GRUPO DE TRABAJO DE PROTECCIÓN DE DATOS DEL ARTÍCULO 29

00062/10/ES
GT 173

Dictamen 3/2010 sobre el principio de responsabilidad

Adoptado el 13 de julio de 2010

RESUMEN

Los principios y obligaciones de protección de datos en la UE no se reflejan suficientemente en medidas internas y prácticas concretas. Si la protección de datos no forma parte de los valores compartidos y las prácticas de una organización y no se asignan expresamente responsabilidades por la misma, se corre un gran peligro de que no se respeten adecuadamente y de que sigan produciéndose desajustes en la protección de datos.

Para fomentar en la práctica la protección de datos, el marco normativo de la UE precisa de herramientas complementarias. El presente Dictamen pretende asesorar a la Comisión sobre una modificación al efecto de la Directiva de Protección de Datos. En especial, el presente Dictamen presenta una propuesta concreta de introducción el principio de responsabilidad que reclamaría de los responsables del tratamiento de datos la aplicación de medidas apropiadas y eficaces que garantizaran la observancia de los principios y obligaciones que dispone la Directiva y la demostraran cuando se lo solicitaran las autoridades de control. Ello contribuiría a que la protección de datos progresara «de la teoría a la práctica» y ayudaría a las autoridades de protección de datos en sus funciones de supervisión y ejecución.

El Dictamen contiene sugerencias para garantizar que el principio de responsabilidad aporte seguridad jurídica, dejando a la vez margen para su modulación progresiva (que permita disponer la aplicación de medidas concretas en función del riesgo del tratamiento y de la naturaleza de los datos). Trata también del impacto previsible de dicho principio en otras materias, incluyendo las transferencias internacionales de datos, los requisitos de notificación, las sanciones y, en su caso, también el desarrollo de programas o sellos de certificación.

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

Creado por la Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre de 1995,

Vistos el artículo 29 y el artículo 30, apartado 1, letra a) y apartado 3, de dicha Directiva, y el artículo 15, apartado 3, de la Directiva 2002/58/CE del Parlamento Europeo y del Consejo, de 12 de julio de 2002,

Visto su reglamento interno,

HA ADOPTADO EL SIGUIENTE DICTAMEN:

1. INTRODUCCIÓN

1. La protección de datos debe progresar «de la teoría a la práctica». Los requisitos jurídicos deben traducirse en medidas concretas de protección de datos. Para fomentar prácticamente la protección de datos, el marco jurídico de protección de datos de la UE precisa mecanismos complementarios. En los debates sobre el futuro marco europeo y global de protección de datos, se han sugerido mecanismos basados en la responsabilidad como manera de incitar a los responsables del tratamiento de datos a aplicar instrumentos prácticos de protección eficaz de los datos.

2. En su Documento sobre «El Futuro de la Privacidad» (WP 168) de diciembre de 2009, el Grupo de Trabajo del artículo 29 manifestaba su opinión de que el vigente marco jurídico no había logrado garantizar que los requisitos de protección de datos se tradujeran en mecanismos eficaces que aportaran una auténtica protección. Para mejorar la situación, el Grupo de Trabajo del artículo 29 proponía que la Comisión se planteara mecanismos basados en la responsabilidad, haciendo especial hincapié en la posibilidad de incluir un principio de «responsabilidad» en la Directiva de protección de datos revisada[1]. Este principio reforzaría el papel del responsable del tratamiento de datos aumentando sus competencias.

[1] Para abordar este problema, sería conveniente introducir en el marco general un principio de responsabilidad. Con arreglo a este principio, los responsables del tratamiento de datos tendrían obligación de emprender las medidas necesarias para garantizar la observancia de los principios y obligaciones materiales de la Directiva vigente en el tratamiento de datos personales. Dicha disposición reforzaría la necesidad de poner a punto políticas y mecanismos que hicieran efectivos los principios y obligaciones materiales de la Directiva vigente. Serviría para reforzar la necesidad de adoptar medidas eficaces que llevaran a una aplicación interna efectiva de los principios y obligaciones materiales que contiene la Directiva vigente. Además, el principio de responsabilidad exigiría que los responsables del tratamiento de datos dispusieran de los mecanismos internos necesarios para demostrar el cumplimiento de las medidas adoptadas para garantizar el cumplimiento a los interesados externos, incluidas las autoridades nacionales de protección de datos. La consiguiente necesidad de demostrar la adopción de medidas adecuadas para garantizar el cumplimiento facilitará grandemente la ejecución de las normas aplicables (WP168, apartado 79. Para mayor información, véanse también los apartados 74-78).

3. Por decirlo con pocas palabras, un principio reglamentario de responsabilidad requeriría expresamente que los responsables del tratamiento de datos aplicaran medidas adecuadas y eficaces para poner en práctica los principios y obligaciones de la Directiva y demostrar este extremo cuando se les solicitara. En la práctica, ello se traduciría en programas modulables tendentes a ejecutar los principios de protección vigentes (a veces llamados «programas de cumplimiento»). Como complemento al principio, podrían establecerse requisitos adicionales tendentes a implantar garantías de protección de datos o a garantizar su eficacia. Un ejemplo sería una disposición por la que se exigiera llevar a cabo una evaluación de impacto sobre la privacidad para operaciones de tratamiento de datos de mayor riesgo.

4. El presente Dictamen quiere basarse en la contribución previa en la materia del Grupo de Trabajo del artículo 29, el Dictamen sobre el Futuro de la Privacidad, a efectos de asesorar a la Comisión en su revisión en curso de la Directiva 95/46. Para ello, el presente Dictamen se divide en cuatro secciones: La primera trata de la necesidad de que los responsables del tratamiento de datos refuercen sus disposiciones prácticas internas (estrategias y procedimientos) para hacer que todo el tratamiento se realice de conformidad con las normas aplicables y del modo en que los sistemas basados en la responsabilidad puedan contribuir a este empeño. El Dictamen examina a continuación cómo se presentaría la arquitectura jurídica de un sistema basado en la responsabilidad y sus precedentes en protección de datos y otras materias. La sección segunda adelanta una propuesta concreta del principio de responsabilidad y describe la lógica subyacente a los distintos aspectos de la propuesta. La sección tercera toca diversos elementos vinculados a un sistema jurídico, que integra un sistema general de rendición de cuentas. Incluye reflexiones sobre la necesidad de una propuesta así que aporte certeza jurídica y que, a la vez, esté formulada en términos suficientemente amplios como para que la propuesta sea modulable (es decir, que permita decidir las medidas concretas y los métodos de verificación aplicables en función del riesgo del tratamiento y de la naturaleza de los datos tratados). Trata luego de asuntos conexos como la relación con las transferencias transoceánicas, hace una descripción de las ventajas que aportaría a las autoridades de protección de datos un mecanismo basado en la responsabilidad y prefigura el margen que ello abriría para la certificación.

