de datos, no impida que se le transmita la información. El considerando 58 especifica que es preciso no permitir la transferencia de la totalidad de los datos o categorías de datos contenidos en el mencionado registro en virtud de esta excepción. Dadas estas restricciones, no hay que considerarla una excepción general relativa a la transferencia de datos de registros públicos. Por ejemplo, es evidente que las transferencias masivas de datos de registros públicos con fines comerciales o la búsqueda de datos a disposición del público con el fin de realizar perfiles de personas físicas específicas no se beneficiarían de la excepción.

CAPÍTULO SEIS: CUESTIONES DE PROCEDIMIENTO

El artículo 25 contempla un planteamiento individualizado en el que la evaluación de la adecuación se efectúa en relación con transferencias particulares o con categorías de transferencias particulares. Sin embargo, es evidente que, dado el elevado número de transferencias diarias de datos personales desde la Comunidad y la multitud de agentes que participan en estas transferencias, ningún Estado miembro, sea cual sea el sistema que elija para aplicar el artículo 25[19], podrá asegurar que cada caso se examine en detalle. Evidentemente, ello no implica que no se vaya a examinar ningún caso en detalle, sino que será preciso idear mecanismos que racionalicen el proceso decisorio para un elevado número de casos, permitiendo tomar decisiones, o al menos decisiones provisionales, sin una demora injustificada o sin implicar recursos excesivos.

Esta racionalización es necesaria independientemente de quién toma la decisión, ya sea el responsable del tratamiento, la autoridad supervisora o algún otro organismo creado por el procedimiento del Estado miembro.

i) Uso del artículo 25.6 de la Directiva

Una forma evidente de contribuir a esta racionalización, prevista en la Directiva misma, sería la determinación de que ciertos terceros países aseguran un nivel adecuado de protección. Estas determinaciones serían "sólo orientativas" y, por tanto, sin perjuicio de los casos que pudieran presentar dificultades concretas. No obstante, constituiría una respuesta práctica al problema.

En particular, estas determinaciones proporcionarían cierta seguridad a los agentes económicos en lo referente a los países que podrían considerarse, en general, garantes de un nivel "adecuado" de protección. También ofrecerían un incentivo claro y público a los terceros países que aún siguen organizando y mejorando sus sistemas de protección. Además, una serie de estas determinaciones a escala comunitaria contribuiría al establecimiento de un enfoque coherente de esta cuestión e impediría la publicación "listas blancas" divergentes, y quizás contradictorias, por parte de los gobiernos o autoridades de protección de datos de los diferentes Estados miembros.

Sin embargo, este enfoque no carece de dificultades. La principal es que muchos terceros países no disponen de una protección uniforme en todos los sectores económicos. Por ejemplo, muchos países disponen de legislación de protección de datos en el sector público pero no en el privado. Algunos países, por ejemplo Estados Unidos, tienen leyes específicas para aspectos concretos (informes comerciales y registros de alquiler de vídeos), pero no para otros. Otra de las dificultades se da en países con constituciones federales como EEUU, Canadá y Australia, donde a menudo hay diferencias entre los distintos estados que conforman la federación. Por ello, actualmente parece improbable que muchos terceros países puedan ser considerados garantes de una protección adecuada de una manera general. Cuanto menor sea el

[19] Los Estados miembros pueden establecer diferentes procedimientos administrativos para cumplir sus obligaciones en virtud del artículo 25. Entre ellos, pueden incluirse la imposición de una obligación directa a los responsables del tratamiento y la utilización de sistemas de autorización previa o de verificación de hechos posteriores por parte de la autoridad supervisora.

número de países sobre los cuales puedan hacerse determinaciones positivas, menos útil será este ejercicio, evidentemente, para proporcionar más seguridad a los responsables del tratamiento. Otro riesgo es que algunos terceros países puedan considerar políticamente provocativa o cuando menos dicriminatoria la ausencia de determinación positiva porque esta ausencia podría obedecer tanto al no examen de su caso como a un juicio negativo sobre su sistema de protección de datos.

