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

XV D/5020/97 - ES 2
WP 4

GRUPO DE TRABAJO DE PROTECCIÓN DE LAS PERSONAS EN LO QUE RESPECTA AL TRATAMIENTO DE DATOS PERSONALES

Primeras orientaciones sobre la transferencia de datos personales a países terceros - Posibles formas de evaluar la adecuación

Documento de debate adoptado por el Grupo de Trabajo el 26 de junio de 1997

Reflexiones sobre la transferencia de datos personales a países terceros - posibles vías para la evaluación de la adecuación

1. Introducción

Este documento no tiene por objetivo tratar todas las cuestiones que surgen en relación con la Directiva respecto a la transferencia de datos personales a países terceros, sino que más bien pretende centrarse en la cuestión de evaluar la *adecuación* en el sentido de los apartados 1 y 2 del artículo 25. El alcance de las excepciones al requisito del "nivel de protección adecuado" del apartado 1 del artículo 26 no se consideran en este documento. La hipótesis de trabajo es que la formulación de estas exenciones es bastante limitada, y que probablemente habrá un gran número de casos que caigan fuera de su alcance y que deban por lo tanto ser objeto de una evaluación de su adecuación. El Grupo de Trabajo examinará el alcance exacto de estas excepciones en el futuro.

No hay que olvidar que el término "adecuado" también se utiliza en el apartado 2 del artículo 26, que prevé la posibilidad de soluciones ad hoc, especialmente de naturaleza contractual, para situaciones donde existe una falta de protección adecuada con arreglo al apartado 2 del artículo 25. Desde el punto de vista procedimental no obstante, la Directiva trata estos casos de forma muy diferente. Mientras que en virtud del artículo 25 los Estados miembros deberán notificar a los demás Estados miembros y a la Comisión los casos donde *no* se garantiza una protección adecuada y por lo tanto se bloquea la transferencia, en virtud del artículo 26 la obligación se ve invertida, y los Estados miembros deberán informar a la Comisión y a los demás Estados miembros acerca de las autorizaciones que concedan. Ello refleja el hecho de que estas soluciones contractuales tienen problemas inherentes, tales como la dificultad del sujeto de los datos para hacer valer sus derechos en virtud de un contrato del cual no es parte, y que sólo son adecuadas en circunstancias específicas y probablemente relativamente excepcionales. El Grupo de Trabajo examinará separadamente las circunstancias donde pueda ser adecuado establecer soluciones contractuales ad hoc, y establecerá principios en cuanto a la posible forma y contenido de dichas soluciones en un futuro. En esencia, este trabajo extraerá probablemente ideas expuestas en este documento, dado que el control de la *adecuación* cae tanto dentro del ámbito del apartado 2 del artículo 26 como de los apartados 1 y 2 del artículo 25.

2. Cuestiones procedimentales

El artículo 25 prevé un enfoque caso por caso en el cual la evaluación de la adecuación se realiza para cada transferencia individual o categorías individuales de transferencias. No obstante, está claro que dado el gran número de transferencias de datos personales que salen de la Comunidad diariamente y la multitud de participantes en dichas transferencias, ningún Estado miembro, independientemente del sistema que escoja para aplicar el apartado 1 del artículo 25[1], podrá garantizar que se examina detalladamente cada uno de

[1] Los Estados miembros podrán establecer distintos procedimientos administrativos para cumplir sus obligaciones en virtud del artículo 25. Éstas podrán consistir en imponer una obligación directa a los

los casos. Ello no significa, por supuesto, que no examinará detalladamente ningún caso, sino que será necesario desarrollar mecanismos que racionalicen el procedimiento de toma de decisiones para un gran número de casos, permitiendo que se adopten decisiones, o al menos decisiones provisionales, sin excesiva dificultad o excesivos costes. Esta racionalización es necesaria independientemente de quien tome la decisión, ya sea el controlador de datos, la autoridad de control o algún otro organismo establecido por los procedimientos de los Estados miembros.