II. RESPONSABILIDAD: OBJETIVOS, ARQUITECTURA JURÍDICA, PRECEDENTES Y TERMINOLOGÍA

II.1 La responsabilidad como vector de la aplicación eficaz de los principios de protección de datos

5. En la actualidad hay una necesidad e interés crecientes de que los responsables del tratamiento de datos garanticen la adopción de medidas eficaces que aporten una auténtica protección de datos. Hay diversas razones para ello, como se discute a continuación.

6. En primer lugar, presenciamos hoy lo que podríamos llamar un efecto de «diluvio de datos» en que la masa de datos personales existente, objeto de tratamiento y de ulterior transferencias, no cesa de aumentar. Tanto los avances tecnológicos, es decir, el crecimiento de los sistemas de información y comunicación, como la creciente capacidad de las personas para utilizar e interactuar con las tecnologías favorecen este fenómeno. A medida que se dispone de más datos y que estos viajan a través del globo, crecen también los riesgos de filtración de datos. Ello subraya la necesidad de que los responsables del tratamiento de datos, tanto del sector público como del privado, apliquen mecanismos internos eficaces para garantizar la protección de la información personal.

7. En segundo lugar, la creciente masa de información personal se acompaña de la revalorización de esta en términos sociales, políticos y económicos. En algunos sectores, especialmente en los entornos en línea, los datos personales se han convertido de hecho en la moneda de cambio del contenido. Al mismo tiempo, desde un punto de vista sociológico, hay un reconocimiento creciente de la protección de datos como valor social. En resumen, a medida que la información personal se hace más valiosa para los responsables del tratamiento de datos de todos los sectores, los ciudadanos, los consumidores y la sociedad en su conjunto adquieren una conciencia creciente de su significación. Esto a su vez refuerza la necesidad de aplicar medidas estrictas para salvaguardarla.

8. Finalmente, de lo que precede se sigue que las filtraciones de información personal pueden tener efectos negativos de importancia para los responsables del tratamiento de datos en el sector público y en el privado. Fallos potenciales en aplicaciones de administración electrónica o de salud electrónica tendrán consecuencias devastadoras, no solo en términos económicos sino sobre todo en términos de prestigio. Por ello, minimizar los riesgos, crear y mantener una buena reputación y ganar la confianza de ciudadanos y consumidores es algo se ha convertido en imprescindible para los responsables del tratamiento de datos de todos los sectores.

9. En definitiva, lo que antecede demuestra la necesidad crucial que tienen los responsables del tratamiento de datos de aplicar medidas reales y eficaces de protección de datos orientadas a la buena gobernanza de protección de datos y que, al tiempo, minimicen los riesgos jurídicos, económicos y de prestigio que podrían derivarse de una práctica precaria de protección de datos. Como se explicará después, los mecanismos basados en la responsabilidad se orientan a la consecución de estos objetivos.

II.2 Una arquitectura jurídica general de mecanismos basados en la responsabilidad

10. En este contexto, un asunto importante de debate es la manera como el marco jurídico podría incitar a los responsables del tratamiento de datos a adoptar medidas que aportaran una protección práctica real. En otras palabras, qué visos tendría la arquitectura jurídica de sistemas basados en la responsabilidad.

11. Como observación previa al debate de dicha arquitectura, debe recalcarse que, en principio, tales sistemas no cambian ni afectan de modo alguno los principios materiales de la protección de datos sino que, por el contrario, buscan un mejor funcionamiento de los mismos.

12. Un modo de incitar a los responsables del tratamiento de datos a poner en práctica tales medidas sería añadir un principio de responsabilidad en la versión revisada de la Directiva. Los efectos previsibles de dicha disposición incluirían la aplicación de medidas y procedimientos internos que pusieran en práctica los actuales principios de protección de datos, garantizando su eficacia y la obligación de demostrarla a instancias de las autoridades de protección de datos. Como se explica a continuación, el tipo de procedimientos y mecanismos variaría en función de los riesgos que representen el tratamiento y la naturaleza de los datos.

13. Amén de lo anterior, pueden imaginarse requisitos particulares como la obligación de realizar evaluaciones de impacto sobre la privacidad en determinados casos o el nombramiento de funcionarios de protección de datos. Estos requisitos particulares podrían complementar el principio general de responsabilidad.

14. El Grupo de Trabajo del artículo 29 reconoce que los responsables del tratamiento de datos pueden desear aplicar estrategias y procedimientos que no estén en rigor previstos en la legislación de protección de datos. Por ejemplo, un responsable del tratamiento de datos puede querer comprometerse a cursar peticiones de acceso en un plazo muy corto de tiempo aun cuando la legislación prevea cierta flexibilidad. Puede también comprometerse a cursar peticiones de acceso en línea y fuera de línea simultáneamente para garantizar una recepción ágil y eficaz de dicha información. Pueden imaginarse situaciones en que el responsable del tratamiento de datos desee ir más allá de los requisitos mínimos concretados en el marco jurídico general. Por ejemplo, un responsable del tratamiento puede decidir nombrar a un funcionario de protección de datos aunque la legislación vigente no lo prescriba. Un responsable del tratamiento de datos puede también encargar a una tercera parte la realización de una auditoría de *todas* sus operaciones de tratamiento para evaluar su conformidad con el marco jurídico de protección de datos. El Grupo de Trabajo del artículo 29 se felicita de dichas iniciativas y anima a que el nuevo marco jurídico de protección de datos plantee incentivos para que los responsables del tratamiento de datos obren de esa manera.