Una vez sopesados estos diferentes argumentos con detenimiento, el Grupo de Trabajo opina que iniciar el trabajo para llegar a una serie determinaciones con arreglo al artículo 25.6 es, a pesar de todo, una medida útil. Se trataría de un proceso continuo, no de un proceso que dé lugar a una lista definitiva, sino a una lista ampliada y revisada constantemente a la luz de las nuevas situaciones. En principio, una determinación positiva no debería limitarse a países con una legislación de protección de datos horizontal, sino que también debe abarcar sectores específicos donde la protección de datos sea adecuada dentro de un país que en otros sectores ofrezca una protección insuficiente.

Es necesario advertir que el grupo del artículo 29 no desempeña un papel explícito en la toma de decisiones sobre transferencias de datos particulares o en las determinaciones de la "adecuación" previstas en el artículo 25.6. Estas decisiones y determinaciones están sujetas al procedimiento de comitología establecido en el artículo 31. Sin embargo, hay que recordar que uno de los deberes específicos del grupo del artículo 29 es expresar a la Comisión su opinión sobre el nivel de protección en terceros países (véase el artículo 30.i.b). Por tanto, examinar la situación en terceros países particulares y alcanzar una conclusión provisional sobre el carácter adecuado de la protección es algo que entra en el mandato del grupo del artículo 29. Para que las determinaciones positivas resulten de utilidad, es preciso que se promulguen ampliamente una vez confirmadas con arreglo al artículo 25.6. Por otro lado, la determinación de que un país no dispone de la protección adecuada no implica necesariamente que el país esté en la "lista negra" implícita o explícitamente. El mensaje público más bien sería que todavía no se dispone de orientación general relativa al país en cuestión.

ii) Análisis de riesgos de transferencias específicas

Aunque el uso del artículo 25.6 descrito anteriormente sea una valiosa ayuda para el proceso de toma de decisiones en relación con un elevado número de transferencias de datos, habrá muchos casos en los que el tercer país en cuestión no será objeto (total o parcialmente) de una determinación positiva. El modo en que los Estados miembros se ocupen de estos casos puede variar de acuerdo con el modo en que el artículo 25 se incorpore en la legislación nacional (véase la nota a pie de página nº 19). Si se otorga a la autoridad de control la función específica de autorizar las transferencias de datos antes de que ocurran o para realizar una revisión *ex post facto*, el enorme volumen de transferencias evidenciará la necesidad de contemplar un sistema para fijar las prioridades en los esfuerzos de la autoridad de control. Este sistema podría adoptar la forma de un conjunto de criterios aceptados que permitan considerar con prioridad una transferencia concreta o una categoría de transferencias porque supone una amenaza particular para la vida privada.

Evidentemente, el efecto de este sistema no alteraría la obligación de todos los Estados miembros de garantizar que únicamente puedan realizarse transferencias cuando los terceros países aseguren un nivel de protección adecuado. Supondría una orientación para determinar qué casos de transferencia de datos requieren prioritariamente un examen o incluso una investigación y, de ese modo, permitiría que se destinen los recursos disponibles a las transferencias que generen mayor preocupación en cuanto a la protección de los interesados.

El Grupo de Trabajo considera que entre las categorías de transferencias que conllevan un riesgo particular para la vida privada y, por tanto, merecen atención especial, figuran las siguientes:

- las transferencias de ciertas categorías sensibles de datos definidas en el artículo 8 de la directiva;
- las transferencias que comportan el riesgo de pérdida financiera (por ejemplo, pagos con tarjeta de crédito a través de Internet);
- las transferencias que comportan un riesgo para la seguridad personal;
- las transferencias cuyo objetivo sea tomar una decisión que afecta significativamente a la persona (como, por ejemplo, decisiones de contratación o promoción, la concesión de créditos, etc.);
- las transferencias que comportan el riesgo de poner a la persona en una situación embarazosa o de empañar su reputación;
- las transferencias que pueden dar lugar a acciones específicas que constituyan una intrusión significativa en la vida privada de una persona, como las llamadas de teléfono no solicitadas;
- las transferencias repetitivas de volúmenes masivos de datos (por ejemplo, datos transaccionales tratados en redes de telecomunicaciones, Internet, etc.);
- las transferencias que incluyen la recopilación de datos mediante nuevas tecnologías que, por ejemplo, podrían realizarse de forma particularmente encubierta o clandestina (por ejemplo, "cookies" de Internet).