(i) Listas blancas

Un mecanismo evidente para esta racionalización sería la elaboración de una "lista blanca" de países terceros que puede presumirse que garantizan un nivel de protección adecuado. Esta lista podría ser "provisional" o "únicamente orientativa", y por lo tanto sin perjuicio de casos específicos que puedan presentar dificultades concretas. No obstante, para ser coherentes con el enfoque global del artículo 25, sería importante basar cualquier decisión relativa a la inclusión de un país en una lista blanca en casos individuales, antes que una evaluación simplificada y abstracta de un texto jurídico. Una vez se hayan considerado casos representativos de transferencias a un país tercero en concreto, y se haya estimado en cada una de ellas que la protección otorgada era adecuada, el país en cuestión podrá incluirse en la "lista blanca".

Una dificultad de este enfoque es que muchos países terceros no tienen una protección uniforme en todos los sectores económicos. Por ejemplo, muchos países tienen legislación sobre protección de datos en el sector público pero no en el privado. En Estados Unidos la situación es aún más compleja, dado que existen leyes específicas para áreas concretas, tales como la información sobre créditos y los registros de alquiler de vídeos pero no en otras. Una dificultad añadida se dará en países que tienen constituciones federales, tales como Estados Unidos y Canadá, donde a menudo existen diferencias entre los distintos países que componen la federación. En vista de esta dificultad, será necesario proceder con cautela al decidir si la protección otorgada a una transferencia de datos concreta es representativa de la totalidad del país o únicamente de un sector o Estado concreto. Nada impediría la inclusión parcial en la lista blanca de un país tercero, y en efecto, respecto a las transferencias de datos procedentes de España, ya se realizan distinciones con arreglo a la ley nacional entre países que garantizan una protección transfronteriza y los que garantizan una protección únicamente en el sector público.

También surge la cuestión de quién debería tomar la decisión relativa a la inclusión en dicha lista. Hay que señalar a este respecto que el Grupo del artículo 29 no tiene una función específica relativa a la toma de decisiones sobre transferencias de datos concretas. Esta función la realizan los Estados miembros en primera instancia, y posteriormente la Comisión en virtud del procedimiento de comitología establecido en el artículo 31. No obstante, como se ha señalado anteriormente, cualquier trabajo del Grupo iría destinado a proporcionar una orientación relativa a una amplia gama de casos, y no necesariamente a determinar un caso concreto. También hay que recordar que una de las misiones específicas del Grupo del artículo 29 es emitir dictámenes destinados a la Comisión respecto del nivel de protección en los países terceros. Corresponde por lo tanto al Grupo del artículo 29 examinar la situación de países terceros concretos a la luz de casos

---

controladores de datos y/o desarrollar sistemas de autorización previa o comprobación factual posterior por parte de la autoridad de control.

individuales, y adoptar una opinión provisional en cuanto a la adecuación de la protección. Cuando dichas decisiones sean positivas, los países en cuestión podrán formar parte de la lista blanca. La lista podrá distribuirse ampliamente y ser utilizada por controladores de datos, autoridades de control y Estados miembros como guía para sus propias decisiones.

Cuando un país no esté incluido en la lista blanca, ello no significa que dicho país esté incluido implícitamente en una "lista negra", sino que aún no se dispone de una orientación general relativa a dicho país. El establecimiento de una lista negra explícita de países, incluso a efectos orientativos, sería muy delicada políticamente.

(ii) Análisis de riesgo de transferencias específicas

Si bien el establecimiento de una lista blanca provisional de países terceros supondría una valiosa ayuda al proceso de toma de decisiones respecto de un gran número de transferencias de datos, seguirá habiendo no obstante muchos casos donde el país tercero en cuestión no figure en la lista blanca. La forma en que los Estados miembros traten estos casos podrá variar dependiendo de la forma en que se incorpore el artículo 25 al Derecho nacional (véase la nota de pie de página de la página anterior). Si se otorga una función específica a la autoridad de control bien para autorizar transferencias de datos antes de que tengan lugar o para realizar un control factual ex post, el gran volumen de transferencias afectadas puede significar que será necesario prever un sistema destinado a jerarquizar los esfuerzos de la autoridad de control. Tal sistema podría adoptar la forma de un conjunto acordado de criterios que permitirían considerar que una transferencia concreta o una categoría concreta de transferencias suponen una amenaza concreta a la vida privada.