15. En línea con lo anterior, la «arquitectura jurídica» de los mecanismos de responsabilidad plantearía dos niveles: el primer nivel consistiría en un requisito reglamentario básico vinculante para *todos* los responsables del tratamiento de datos. El contenido del requisito incluiría dos elementos: la aplicación de medidas/procedimientos y el mantenimiento de pruebas de dicho extremo. Este primer nivel podría complementarse con requisitos particulares. Un segundo nivel incluiría sistemas discrecionales de responsabilidad que superaran los requisitos jurídicos mínimos de los principios subyacentes de protección de datos (proporcionando garantías más estrictas que las exigidas por la normativa aplicable) y las modalidades de aplicación o de garantía de la eficacia de las medidas (requisitos de aplicación que sobrepasen el nivel mínimo). Aunque reconoce la importancia y los beneficios de dichos sistemas, el presente Dictamen

se ocupa principalmente del primer requisito, especialmente del principio de responsabilidad general.

II.3 Principio de responsabilidad en la protección de datos y otras materias y terminología

Antecedentes

16. El Grupo de Trabajo del artículo 29 hace observar que el principio de responsabilidad no es exactamente nuevo. Su reconocimiento expreso figura en las directrices sobre privacidad adoptadas en 1980 por la Organización de Cooperación y Desarrollo Económicos (OCDE). El principio de responsabilidad de estas reza así: «Todo responsable de datos debería ser responsable de cumplir con las medidas que hagan efectivos los principios [materiales] expuestos».

17. Recientemente el principio quedó incluido en las Normas Internacionales de Madrid, desarrolladas por la Conferencia Internacional de Comisarios de Protección de Datos y Privacidad[2]. Ha quedado también incorporado a la propuesta de norma más reciente de ISO 29100, que establece un marco de privacidad, y es uno de los conceptos principales del marco de privacidad de la CEAP y de sus normas de privacidad transfronteriza[3].

18. Desde un punto de vista «reglamentario», el Grupo de Trabajo del artículo 29 observa que los Principios de Información Leal de Canadá incluidos en la Ley de Protección de la Información Personal y de Documentos electrónicos aluden a la responsabilidad. Entre otros, el primer principio requiere políticas y prácticas de desarrollo y aplicación para respetar los 10 Principios de Información Leal, que incluyen procedimientos de aplicación para la protección de la información personal y el establecimiento de procedimientos para recibir y cursar quejas y peticiones.

19. Amén de lo anterior, el Grupo de Trabajo del artículo 29 observa que las Normas Corporativas Vinculantes (BCR), que se utilizan en el contexto de las transferencias de datos internacionales, reflejan el principio de responsabilidad. En efecto, estas Normas son códigos de conducta que redactan y siguen organizaciones multinacionales y que contienen medidas internas pensadas para poner en práctica principios de protección de datos (como auditoría, programas de formación, red de funcionarios de privacidad, sistema de tratamiento de quejas). Una vez revisadas por las autoridades nacionales de protección de datos, las Normas Corporativas Vinculantes deben garantizar salvaguardias adecuadas para transferencias o categorías de transferencias de datos personales entre empresas que formen parte del mismo grupo corporativo y estén sujetas a dichas normas

---

2 La persona responsable a. adoptará todas las medidas necesarias para observar los principios y obligaciones establecidos en el presente Documento y en la legislación nacional aplicable y b. pondrá a punto los mecanismos internos necesarios para demostrar dicho cumplimiento tanto a las personas interesadas como a las autoridades de supervisión en el desempeño de sus competencias, como se dispone en la sección 23».

3 Además de lo anterior, el Centre for Information Policy Leadership (Centro de liderazgo de la política de información) trabaja en una iniciativa para examinar los efectos del principio de responsabilidad en lo que respecta a la protección de datos y la privacidad. Véase www.informationpolicycentre.com

corporativas en el sentido del artículo 25 y el artículo 26, apartado 2, de la Directiva 95/46.

20. Fuera del contexto de la protección de datos, hay también ejemplos del principio: como un programa que especifique las estrategias y procedimientos del responsable del tratamiento de datos para garantizar la observancia de las leyes y los reglamentos. Por ejemplo, los programas de cumplimiento legislativo son obligatorios según los reglamentos de servicios financieros. En otros casos, los programas de cumplimiento no son obligatorios pero se incita a que lo sean, como sucede en el Derecho de competencia. Por ejemplo, en Canadá, el Comisario de la Competencia ha elaborado estrategias afinadas de programas de cumplimiento corporativo. La decisión de aplicar o no un programa es voluntaria para las empresas. No obstante, el Comisario de la competencia canadiense subraya la importancia del cumplimiento de las normas como instrumento de disminución de riesgos y hace hincapié en los beneficios jurídicos, económicos y de prestigio[4].

Terminología

21. El término «responsabilidad» (**accountability**) proviene del mundo anglosajón donde es de uso general y donde se da una comprensión ampliamente compartida de su significado, aunque la definición exacta de «responsabilidad» resulta compleja en la práctica. Pero de forma general, el término apunta sobre todo al modo en que se ejercen las competencias y al modo en que esto puede comprobarse. Competencia y responsabilidad son dos caras de la misma moneda y sendos elementos esenciales de la gobernanza. Solo cuando la responsabilidad funciona en la práctica puede desarrollarse la confianza suficiente.

22. En la mayoría de las demás lenguas europeas, debido sobre todo a diferencias en los sistemas de Derecho, el término «accountability» no es fácil de traducir. Consiguientemente hay un gran riesgo de que el término se interprete diversamente llegándose con ello a una falta de armonización. Se han apuntado otras palabras para recoger el sentido de responsabilidad, como son «competencia reforzada», «garantía», «fiabilidad», fiabilidad» o, en español, «obligación de rendir cuentas», etc. Puede también sugerirse que la responsabilidad se refiere a la «aplicación de principios de protección de datos».