iii) Cláusulas contractuales tipo

Como se ha especificado en el capítulo cuatro, la Directiva contempla la posibilidad de que, incluso cuando el nivel de protección no sea adecuado, un responsable del tratamiento pueda alegar que una transferencia de datos reúne garantías adecuadas gracias a un contrato. El artículo 26.2 de la Directiva permite a los Estados miembros autorizar transferencias en virtud de tales disposiciones contractuales, decisión que después debe notificarse a la Comisión. En caso de oposición a la autorización, la Comisión puede anular o confirmar la decisión, de acuerdo con el procedimiento de comitología establecido en el artículo 31. Además de las autorizaciones de los Estados miembros, el artículo 26.4 de la Directiva permite a la Comisión, también de acuerdo con el procedimiento de comitología establecido en el artículo 31, juzgar si ciertas cláusulas contractuales tipo ofrecen las garantías suficientes. Estos juicios son vinculantes para los Estados miembros.

Dada la manifiesta complejidad y dificultad de estas soluciones contractuales, es evidente que los responsables del tratamiento que contemplen este uso de los contratos

precisan una orientación consensuada. En los Estados miembros, es posible que las autoridades nacionales competentes asuman una mayor responsabilidad en la facilitación de esta orientación, en particular al preparar autorizaciones en el contexto del artículo 26.2. Las autoridades de los Estados miembros y la Comisión deberían cooperar e intercambiar opiniones sobre las cláusulas contractuales que se les sometan. Cuando se presentan propuestas de cláusulas tipo a las autoridades de los Estados miembros o directamente a la Comisión, sería preciso desarrollar un procedimiento para garantizar que también el Grupo de Trabajo examine estas cláusulas, para evitar diferencias en las prácticas nacionales y para garantizar que la Comisión pueda asesorarse debidamente antes de adoptar ninguna decisión en virtud del artículo 26.4.

ANEXO 1

QUÉ IMPLICACIONES PUEDEN TENER EN LA PRÁCTICA LOS ARTÍCULOS 25 Y 26 DE LA DIRECTIVA EN LA TRANSFERENCIA DE DATOS PERSONALES A TERCEROS PAÍSES

Introducción

La parte principal de este documento presenta un enfoque global de la cuestión de las transferencias a terceros países que incluye:

- qué debe entenderse por protección adecuada en el sentido del artículo 25 de la directiva sobre protección de datos;
- una evaluación de los medios alternativos para justificar garantías suficientes a través de soluciones contractuales, como se contempla en el artículo 26.2;
- una evaluación de las excepciones al requisito de protección adecuada previstas en el artículo 26.1.

Sin embargo, un conocimiento de estas cuestiones no sería completo sin un ejemplo del modo en que este enfoque global puede repercutir en las transferencias reales de datos personales. Por tanto, en este anexo se examinan una serie de casos realistas (aunque ficticios) de transferencias de datos en la forma en que, previsiblemente, se examinarán cuando entren en vigor las legislaciones nacionales que aplican la Directiva.

Se exponen tres casos diferentes. En cada caso el primer paso consiste en evaluar si la protección en el país de destino es adecuada en virtud de las legislaciones pertinentes o de la autorregulación efectiva del sector privado. Si no es así, entonces el segundo paso es buscar una solución al problema entre las posibilidades enumeradas en el artículo 26, apartados 1 (excepciones) y 2 (soluciones contractuales). Sólo entonces, si ninguna solución es apropiada, el tercer paso sería bloquear la transferencia.

CASO (1): una transferencia de datos relativos a la solvencia crediticia

Un ciudadano comunitario desea comprar una residencia secundaria en el país A, fuera de la CE, y solicita un crédito a una institución financiera en este país. La institución financiera solicita un informe comercial a una agencia de informes comerciales. La agencia no tiene ningún fichero sobre dicha persona, pero solicita la transferencia del historial crediticio completo de esta persona a su agencia "hermana", la Agencia de Referencia Crediticia del Reino Unido. El país A es un país industrializado y desarrollado, con instituciones democráticas antiguas y estables. El sistema judicial está bien dotado de recursos y funciona eficazmente. Tiene una estructura constitucional federal.