El efecto de dicho sistema no sería modificar la obligación de cada Estado miembro de garantizar que sólo se permitirá la realización de aquellas transferencias para las que los países terceros garanticen un nivel de protección adecuado. El hecho de que una transferencia no plantee una amenaza concreta no suprime el requisito básico del artículo 25 de garantizar una protección adecuada. No obstante, el nivel de riesgo respecto de los sujetos de los datos que conlleva la transferencia proporcionará una útil orientación para ayudar a determinar la naturaleza concreta de lo que se considera una "protección adecuada". El sistema también constituirá una orientación respecto de los casos de transferencia de datos que deberán considerarse "prioritarios" para su examen o investigación, permitiendo así que los recursos utilizados para "controlar el sistema" se dirijan hacia aquellas transferencias que supongan una mayor preocupación en cuanto a la protección de los sujetos de los datos.

El Grupo de Trabajo elaborará un documento más específico y detallado señalando las categorías de transferencias que considere plantean riesgos específicos a la vida privada. No obstante, es probable que dichas categorías incluyan las siguientes:

- aquellas transferencias que afecten a categorías sensibles de datos, definidas en el artículo 8 de la Directiva
- transferencias que supongan un riesgo de pérdida financiera (por ejemplo, pagos con tarjetas de crédito por Internet)
- transferencias que supongan un riesgo a la seguridad personal
- transferencias realizadas a efectos de tomar una decisión que afecte significativamente al individuo (tales como decisiones de contratación o promoción, concesión de créditos, etc.)
- transferencias que supongan un riesgo de perjudicar o manchar la reputación de un individuo
- transferencias que puedan resultan en acciones concretas que constituyan una considerable invasión de la vida privada de los individuos, tales como llamadas telefónicas no deseadas
- transferencias repetitivas que supongan grandes volúmenes de datos (tales como datos de transacciones procesados en redes de telecomunicaciones, Internet, etc.)
- transferencias que supongan la recogida de datos de forma especialmente cubierta o clandestina (por ejemplo, "chivatos" (cookies) Internet)

3. ¿Qué constituye una "protección adecuada"?

El objeto de la protección de datos es proporcionar protección a los individuos cuyos datos son procesados. Esto se logra típicamente mediante una combinación de derechos para el sujeto de los datos y de obligaciones para aquellos que procesan los datos o que ejercen un control sobre dicho tratamiento. Los derechos y obligaciones establecidos en la Directiva 95/46/CE se basan en los establecidos en el Convenio del Consejo de Europa nº 108 (1981), que a su vez son parecidos a los incluidos en las directrices de la OCDE (1980) o las orientaciones de la ONU (1990). Resultaría por lo tanto que existe un grado de consenso en cuanto al contenido de las normas de protección de datos, que se extiende más allá de los 15 Estados de la Comunidad.

No obstante, las normas sobre protección de datos únicamente contribuyen a la protección de individuos si se aplican en la práctica. Es por lo tanto necesario considerar no sólo el contenido de las normas aplicables a los datos personales transferidos a un país tercero, sino también los mecanismos procedimentales existentes destinados a garantizar la eficacia de dichas normas. En Europa, históricamente la tendencia ha sido que las normas de protección de datos se materialicen en la ley, lo que supone una posibilidad de sancionar su incumplimiento y de conceder a los individuos el derecho a la reparación. Además, dichas leyes incluyen generalmente mecanismos procedimentales adicionales, tales como el establecimiento de autoridades de control con funciones de seguimiento e investigación de denuncias. Estos aspectos procedimentales se reflejan en la Directiva 95/46/CE, con sus disposiciones sobre responsabilidad, sanciones, recursos, autoridades de control y notificación. No obstante, fuera de la Comunidad es menos frecuente hallar estos medios procedimentales para garantizar el cumplimiento de las normas de protección de datos. Las partes del Convenio 108 están obligadas a reflejar en una ley los principios de protección de datos, pero no existe un requisito respecto de mecanismos adicionales tales como una autoridad de control. Las orientaciones de la OCDE, no obstante, incluyen