23. En el presente documento, nos centramos, pues, en las medidas que pudieran adoptarse o preverse para garantizar la observancia en materia de protección de datos. Las referencias a la responsabilidad deben, pues, entenderse en el sentido empleado en el presente Dictamen, sin perjuicio de hallar otra formulación que refleje más fielmente el concepto aquí expuesto. Por esta razón, el documento no se centra en los términos sino que aborda con pragmatismo las medidas precisas más que el concepto en sí.

4 www.bureaudelaconcurrence.gc.ca/eic/site/cb-bc.nsf/eng/02732.html.

III. HACIA UNA PROPUESTA DE DISPOSICIÓN GENERAL SOBRE RESPONSABILIDAD

III.1 Disposición general para recalcar y reforzar la responsabilidad de los responsables del tratamiento de datos

24. Guiado por las consideraciones que se hacen en la sección I, el Grupo de Trabajo del artículo 29 ha profundizado en la idea de introducir soluciones basadas en la responsabilidad en el nuevo marco jurídico general.

25. En consecuencia de ello, ha confirmado su opinión, ya expresada en su Dictamen sobre el Futuro de la Privacidad, de incluir un principio general de responsabilidad en un nuevo y amplio marco legislativo. El objetivo de dicha disposición sería recalcar y reforzar la responsabilidad de los responsables en el tratamiento de datos personales. Ello sin prejuzgar medidas concretas de responsabilidad que pudieran complementar dicho principio.

26. Estas nuevas disposiciones estarían en sintonía con disposiciones específicas ya vigentes en el marco legislativo actual. Podemos referirnos en particular al artículo 6 de la Directiva 95/46/CE, que alude a los principios relativos a la calidad de los datos en su apartado 1 y que, en su apartado 2, declara: «Corresponderá a los responsables del tratamiento garantizar el cumplimiento de lo dispuesto en el apartado 1». Esto concordaría con el artículo 17, apartado 1, que establece que los responsables del tratamiento de datos apliquen medidas técnicas y organizativas. En efecto, una disposición general de responsabilidad reforzaría la necesidad de que los responsables del tratamiento de datos aplicaran los requisitos de seguridad del artículo 17, además de los que se exponen en las restantes disposiciones.

III.2 Hacia una propuesta concreta del principio general de responsabilidad

27. La nueva disposición tendería a fomentar la adopción de medidas concretas y prácticas, convirtiendo los principios generales de protección de datos en estrategias y procedimientos concretos definidos al nivel del responsable del tratamiento de los datos en cumplimiento de las leyes y reglamentos aplicables. El responsable del tratamiento debe garantizar igualmente la eficacia de las medidas adoptadas y demostrar, si así se le requiere, que ha adoptado dichas acciones.

28. De forma esquemática, dicha disposición general se centraría en dos elementos principales:

    i) la necesidad de que el responsable del tratamiento adopte medidas adecuadas y eficaces para aplicar los principios de protección de datos;
    ii) la necesidad de demostrar, si así se requiere, que se han adoptado medidas adecuadas y eficaces; así pues, el responsable del tratamiento de datos deberá aportar pruebas de (i).

29. Las obligaciones deben cubrir a todos los responsables del tratamiento de datos y en todas las situaciones.

30. El primer elemento de la obligación requeriría que los responsables del tratamiento aplicaran medidas adecuadas. El tipo de medidas no se especificaría en el texto de la disposición general sobre responsabilidad. Orientaciones ulteriores que dieran las autoridades nacionales de protección de datos, el Grupo de Trabajo del artículo 29 o la Comisión (mediante procedimientos de comitología) podría especificar, en determinados casos, el mínimo de medidas específicas que constituyera medidas adecuadas. Un ejemplo de dichas medidas sería la adopción en determinados casos de las estrategias y los procesos necesarios para aplicar los principios de protección de datos, reflejo de las leyes y los reglamentos aplicables.

31. La aplicación de dichas medidas y procesos puede también hacerse de modo eficaz mediante la atribución de competencias y mediante la formación del personal implicado en las operaciones de tratamiento. En especial, en cumplimiento del artículo 18 de la Directiva, debe animarse a los responsables del tratamiento de datos a que designen funcionarios de protección de datos. En cualquier caso, debe incitarse a que se asignen cometidos a diferentes niveles de la organización para garantizar que se cumplen los cometidos.

32. En relación con las transferencias de datos personales fuera de la Unión Europea, los responsables del tratamiento de datos deben adoptar y aplicar medidas adecuadas para cumplir con el requisito de «ofrecer garantías suficientes» dispuesto en el artículo 26 de la Directiva 95/46/CE y en las BCR.

33. Los responsables del tratamiento de datos deben también garantizar la eficacia de las medidas prácticas aplicadas para cumplir con los principios de protección de datos. En caso de un tratamiento más amplio o complejo o de alto riesgo, la eficacia de las medidas adoptadas debe verificarse periódicamente. Hay diversos modos de evaluar la eficacia (o ineficacia) de las medidas: seguimiento, auditorías internas y externas, etc.

34. En línea con las anteriores observaciones, el Grupo de Trabajo del artículo 29 estudió la formulación de una disposición concreta que podría introducirse en un marco legislativo amplio y que rezaría como sigue:

«Artículo X – Aplicación de los principios de protección de datos

1. El responsable del tratamiento de datos aplicará medidas adecuadas y eficaces para garantizar el cumplimiento de los principios y obligaciones dispuestos en la Directiva.
2 A instancias de la autoridad de control, el responsable del tratamiento de datos demostrará el cumplimiento del apartado 1.»

IV. DISCUSIÓN DE VARIOS EXTREMOS RELACIONADOS CON EL PRINCIPIO GENERAL DE RESPONSABILIDAD

IV.1 Reforzar las obligaciones vigentes

35. El Grupo de Trabajo del artículo 29 es consciente de que algunos responsables del tratamiento de datos pueden considerar que el principio general de responsabilidad les impone nuevos y pesados requisitos legales, en especial teniendo en cuenta la actual situación económica, tan comprometida, de la UE. Esta percepción no es correcta.