PRIMER PASO: EVALUAR EL CARÁCTER ADECUADO DE LA PROTECCIÓN

Normas aplicables

El responsable del tratamiento receptor está sujeto a una legislación federal que establece normas relativas a la información personal empleada para evaluar riesgos crediticios. Además, el responsable del tratamiento afirma que cumple la política de protección de la intimidad que ha instaurado en su entidad y que ha hecho pública. No hay ninguna ley nacional aplicable ni ningún código de autorregulación industrial.

Evaluación del contenido de las normas aplicables

En primer lugar, es preciso indicar que la comunicación de la agencia de referencia crediticia ubicada en el Reino Unido estaría, como cualquier comunicación dirigida a un responsable del tratamiento establecido en otro lugar distinto del Reino Unido u otro Estado miembro, sujeta a los requisitos normales de la legislación nacional que aplica todos los artículos de la Directiva, excepto los artículos 25 y 26. Esto es importante porque elimina la necesidad de examinar la legalidad de la propia comunicación. Se prestará más atención a la protección ofrecida a los datos una vez transferidos al país A.

Lógicamente, la evaluación del contenido de las normas empezará con la legislación federal. Si se encuentran lagunas, puede estudiarse la norma menos vinculante que es la política de protección de la intimidad para ver si suple esta carencia. A continuación, se ofrece una lista del contenido necesario y un juicio sobre la presencia de este contenido necesario en la legislación o en la política de protección de la intimidad.

- En este contexto, el principio de limitación de objetivos puede centrarse únicamente en el requisito de que todo uso y divulgación secundarios de los datos transferidos no sean incompatibles con el objetivo de su transferencia. La inclusión de los datos en una lista de correo que se vende o alquila en el mercado abierto podría considerarse incompatible, al igual que la divulgación de datos a posibles empleadores o socios comerciales interesados en la solvencia de la persona física

afectada. Sin embargo, es posible que la divulgación de los datos a otros otorgantes de crédito (bancos, empresas de tarjetas de crédito) se considere compatible.

En este caso, la legislación nacional establece un número limitado de objetivos para los cuales la información personal crediticia puede revelarse legítimamente. No obstante, estos objetivos incluyen el "empleo" y la "necesidad comercial legítima relativa a una transacción comercial que implica a la persona física". Este último concepto incluye ciertos usos comerciales de los datos que podrían llevar aparejada la mercadotecnia de productos o servicios, excepto créditos, por parte de terceros.

Por tanto, parece que el objetivo no está suficientemente limitado por la legislación federal y que, en este punto, la protección no es adecuada. La política de protección de la intimidad de la empresa no mejora la situación.

- El principio de transparencia debería permitir al interesado conocer la identidad de la agencia de informes comerciales del país A, así como cualquier nuevo objetivo del tratamiento de los datos. El método para lograrlo debe ser equiparable al previsto en el artículo 11 de la Directiva.

  En este caso, la legislación federal no contiene disposiciones específicas sobre la transparencia que obliguen directamente a la agencia de informes comerciales. Sin embargo, el otorgante de crédito del país A deberá informar a la persona de que se solicitará un informe comercial a la Agencia de Informes Comerciales, aunque no es preciso indicar el nombre y la dirección de la agencia.

  Por tanto, la persona no disfruta de garantía jurídica de que se le vaya a informar sobre el hecho de que la Agencia de Informes Comerciales en cuestión está tratando sus datos. Sin embargo, dado que la agencia no tiene contacto directo con la persona, obligar a la agencia a entrar en contacto con la persona especialmente para informarle parece ser un "esfuerzo desproporcionado", en el sentido del artículo 11 de la Directiva. Por tanto, el nivel de protección en cuanto a la transparencia parece adecuado.

- El principio de proporcionalidad y de calidad incluye varios elementos diferentes. No existe ninguna restricción a la recopilación y tratamiento de datos innecesarios en la legislación federal. Respecto de la duración de almacenaje, hay normas que evitan la divulgación de la información obsoleta (decisiones judiciales de insolvencia con más de 10 años de antigüedad), y que permiten eficazmente la eliminación de esta información. No existen requisitos jurídicos generales para conservar fielmente los datos, aunque cuando una persona que ha solicitado acceder a sus informes comerciales impugne parte de la información, los datos que no puedan verificarse deben borrarse.