únicamente el requisito de que "deberán tenerse en cuenta" en la legislación nacional, por lo que no garantizan medios procedimentales para garantizar que las orientaciones redunden en una protección efectiva para los individuos. Las últimas orientaciones de la ONU, incluyen no obstante disposiciones sobre supervisión y sanciones, que reflejan una creciente concienciación mundial respecto de la necesidad de aplicar correctamente las normas sobre protección de datos.

Con estos antecedentes está claro que cualquier análisis significativo de la protección adecuada debe comprender dos elementos básicos: el contenido de las normas aplicables, y los medios de garantizar su aplicación efectiva.

Utilizando la Directiva 94/46/CE como punto de partida, y teniendo en cuenta las disposiciones de otros textos internacionales sobre protección de datos, debería ser posible llegar al núcleo del "contenido de los principios de la protección de datos" y los requisitos de aplicación y procedimentales, cuyo cumplimiento debería considerarse como un requisito mínimo para que la protección pueda considerarse eficaz. Esta lista mínima no debería ser inmutable. En algunos casos será necesario realizar añadidos a la lista, mientras que en otros casos deberá ser posible reducir la lista de requisitos. El grado de riesgo que plantea la transferencia al sujeto de los datos (véase la anterior sección 2(ii)) será un factor importante para determinar los requisitos exactos de un caso en concreto. A pesar de esta salvedad, la compilación de una lista básica de condiciones mínimas constituye un útil punto de partida para cualquier análisis.

(i) Principios del contenido

Se ha sugerido que los principios básicos que deberán incluirse son los siguientes:

1) **El principio de limitación del propósito** - los datos deberán tratarse para un propósito específico y utilizarse o comunicarse posteriormente únicamente en la medida en que ello no sea incompatible con el propósito de la transferencia. Las únicas excepciones a esta norma serían las necesarias en una sociedad democrática por una de las razones establecidas en el artículo 13 de la Directiva.

2) **La calidad de los datos y el principio de proporcionalidad** - los datos deberán ser exactos y, cuando sea necesario, actualizados. Los datos deberán ser adecuados, relevantes y no excesivos en relación al objeto por el que se transfieren o se tratan.

3) **El principio de transparencia** - deberá proporcionarse a los individuos información respecto al propósito del tratamiento y la identidad del controlador de datos en el país tercero, así como cualquier otra información siempre que sea necesario para garantizar la equidad. Las únicas excepciones permitidas deberán ser acordes con el apartado 2 del artículo 11 y el artículo 13 de la Directiva.

4) **El principio de seguridad** - el controlador de los datos deberá adoptar medidas de seguridad técnicas y organizativas adecuadas a los riesgos que presente el tratamiento. Cualquier persona que actúe bajo la autoridad del controlador de datos, incluidos los responsables del tratamiento, no deberán tratar los datos salvo por instrucción del controlador.

5) **Los derechos de acceso, rectificación y oposición** - el sujeto de los datos deberá tener derecho a obtener una copia de todos los datos relativos a él o ella que sean tratados, y un derecho a rectificar dichos datos cuando resulten inexactos. En

determinadas situaciones el sujeto también deberá poder oponerse al tratamiento de los datos relativos a él/ella. Las únicas excepciones a estos derechos deberán ser acordes con el artículo 13 de la Directiva.

6) **Restricciones a las transferencias sucesivas a otros países terceros** - las transferencias sucesivas de datos personales a partir del país tercero de destino a otro país tercero deberán permitirse únicamente cuando el segundo país tercero también garantice un nivel adecuado de protección. Las únicas excepciones permitidas deberán ser acordes con el artículo 26 de la Directiva.