36. El Grupo de Trabajo del artículo 29 desea subrayar que la mayor parte de los requisitos expuestos en esta nueva disposición rigen ya, si bien de modo menos explícito, con arreglo a la legislación actual. En efecto, con arreglo al actual marco jurídico, los responsables del tratamiento de datos están obligados a cumplir los principios y obligaciones dispuestos en la Directiva. Para ello, es intrínsecamente necesario establecer, y posiblemente verificar, procedimientos de protección de datos. Desde esta perspectiva, una disposición sobre responsabilidad no representa una gran novedad y, en lo esencial, no impone requisitos que no estuvieran ya implícitos en la legislación vigente. En resumen, la nueva disposición no pretende someter a los responsables del tratamiento de datos a nuevos principios sino más bien garantizar de hecho un cumplimiento efectivo de los principios existentes.

37. De hecho, cuando la Directiva 2002/58 se modificó, en 2009, ya se produjo un cambio legislativo similar.[5] En este caso, la ley impone la obligación de aplicar una política de seguridad, a saber, «*garantizar la aplicación efectiva de una política de seguridad con respecto al tratamiento de datos personales*». Así pues, en lo que se refiere a las disposiciones sobre seguridad de dicha Directiva, el legislador decidió que era necesario introducir un requisito explícito para tener y aplicar una política de seguridad. Además, el artículo 18 de la Directiva 95/46, referido a la designación de funcionarios de protección de datos, así como a las normas corporativas obligatorias antes mencionadas, ofrece ya ejemplos de medidas prácticas que pueden adoptar los responsables del tratamiento de datos.

38. Una cuestión relacionada con lo anterior es la consecuencia vinculada al cumplimiento (o incumplimiento) del principio de responsabilidad. El Grupo de Trabajo del artículo 29 hace hincapié en que la observancia del principio de responsabilidad no implica necesariamente que el responsable del tratamiento de datos cumpla los principios materiales establecidos en la Directiva, es decir, no ofrece presunción jurídica de cumplimiento ni sustituye a ninguno de dichos principios. Un responsable del tratamiento de datos puede haber aplicado y verificado las medidas que ha puesto en práctica y, pese a ello, hallarse en una situación de irregularidad. Consiguientemente, la adopción de medidas para cumplir con los principios no debe en ningún caso eximir a los responsables del tratamiento de datos de actuaciones ejecutorias por parte de las autoridades de

[5] Directiva 2009/136/CE del Parlamento Europeo y del Consejo, de 25 de noviembre de 2009 , por la que se modifican la Directiva 2002/22/CE relativa al servicio universal y los derechos de los usuarios en relación con las redes y los servicios de comunicaciones electrónicas, la Directiva 2002/58/CE relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las comunicaciones electrónicas y el Reglamento (CE) n o 2006/2004 sobre la cooperación en materia de protección de los consumidores.

protección de datos. En la práctica, los responsables del tratamiento de datos del sector público y privado que hayan adoptado medidas en programas de cumplimiento sólidos tienen más probabilidades de respetar la ley. Efectivamente, al haber llevado a cabo medidas eficaces tendentes a observar los principios materiales de la protección de datos, sería menos probable que violaran la ley. Por ello, al evaluar las sanciones relacionadas con las infracciones en la protección de datos, las autoridades de protección de datos podrían sopesar la aplicación (o inaplicación) de las medidas y su verificación.

IV.2 Medidas adecuadas para aplicar las disposiciones de la Directiva

39. Una disposición sobre responsabilidad requeriría que los responsables del tratamiento de datos definieran y aplicaran las medidas necesarias para garantizar el cumplimiento de los principios y obligaciones de la Directiva y hacer verificar periódicamente su eficacia.

40. El principio de responsabilidad general propuesta evita voluntariamente detallar claramente el tipo de medidas que deban aplicarse. Ello da lugar a las dos preguntas siguientes, relacionadas entre sí: *i)* ¿qué medidas comunes cumplirían con el principio de responsabilidad; *ii)* ¿cómo modular y adaptar las medidas a circunstancias específicas?

Las medidas: ilustración

41. El Grupo de Trabajo del artículo 29 considera que las medidas comunes de responsabilidad pueden incluir las que figuran en la siguiente lista, no exhaustiva:

- establecimiento de procedimientos internos *previos* a la creación de nuevas operaciones de tratamiento de datos personales (revisión interna, evaluación, etc.);[6]
- establecimiento de políticas escritas y vinculantes de protección de datos que se tengan en cuenta y se valoren en nuevas operaciones de tratamiento de datos (p.ej., cumplimiento de los criterios de calidad de datos, notificación, principios de seguridad, acceso, etc.) que deben ponerse a disposición de las personas interesadas;
- cartografía de procedimientos que garanticen la identificación correcta de todas las operaciones de tratamiento de datos y el mantenimiento de un inventario de operaciones de tratamiento de datos;
- nombramiento de un funcionario de protección de datos y otras personas responsables de la protección de datos;
- oferta adecuada de protección de datos y formación a los miembros del personal; esto debe incluir a los procesadores (o responsables del proceso) de datos personales (como los directores de recursos humanos) pero también a los administradores de tecnologías de la información, conceptores y directores de unidades comerciales; deben asignarse recursos suficientes para la gestión de la privacidad, etc…;

[6] Las operaciones de tratamiento de datos actuales necesitarían un período de transición para acompasarse a la ley.

- establecimiento de procedimientos de gestión del acceso y de las demandas de corrección y eliminación de datos con transparencia para las personas interesadas;
- establecimiento de un mecanismo interno de tratamiento de quejas;
- establecimiento de procedimientos internos de gestión y notificación eficaces de fallos de seguridad;
- realización de evaluaciones de impacto sobre la privacidad en circunstancias específicas;
- aplicación y supervisión de procedimientos de verificación que garanticen que las medidas no sean solo nominales sino que se apliquen y funcionen en la práctica (auditorías internas o externas, etc.).

42. También podría plantearse un enfoque complementario del principio general de responsabilidad. Según dicho enfoque, el marco jurídico no incluiría meramente un principio general de responsabilidad sino también una lista ilustrativa de medidas que se pudieran fomentar a nivel nacional[7]. Esta disposición podría dar una lista ilustrativa, no exhaustiva de medidas que constituyeran una «caja de herramientas» para responsables de tratamiento de datos. Ofrecería también orientación a los responsables del tratamiento sobre aquello que pudiera constituir, en función de los casos, medidas adecuadas que adoptara el responsable del tratamiento. Naturalmente esta lista ilustrativa sería solo un complemento de la obligación legal general de adoptar medidas adecuadas.