  De nuevo, la protección no parece del todo adecuada, y la política de intimidad de la empresa no supera a la legislación federal.

- El principio de seguridad se refleja en la legislación federal mediante un requisito

de adopción de medidas justificadas para evitar la divulgación ilegal. La política de intimidad de la empresa evidencia que se han establecido controles estrictos para evitar el acceso no autorizado a información crediticia y la manipulación de la misma. Estos controles adoptan la forma de dispositivos técnicos (contraseñas, etc.) e instrucciones a empleados cuyo incumplimiento puede dar lugar a expedientes disciplinarios. Todo ello parece garantizar un nivel adecuado de seguridad.

- Los derechos de acceso y rectificación se incluyen en la legislación federal y son equiparables a los encontrados en la Directiva. Cuando se ha denegado el crédito a una persona, el acceso al informe comercial es gratuito. Sin embargo, no hay derecho de oposición aunque una persona puede quejarse ante un organismo federal especializado o ir a los tribunales (véase más adelante), cuando sus derechos jurídicos establecidos en la legislación federal han sido violados.

- Los datos sensibles sobre la salud de la persona física forman parte de los datos transferidos. La legislación federal incluye disposiciones más estrictas para el tratamiento de la información relativa a antecedentes penales, sexo, raza, origen étnico, edad y estado civil, pero no para la información sobre la salud. Sin embargo, en su política de intimidad, la agencia de informes comerciales establece que los datos sobre la salud no se utilizarán para la evaluación crediticia, sino únicamente para revisiones médicas a efectos de empleo o de seguros. En estas dos situaciones, el uso de dichos datos deberá autorizarlo la persona en un impreso de solicitud de empleo o de seguros.

  Por tanto, parece que la protección de los datos sobre la salud de este ejemplo se ha reforzado sustancialmente, aunque no se prevé jurídicamente.

- El uso de los datos para la mercadotecnia directa por parte de la agencia de informes comerciales (y la divulgación de los datos a terceros con el mismo fin) es una cuestión importante en este caso. No existen verdaderos impedimentos jurídicos a este uso, y tampoco requisitos jurídicos que ofrezcan la exclusión voluntaria. Esto es claramente inadecuada, sobre todo porque en este caso la agencia no sólo utilizará los datos (para realizar envíos publicitarios por cuenta de instituciones financieras de concesión de crédito), sino que también se divulgarán a terceros para la mercadotecnia de productos afines y no afines a los servicios financieros, como cortacéspedes o vacaciones.

- Parece que el objetivo de la transferencia sea permitir la adopción de una decisión automatizada sobre la concesión de un crédito al interesado. Por tanto, es preciso que el interesado se beneficie de las garantías complementarias a este respecto. Aunque la legislación federal incluye disposiciones que permiten a la persona afectada impugnar la información contenida en un informe financiero y adjuntar explicaciones al informe si es necesario, no hay disposiciones que permitan recusar y revisar una decisión tomada sobre la base de información errónea o incompleta y modificarla si la recusación está justificada. Este mecanismo permite alterar un informe comercial para evitar problemas futuros, pero no resuelve necesariamente el problema de una decisión crediticia ya adoptada. Esta no retroactividad de la protección jurídica supone una insuficiencia.

- Restricciones a transferencias posteriores de los datos a otro tercer país o a organizaciones de otros sectores dentro del país A no sujetas a las normas establecidas en la legislación federal. No existen estas disposiciones ni en la legislación federal ni en la política de protección de la intimidad de la empresa.

- Ámbito de aplicación de la legislación federal y de la política de protección de la intimidad. Es necesario realizar otra comprobación para garantizar que tanto la legislación como la política de intimidad se aplican a los datos de todas las personas, y no sólo a los datos sobre residentes o nacionales del país A. En este caso, no existen restricciones al ámbito de aplicación.