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

1) **Datos sensibles** - cuando se trate de categorías de datos "sensibles" (los que figuran en el artículo 8) deberán adoptarse medidas de protección adicionales, tales como el requisito de que el sujeto de los datos otorgue su consentimiento explícito para el tratamiento.

2) **Marketing directo** - cuando los datos se transfieran a efectos de marketing directo, el sujeto de los datos deberá tener la opción de retirar sus datos a dichos efectos en cualquier momento.

3) **Decisión individual automatizada** - cuando el objeto de la transferencia sea adoptar una decisión automatizada en el sentido del artículo 15 de la Directiva, el individuo deberá tener derecho a conocer la lógica por la que funciona esta decisión, y deberán adoptarse otras medidas para proteger los intereses legítimos de los individuos.

(ii) Mecanismos procedimentales y de aplicación

En Europa existe un amplio consenso respecto a que los principios de protección de datos deberán encarnarse en una ley. También existe un amplio acuerdo acerca de que un sistema "de control externo" en forma de una autoridad independiente es una característica necesaria para un sistema de aplicación de la protección de datos. No obstante, no es suficiente manifestar simplemente, sin ningún razonamiento o justificación, que estos dos rasgos son de alguna forma inherentemente necesarios para que la protección sea adecuada. Ello sería establecer criterios puramente formales para la evaluación de esta cuestión.

Se ha sugerido que un mejor punto de partida es tratar de identificar los objetivos subyacentes de un sistema procedimental de protección de datos, y sobre esta base juzgar la variedad de diferentes mecanismos procedimentales judiciales y no judiciales que se utilizan en los países terceros, en términos de su capacidad para cumplir estos objetivos.

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

1) Proporcionar un **buen nivel de cumplimiento de las normas**. (Ningún sistema puede garantizar un cumplimiento al 100%, pero hay sistemas mejores que otros). Un buen sistema se caracteriza generalmente por un elevado nivel de concienciación entre los controladores de datos respecto de sus obligaciones, y entre los sujetos de los datos respecto de sus derechos y su forma de ejercicio. La existencia de sanciones efectivas y disuasorias es importante para garantizar el respeto por las normas, así como los sistemas de comprobación directa por parte de las autoridades, auditores o funcionarios independientes responsables de la protección de datos.

2) Proporcionar **apoyo y ayuda a los sujetos de datos individuales** en el ejercicio de sus derechos. Los individuos deberán ser capaces de ejercer sus derechos de forma rápida y eficaz, y sin costes prohibitivos. Para ello deberá existir algún tipo de mecanismo institucional que permita una investigación independiente de las denuncias.

3) Proporcionar una **reparación adecuada** a las partes perjudicadas cuando no se cumplan las normas. Esto es un elemento clave que debe contar con un sistema de arbitraje independiente que permita pagar una compensación e imponer sanciones cuando sea oportuno.

4. Aplicación de la teoría en la práctica

(i) Países que han ratificado el Convenio 108 del Consejo de Europa

El Convenio 108 es el único instrumento existente de Derecho internacional en el ámbito de la protección de datos, aparte de la Directiva. La mayoría de las partes del Convenio son también Estados miembros de la Unión Europea (ya lo han ratificado los 15 Estados miembros) o países, tales como Noruega e Islandia, que están vinculados en cualquier caso por la Directiva en virtud del Acuerdo del Espacio Económico Europeo. No obstante, Eslovenia también ha ratificado el Convenio, y otros países terceros, tales como Suiza, podrán hacerlo en un futuro próximo. Reviste por lo tanto un interés mayor que el puramente académico examinar si los países que han ratificado el Convenio puede considerarse que proporcionan un nivel de protección adecuado en el sentido del artículo 25 de la Directiva.

Dicho examen debería realizarse, tal y como se señala en la sección 2 de este documento, examinando diversos casos específicos. No obstante, resulta útil como punto de partida examinar el texto del propio Convenio a la luz del término teórico "protección adecuada" expuesto anteriormente en este documento.