---

7 Por ejemplo, las Normas Técnicas Internacionales adoptadas en Madrid por las autoridades de protección de datos incluyen en su artículo 22 una disposición sobre medidas proactivas que reza así: *Los Estados deben fomentar, mediante su legislación nacional, la aplicación por parte de las personas involucradas en cualquier fase del tratamiento de medidas que fomenten un cumplimiento de la legislación de protección de privacidad aplicable en relación al tratamiento de datos personales. Tales medidas podrían incluir, por ejemplo*:

a) La aplicación de procedimientos para impedir y localizar las filtraciones, que pueden basarse en modelos tipificados de gobernanza o gestión de seguridad de la información.

b) El nombramiento de uno o más funcionarios de protección de datos o privacidad, con cualificaciones, recursos y competencias adecuados para ejercer adecuadamente sus funciones de supervisión.

c) La realización periódica de programas de formación, educación y sensibilización entre los miembros de la organización dirigidos a una mejor comprensión de la legislación aplicable sobre protección de la privacidad en relación al tratamiento de datos personales así como de los procedimientos establecidos al efecto por la organización.

d) La realización periódica de auditorías transparentes por partes cualificadas y preferentemente independientes que verifiquen el cumplimiento de la legislación aplicable sobre protección de la privacidad en relación al tratamiento de datos personales así como con los procedimientos establecidos al efecto por la organización..

e) La adaptación de los sistemas de información o de las tecnologías de tratamiento de datos personales a la legislación aplicable sobre protección de la privacidad en relación al tratamiento de datos personales, particularmente en el momento de decidir sobre sus especificaciones técnicas y sobre su desarrollo y aplicación.

f) La aplicación de evaluaciones de impacto sobre la privacidad previas a la implantación de nuevos sistemas de información o de tecnologías de tratamiento de datos personales y previos también a la realización de cualquier nuevo método de tratamiento de datos personales o de modificaciones sustanciales en el tratamiento existente.

g) La adopción de códigos de prácticas de observancia vinculante que incluyan elementos que permitan medir la eficacia en cuanto afecte al cumplimiento y al nivel de protección de los datos personales y que establezcan medidas eficaces en caso de incumplimiento.

h) La aplicación de un plan de respuesta que establezca directrices de actuación en caso de que se verifique una infracción de la legislación sobre protección de la privacidad aplicable en relación al tratamiento de datos personales, que incluya al menos la obligación de determinar la causa y gravedad de la infracción, de describir sus efectos negativos y de adoptar las medidas adecuadas para impedir infracciones ulteriores.

Modulación de medidas

43. La anterior es una lista ilustrativa de las medidas que podrían poner en práctica los responsables del tratamiento de datos para conformarse a la primera parte del principio de responsabilidad (*El responsable del tratamiento de datos aplicará medidas adecuadas y eficaces para garantizar el cumplimiento de los principios y obligaciones dispuestos en la Directiva.).*

44. Algunas medidas son «componentes fijos» que deberán aplicarse en la mayoría de las operaciones de tratamiento de datos. La preparación de políticas y procedimientos internos que apliquen los principios (procedimientos de gestión de las solicitudes de acceso, denuncias) puede constituir ejemplos de medidas adecuadas de algunos tratamientos de datos. La idoneidad de las medidas deberá decidirse caso por caso. Corresponde a los responsables del tratamiento de datos adoptar dichas decisiones siguiendo, en su caso, las directrices publicadas por las autoridades nacionales de protección de datos y el Grupo de Trabajo del artículo 29 (véase más adelante).

45. De lo que antecede se sigue que, al determinar los tipos de medidas aplicables, no hay otra opción que las soluciones «particularizadas». En efecto, las medidas específicas aplicables deben determinarse en función de los hechos y circunstancias de cada caso particular, con atención especial al riesgo del tratamiento y a los tipos de datos. Un enfoque de «talla única» tan solo forzaría a los responsables del tratamiento a embutirse en estructuras mal adaptadas y acabaría fracasando.

46. Según este enfoque, los responsables del tratamiento de datos deben ser capaces de adecuar las medidas a la realidad específica del responsable del tratamiento y a las operaciones de tratamiento de datos de que se trate. En este contexto, el Grupo de Trabajo del artículo 29 reitera los criterios empleados en el artículo 17 de la Directiva vigente[8] para determinar el tipo de medidas de seguridad aplicables: a saber, los riesgos que representan el tratamiento de datos y la naturaleza de los datos. Estos dos factores podrían emplearse por analogía para determinar los tipos generales de medidas aplicables. Más en concreto, aspectos como el tamaño de las operaciones de tratamiento de datos, los objetivos declarados del tratamiento y el número de transferencias de datos previstos pueden determinar el nivel de riesgo. El tipo de datos, incluido su carácter sensible o no sensible, debe también considerarse. A la luz de dicho principio de responsabilidad, podría también lanzarse una reflexión sobre la necesidad de imponer determinadas obligaciones al responsable del tratamiento de datos o a los conceptores o fabricantes de ICT (tecnologías de la información y la comunicación).