Evaluación de la eficacia de la protección

La legislación federal en cuestión tiene fuerza de ley y también establece una autoridad pública con ciertas competencias de control externo. Las personas también pueden iniciar procesos judiciales privados al amparo de la legislación para ejercer sus derechos. Sin embargo, la autoridad pública no está claramente obligada a investigar cada una de las quejas, y según algunos analistas no siempre ha sido particularmente activa en la aplicación de la ley. Para las personas, los procesos judiciales privados constituyen medios caros, y a menudo lentos, de asegurar una vía de recurso, en particular cuando el interesado vive en un país diferente al país en el que tiene lugar el procedimiento judicial.

La política de intimidad de la empresa no comprende ningún mecanismo independiente que permita a la persona afectada ejercer sus derechos, pero sí contiene algunas sanciones disciplinarias para empleados que infringen la política. De hecho, varios empleados ya han sido sancionados en relación con infracciones en el pasado.

La combinación de legislación y código interno de protección de la intimidad debe evaluarse en función de los "objetivos" establecidos para los mecanismos de procedimiento. En este caso, las cuestiones clave podrían incluir:

Nivel satisfactorio de cumplimiento general

El estímulo principal de la empresa para cumplir su política de intimidad es el riesgo de la publicidad dañina en la prensa si se descubre el incumplimiento de sus promesas. Además, las personas que trabajan en la empresa pueden estar sujetas a medidas disciplinarias si desobedecen las normas de seguridad.

Sin embargo, estos mecanismos no parecen suficientes para garantizar que en la práctica se cumple la política de protección de la intimidad.

Esta conclusión podría haber sido diferente si:

1) la política de intimidad de la empresa se hubiera plasmado en un código industrial de conducta establecido por la asociación gremial del sector, en virtud del cual toda empresa que violara el código sería expulsada inmediatamente de la

asociación; o

2) un principio general de la legislación permitiera a un organismo público demandar a una empresa que hubiera violado su código de intimidad hecho público por prácticas "desleales y engañosas".

Respecto de la legislación federal, la posibilidad de emprender procesos judiciales privados en el caso de incumplimiento induce al cumplimiento. La perspectiva de ser llevado a los tribunales ejercería cierta influencia disuasoria sobre el responsable del tratamiento. Sin embargo, esta influencia es muy escasa en el método de la verificación directa y externa de los procedimientos de tratamiento de los datos, pues la autoridad pública sólo reacciona cuando se llama su atención sobre un problema a través de una queja o de la prensa, por ejemplo.

Apoyo y ayuda a los interesados

Está claro que existe un organismo público que centraliza las quejas de personas en relación con sus informes comerciales. La investigación de quejas no supone ningún coste para estas personas.

Reparación adecuada

En caso de incumplimiento de las estrictas obligaciones judiciales de la legislación federal, la persona afectada puede obtener reparación de un tribunal. Sin embargo, es un proceso relativamente caro, y el interesado no suele recibir apoyo del organismo público en estos procedimientos judiciales. El tribunal puede ordenar al responsable del tratamiento el pago de una indemnización por daños y perjuicios a dicha persona (si se demuestra que éstos se han producido) y la modificación de sus procedimientos de tratamiento de datos y el contenido del fichero crediticio en cuestión. En cuanto al incumplimiento de los principios de protección de datos englobados únicamente en la política de intimidad, esta reparación no es posible.

Veredicto

1) Algunos principios de protección de datos, establecidos como "principios básicos" en el documento de debate, pueden encontrarse en cierto modo en la legislación federal aplicable al fichero crediticio. Otros principios se encuentran en la política de intimidad. Incluso aunque se reúnan todos, no puede decirse que esté presente el conjunto completo de los "principios básicos", y la presencia de algunos (por ejemplo, el principio de limitación de objetivos) es bastante precaria.

2) Se plantea el problema más general de si la política de intimidad de la empresa es, en cualquier caso, un mecanismo suficientemente eficaz como para tenerlo en cuenta. A menos que la política cuente con un mayor sostén y con una mayor fuerza ejecutiva a través de poderes de control externo conferidos a una asociación industrial o a un órgano público, sus disposiciones son, en gran parte, inejecutables y, por tanto, pueden dejarse de lado.