Por lo que respecta al contenido de los principios básicos, puede decirse que el Convenio incluye las cinco primeras de las "seis condiciones mínimas"[2]. El Convenio también incluye el requisito de protección adecuada para los datos sensibles, que debería ser un requisito para la adecuación por lo que a estos datos se refiere.

El elemento que falta en el Convenio en cuanto al contenido de sus normas substantivas es la falta de restricciones de las transferencias hacia países que no forman parte del mismo. Ello crea el riesgo de que un país miembro del Convenio 108 pueda ser utilizado como "puerto de estacionamiento" en una transferencia de datos procedente de la Comunidad hacia un país tercero con niveles de protección totalmente inadecuados.

El segundo aspecto de "la protección adecuada" afecta a los mecanismos de procedimiento existentes para garantizar la eficacia de los principios básicos. El Convenio exige que estos principios se incorporen al Derecho nacional y que se establezcan las sanciones y recursos adecuados para los casos de violación de los mismos. Ello sería suficiente para garantizar un nivel razonable de cumplimiento de las normas y una

---

[2] Pueden caber ligeras dudas sobre el principio de transparencia. El artículo 8 a del Convenio puede no equivaler al derecho *activo* de proporcionar información, que constituye la esencia de los artículos 10 y 11 de la Directiva.

reparación adecuada a los sujetos de los datos cuando no se cumplan las normas (objetivos 1 y 3 de un sistema de aplicación de la protección de datos). No obstante, el Convenio no obliga a las partes contratantes a establecer mecanismos institucionales que permitan una investigación independiente de las denuncias, aunque en la práctica los países que han ratificado el Convenio lo han hecho por regla general. Esto constituye un punto débil por cuanto sin dichos mecanismos institucionales no podrá garantizarse una ayuda adecuada a los sujetos de datos individuales en el ejercicio de sus derechos (objetivo 2).

Este breve análisis parece indicar que las transferencias de datos personales a países que han ratificado el Convenio 108 pueden considerarse permitidas en virtud del apartado 1 del artículo 25 de la Directiva, siempre que:

- el país en cuestión cuente también con mecanismos institucionales adecuados, tales como una autoridad de control independiente con poderes adecuados, y
- el país en cuestión sea el destino final de la transferencia y no un país intermedio por el que transiten los datos.

Evidentemente, éste es un examen simplificado y superficial del Convenio. Los casos específicos de transferencia de datos a países del Convenio pueden plantear nuevos problemas que no se consideran aquí.

(ii) Otros casos

Claramente, la gran mayoría de las transferencias de datos procedentes de la Unión Europea se realizan a países terceros que no han ratificado el Convenio 108. En estos casos, donde no es aplicable ningún instrumento vinculante de Derecho internacional, no existe alternativa salvo volver al enfoque básico de este documento, es decir, sacar conclusiones sobre la adecuación del nivel de protección de un país tercero sobre la base de varios casos concretos. A veces, una evaluación de una transferencia de datos concreta puede considerarse válida para amplias categorías de casos análogos. El análisis de transferencias muy representativas facilitará el desarrollo de una lista blanca provisional de países o de sectores dentro de los países.

Parece que en virtud de la Directiva serían posibles tres tipos de transferencia:

1) una comunicación de datos personales por un controlador de datos basado en la Comunidad a otro controlador de datos establecido en un país tercero
2) una comunicación de datos personales por un controlador de datos establecido en la Comunidad a un procesador de un país tercero que procese en nombre de un controlador establecido en la Comunidad
3) una comunicación de datos personales por parte de un sujeto de datos establecido en la Comunidad a un controlador de datos establecido en un país tercero.

Los principios fundamentales establecidos en la sección 3 podrán aplicarse de forma diferente a estos tres tipos distintos de transferencia. Por ejemplo, la situación clásica donde un controlador de datos establecido en la Comunidad realice una transferencia a otro controlador de datos establecido en un país tercero es por su propia naturaleza muy diferente a un caso donde los datos sean directamente recogidos a los sujetos de datos

individuales de la Comunidad por el controlador de datos establecido fuera de la Comunidad, por teléfono o por Internet.