47. Sin perder de vista dichos criterios, en principio, los responsables de grandes tratamientos de datos deben aplicar medidas coercitivas. En algunos casos, a los responsables de tratamientos pequeños o medios, por ejemplo si trabajan en tratamientos de datos con riesgo, como pueden ser algunas operaciones de datos sanitarios, se les puede exigir que establezcan salvaguardias estrictas. Por

---

8 «Dichas medidas deberán garantizar, habida cuenta de los conocimientos técnicos existentes y del coste de su aplicación, un nivel de seguridad apropiado en relación con los riesgos que presente el tratamiento y con la naturaleza de los datos que deban protegerse» .

ejemplo, a una administración local (ayuntamiento), una multinacional, una pequeña empresa (de Internet), una organización para la que el tratamiento de datos representa su actividad básica o una organización con antecedentes de infracciones legales puede exigírseles medidas específicas particulares que hagan creíble y eficaz la buena gobernanza informativa. De resultas de ello, en casos sencillos y básicos, como el tratamiento de datos personales relativos a recursos humanos para establecer un directorio corporativo, la «obligación de demostrar», a que se refiere el apartado 2 de las disposiciones sobre responsabilidad, podría cumplirse fácilmente (por ejemplo, mediante las notificaciones que se hicieran, la descripción de medidas básicas de seguridad, etc.). Por el contrario, en casos más complejos como, por ejemplo, el uso de dispositivos biométricos innovadores, el cumplimiento de la «obligación de demostrar» podría necesitar requisitos adicionales. El responsable del tratamiento de datos puede, por ejemplo, tener que demostrar que realizó una evaluación de impacto sobre la privacidad, que el personal implicado en el tratamiento recibe formación e información regulares, etc.

48. La transparencia es un elemento integral de muchas medidas de responsabilidad. La transparencia frente a las personas interesadas y el público en general contribuye a la toma de conciencia de los responsables del tratamiento de datos. Por ejemplo, haciendo públicas en Internet las políticas de privacidad, aportando transparencia en relación a los procedimientos de denuncias internas y publicando informes anuales se logra un mayor nivel de responsabilidad.

Directrices y seguridad jurídica

49. Aunque la necesidad de modulación y, por ende, de flexibilidad, aconsejan recurrir a un lenguaje abierto, el Grupo de Trabajo del artículo 29 es consciente de que una disposición amplia con margen para la flexibilidad y la modulación puede abocar a la incertidumbre. Los responsables del tratamiento de datos pueden considerar que la disposición no es suficientemente detallada para aportar seguridad jurídica. Por ejemplo, pueden tener dudas sobre el nivel de detalle que se espera de las políticas y procedimientos de privacidad, sobre cuándo y cómo designar a un funcionario de protección de datos, sobre cuándo organizar sesiones de formación, etc. La inseguridad puede también tener que ver con el tipo de verificación necesario (interna o por terceros). Además, los responsables del control de datos pueden también temer ser objeto de interpretaciones nacionales divergentes y arbitrarias en relación al ámbito y naturaleza de sus obligaciones.

50. El Grupo de Trabajo del artículo 29 comprende esta preocupación. No obstante, por las razones antes apuntadas tocantes a la necesidad de flexibilidad y modulación, la solución para lograr seguridad jurídica no puede venir de la propia Directiva. Para lograr la necesaria seguridad jurídica, el Grupo de Trabajo del artículo 29 considera que las directrices de armonización publicadas por la Comisión (por ejemplo, mediante medidas de aplicación técnicas) o el Grupo de Trabajo del artículo 29 podrían constituir herramientas útiles que aportaran mayor

seguridad y eliminaran diferencias potenciales a nivel de ejecución.[9] El Grupo de Trabajo del artículo 29 podría también preparar directrices generales presentando una base de elementos necesarios para el responsable tipo del tratamiento de datos. Esta base podría adaptarse a las necesidades específicas de cada responsable de tratamiento de datos.

51. También podría ser útil desarrollar un *programa de cumplimiento de datos tipo* que utilizaran los responsables de tratamientos medios y grandes como base sobre la que preparar sus programas, como se hizo en el caso de las BCR con las directrices desarrollas por el Grupo de Trabajo del artículo 29[10]. Estos modelos deben crearse tras revisar atentamente las prácticas al uso y los modelos disponibles y en consulta con todas las partes interesadas. Esta es un área que precisará un empeño serio de todos los interesados.

Eficacia de las medidas

52. Puntos similares a los aquí tratados a propósito de las medidas aplicables se plantean a la hora de garantizar la eficacia de las medidas. En función del tipo de tratamiento de datos, variará el modo de garantizar la eficacia.

53. Hay muchos modos distintos de que los responsables del tratamiento de datos evalúen la eficacia (o ineficacia) de las medidas. Para tratamientos grandes, más complejos y de alto riesgo, son métodos comunes de verificación las auditorías internas y externas. El modo en que se realizan las auditorías puede oscilar entre auditorías completas y auditorías negativas (que pueden también adoptar diferentes formas y configuraciones). Para decidir el modo de garantizar la eficacia de las medidas, el Grupo de Trabajo del artículo 29 sugiere utilizar los mismos criterios que para decidir sobre las medidas derivadas del artículo 18 de la Directiva 95/46/CE, a saber, los riesgos que representan el tratamiento de datos y la naturaleza de los datos. Por ello, el modo en que un responsable del tratamiento de datos deba garantizar la eficacia de las medidas dependerá de la sensibilidad de los datos, la masa de datos objeto de tratamiento y los riesgos especiales planteados por el tratamiento. Las directrices del Grupo de Trabajo del artículo 29 sobre las medidas pueden también incluir directrices sobre este punto.

IV.3 Relación con otros requisitos

Notificaciones previas

54. Podría iniciarse una reflexión sobre el posible impacto en las notificaciones previas cuando las salvaguardias adecuadas se definen a nivel del responsable del tratamiento de datos. Puede plantearse que determinados mecanismos de responsabilidad sustituyan o disminuyan los requisitos administrativos de la

---

9 Ejemplo de este tipo de orientación es PIPEDA, una herramienta de autoevaluación, publicada por la Oficina del Comisario de privacidad de Canadá para ayudar a los responsables de tratamientos medios y grandes a desarrollar y aplicar una buena gobernanza y gestión de la privacidad. La herramienta de autoevaluación puede consultarse en: http://www.priv.gc.ca/information/pub/ar-vr/pipeda_sa_tool_200807_e.pdf .

10 Documento 153 del Grupo de Trabajo del artículo 29 en que se establece un cuadro de elementos y principios que deben figurar en las Normas Corporativas Vinculantes y Documento de trabajo 154 por el que se establece un marco de estructura de las Normas Corporativas Vinculantes.

legislación sobre protección de datos vigente como ya sugirió el Grupo del artículo 29 en su Dictamen sobre el Futuro de la Privacidad.