3) Aunque el organismo público creado para hacer cumplir la legislación federal no disfruta de los mismos poderes que la típica autoridad de protección de datos europea, la legislación proporciona cierta seguridad jurídica, especialmente en el contexto de un sistema judicial que funciona debidamente y de la "cultura de litigio" del país A. La legislación contiene disposiciones claras relativas a los principios de protección de datos que quizá sean los más importantes: el derecho de acceso y rectificación, y algunas limitaciones del objetivo con el que se pueden utilizar los datos.

Conclusión

La protección no es adecuada porque la legislación no abarca suficientes "principios básicos" y porque la política de intimidad, por sí misma, no es un medio eficaz para proporcionar protección. Podría llegarse a un veredicto de "adecuado" si el desarrollo de la legislación incluyera principios como la transparencia y la protección de datos sobre la salud, o si uno de los métodos antes sugeridos (es decir, hacer del cumplimiento una condición para ser miembro de una asociación industrial o facultar a un organismo público para procesar a la empresa por prácticas engañosas si ha incumplido su propia política) dotara de mayor eficacia a la política de intimidad.

SEGUNDO PASO: BÚSQUEDA DE UNA SOLUCIÓN

De las excepciones posibles expuestas en el Artículo 26.1, únicamente la a), el consentimiento del interesado, parece adecuada. La excepción b) referente a las transferencias necesarias por motivos contractuales, no es aplicable porque la parte remitente, la agencia de referencia crediticia ubicada en el Reino Unido, no tiene ninguna relación contractual con el interesado. También es difícil defender el argumento de la necesidad de la transferencia en razón de un contrato "en interés del interesado", como dispone la excepción c).

No obstante, el consentimiento del interesado parece ser una solución relativamente sencilla al problema. El consentimiento podría obtenerlo directamente la agencia de referencia de crédito con sede en el Reino Unido o, en su nombre, la institución financiera radicada en el país A, que podría recabarlo en el impreso de solicitud de préstamo. Independientemente del método elegido, sería preciso informar al interesado del riesgo concreto que supone la transferencia de sus datos a un país que carece de protección adecuada.

Dado que este tipo de transferencia todavía es relativamente raro, la obtención del consentimiento con carácter puntual probablemente sea la solución más práctica. Si las agencias de referencia de crédito y de informes comerciales de todo el mundo empiezan a intercambiar datos de forma más sistemática, podrían ponerse a punto otros acuerdos como las soluciones contractuales o un código de conducta internacional.

CASO (2): transferencia de datos sensibles en el sector aeronáutico

Un ciudadano portugués reserva un billete en una agencia de viajes de Lisboa para volar con una compañía aérea con sede en el país B. Los datos recabados incluyen información sobre la discapacidad del ciudadano y sobre el hecho de que utiliza una silla de ruedas. Los datos se introducen en un sistema informático internacional de reservas y, desde allí, la compañía aérea los descarga en su base de datos sobre pasajeros, ubicada en el país B, donde se conservan indefinidamente. La compañía aérea decide utilizar los datos para prestar un mejor servicio al pasajero en caso de que viaje con ellos en el futuro, así como para la planificación de la gestión interna.[20]

PRIMER PASO: EVALUAR EL CARÁCTER ADECUADO DE LA PROTECCIÓN

Normas pertinentes aplicables

Aunque existe un código de conducta internacional que se aplica a los datos contenidos en un sistema informático de reservas, no hay normas vigentes de protección de los datos contenidos en la base de datos de la compañía aérea con sede en el país B.

Evaluación del contenido de las normas aplicables

No existen normas aplicables.

Evaluación de la eficacia de la protección

No es pertinente.

Veredicto

Los niveles de protección en el país B no son adecuados, particularmente dada la sensibilidad de los datos en cuestión.

SEGUNDO PASO: BÚSQUEDA DE UNA SOLUCIÓN

La transferencia de datos al sistema informático de reservas y su uso por parte de la compañía aérea para prestar el servicio apropiado al pasajero discapacitado en el vuelo en cuestión, es una transferencia necesaria para la ejecución del contrato entre el pasajero y la compañía aérea (artículo 26.1.b). No obstante, la conservación permanente de los datos (que incluyen datos sensibles sobre la salud del interesado) en la base de datos de la compañía aérea no puede justificarse por estos motivos. Por

[20] Este caso es similar, en algunos aspectos, a un caso real surgido en el marco de la legislación sueca y en el que se vieron implicados American Airlines y Lufthansa. El caso todavía está en recurso de apelación.

tanto, es preciso que la transferencia de datos a la compañía aérea sea cubierta por una excepción diferente.

Como con el caso 1), el consentimiento del interesado parecería la mejor solución. El agente de viajes de Lisboa podría obtener el consentimiento en nombre de la compañía aérea. Es recomendable comunicar al interesado los riesgos que pueden derivarse de conservar los datos en el país B, y que la transferencia y la conservación de los datos en la base de datos de la compañía aérea no son necesarias para la reserva del vuelo en cuestión.

CASO (3): transferencia de datos de una lista de direcciones

Una empresa de los Países Bajos está especializada en la elaboración de listas de direcciones. Empleando muchas fuentes distintas de información pública disponibles en los Países Bajos, junto con listas de clientes alquiladas de otras empresas holandesas, las listas resultantes pretenden incluir a personas que se ajusten a un perfil socioeconómico particular. Después, la empresa holandesa vende estas listas a clientes no sólo de los Países Bajos y de la UE, sino también de muchos otros países. Las empresas clientes receptoras utilizan las listas (que incluyen direcciones postales de correo electrónico, números de teléfono y, a menudo, direcciones de correo electrónico) para entrar en contacto con las personas relacionadas con vistas a vender una desconcertante selección de diferentes productos y servicios. Un elevado número de personas incluidas en las listas se han quejado a la autoridad de protección de datos holandesa en relación con las proposiciones comerciales de que han sido objeto.

Normas pertinentes aplicables

Algunas de las empresas que compran las listas de direcciones ofertadas por la empresa holandesa se ubican en países con una legislación general de protección de datos que incluye el derecho de las personas a optar por no ser objeto de estas proposiciones comerciales. Otras se encuentran en países que no disponen de tal legislación, pero son miembros de asociaciones de autorregulación que han elaborado códigos de protección de datos. Otras no están sujetas a ninguna norma de protección de datos.

Evaluación del contenido de las normas aplicables

Este caso por sí solo exigiría la evaluación de un elevado número de diferentes leyes y códigos. Si la empresa ubicada en los Países Bajos tiene la intención de mantener la actividad de venta o alquiler de sus listas a empresas ubicadas en cualquier país del mundo, entonces necesariamente habrá situaciones donde el nivel de protección no sea adecuado.

SEGUNDO PASO: BÚSQUEDA DE UNA SOLUCIÓN

En este ejemplo, debido a que los datos se recaban de fuentes públicas y sin establecer ningún contacto directo con el interesado, sería muy problemático para la empresa de los Países Bajos recabar el consentimiento de cada uno de los interesados para incluirlo en las listas de direcciones. Por ello, es improbable que alguna de las excepciones del artículo 26.1 sea de utilidad.

La empresa holandesa tiene dos posibilidades, que podrían utilizarse como alternativas o juntas. En primer lugar, limitar su actividad comercial con las listas de direcciones a empresas ubicadas en países que aseguren inequívocamente la protección adecuada en virtud la ley o de instrumentos de autorregulación eficaces. A la hora de adoptar esta

decisión, la empresa puede obtener orientación en cualquier "lista blanca" disponible.

La segunda posibilidad consiste en solicitar compromisos contractuales de todos los clientes (o al menos de los radicados en países "no adecuados") en relación con la protección de los datos transferidos. Estos acuerdos contractuales deberían seguir el consejo expuesto en el capítulo cuatro del documento principal. En particular, es preciso que su objetivo sea la creación de una situación en la cual la empresa de los Países Bajos se responsabilice, con arreglo a la legislación holandesa, de toda violación de los principios de protección de datos causada por las acciones del cliente al cual se transfirió la lista de direcciones.

Esta solución contractual, si se aplica debidamente, permitiría superar la efectiva barrera a la actividad comercial que la falta de protección adecuada de datos crea en determinados terceros países.

Bruselas, 24 de julio de 1998

Por el Grupo de Trabajo

El Presidente

P.J. HUSTINX