Transferencias internacionales de datos

55. Las normas corporativas vinculantes son un ejemplo de cómo aplicar los principios de protección de datos con arreglo al principio de responsabilidad. Son un modo seleccionado y aceptado por el Grupo de Trabajo del artículo 29 para ofrecer garantías adecuadas en las transferencias fuera de la Unión Europea.

56. Este punto se beneficiaría de un análisis más profundo a la luz de la revisión de la Directiva 95/46/CE. Sería especialmente importante examinar si el artículo 26, apartado 2, de la Directiva («*Los Estados miembros podrán autorizar una transferencia ... cuando el responsable del tratamiento ofrezca garantías suficientes…; dichas garantías podrán derivarse, en particular, de cláusulas contractuales apropiadas*») cubre plenamente las normas corporativas y eventualmente otros mecanismos vinculantes similares de responsabilidad como herramientas que aporten garantías adecuadas.

57. En este contexto, es extremadamente importante evaluar, entre otras cosas, los mecanismos utilizados por los responsables del tratamiento de datos para aplicar internamente los principios y obligaciones y los sistemas para su verificación. Importa también mucho debatir los mecanismos para racionalizar el sistema actual, basado en la autorización de transferencias de datos por las autoridades nacionales de protección de datos.

IV.4 Función de las autoridades de protección de datos

58. Un punto que abordar es ver si el principio de responsabilidad propuesto en el presente Dictamen puede afectar las competencias de las autoridades de protección de datos, especialmente en sus funciones ejecutivas. Como se describe con más detalle a continuación, el principio no hurta ninguna competencia a las autoridades de protección de datos. Por el contrario, beneficiará a las autoridades de protección de datos.

59. En lo que atañe a las competencias de ejecución, el principio propuesto reconoce la competencia de las autoridades de protección para recabar del responsable del tratamiento de datos pruebas de cumplimiento del principio de responsabilidad, con lo que se suma a las actividades ejecutivas de las autoridades. Esto garantiza que las autoridades sigan siendo competentes, en todo momento, para emprender actuaciones ejecutorias. Debe quedar claro que, en todo caso, las autoridades de protección de datos seguirían guardando sus atribuciones para supervisar no solo las medidas adoptadas por los responsables del tratamiento, sino ante todo y sobre todo para supervisar el cumplimiento de los principios y obligaciones subyacentes.

60. Además, poner en práctica el principio de responsabilidad proporcionará información útil a las autoridades de protección de datos para supervisar los niveles de cumplimiento del mismo. En efecto, como los responsables del

tratamiento de datos deberán poder demostrar a las autoridades si han aplicado las medidas, y cómo lo han hecho, las autoridades dispondrían de información muy pertinente sobre el cumplimiento del principio. Podrán luego utilizar esta información en el contexto de sus actuaciones ejecutivas. Además, si dicha información no se proporciona cuando se solicite, las autoridades de protección de datos tendrán una causa directa de actuación contra los responsables del tratamiento, independientemente de la supuesta violación de otros principios subyacentes de protección de datos.

61. El principio puede también ser útil para las autoridades de protección de datos al ayudarlas a ser más selectivas y afinar su estrategia, permitiéndoles dedicar sus recursos para lograr el máximo nivel posible de cumplimiento de las normas.

62. El Grupo de Trabajo del artículo 29 observa que el principio de responsabilidad puede contribuir al desarrollo de conocimientos jurídicos y técnicos en la aplicación de los requisitos de protección de datos. En este campo se precisará de personas extremadamente competentes con conocimientos técnicos y jurídicos en materia de protección de datos, con capacidad de comunicar, formar al personal, establecer y ejecutar políticas; se precisarán también auditorías. Tal capacidad técnica será necesaria tanto internamente como en las empresas externas cuyos servicios se contraten. Este punto será crucial para garantizar que los responsables del tratamiento de datos ejecuten sus obligaciones, incluyendo, si fuera necesario, la realización de auditorías internas y externas/internas. Al mismo tiempo, este punto será beneficioso para las autoridades de protección de datos dado que el sistema contribuirá a un cumplimiento general de las normas, que las autoridades dispondrán de información más coherente sobre las prácticas internas de las empresas y que la formación de especialistas extremadamente preparados y competentes las ayudará sin duda en su interacción con los responsables del tratamiento de datos.

63. Puede deducirse que la actividad de las autoridades de protección de datos se centra más en su función «ex post» que en su función «ex ante». Dado que el principio de responsabilidad hace hincapié en determinados resultados que han de conseguirse en materia de buena gobernanza de protección de datos, es un principio, podemos decir, que se centra en los resultados; su énfasis está en el «ex post» (después de iniciarse el tratamiento de datos).

IV. 5 Sanciones

64. El sistema propuesto solo puede funcionar si a las autoridades de protección de datos se les atribuyen competencias sancionadoras significativas. En especial, cuando, y si, los responsables del tratamiento de datos incumplen el principio de responsabilidad, se precisan sanciones significativas. Por ejemplo, si el responsable del tratamiento de datos no respeta sus compromisos en políticas internas vinculantes. Evidentemente, esto se sumará a la violación concreta de los principios materiales de protección de datos.

65. Además de lo dicho, el Grupo de Trabajo del artículo 29 considera que las competencias de las autoridades nacionales de protección de datos deben incluir la posibilidad de imponer instrucciones precisas a los responsables del tratamiento de datos en relación con su sistema de cumplimiento de las normas.

IV.6 El desarrollo de sistemas de certificación

66. A largo plazo, la disposición sobre responsabilidad puede incitar el desarrollo de programas o sellos de certificación. Tales programas contribuirían a demostrar que los responsables del tratamiento de datos respetan la disposición y consiguientemente que han definido y aplicado las medidas adecuadas que han sido objeto periódico de auditorías. Hay distintos factores que apuntan en esta dirección:

67. En general, puede preverse que, para diferenciarse, los servicios de impacto sobre la protección/auditoría/intimidad ofrezcan cada vez más certificaciones/sellos que los singularicen en el mercado o les den una ventaja competitiva. Los responsables del tratamiento de datos pueden decidir utilizar la opción de servicios fiables que expidan certificados. Dado que determinados sellos serían conocidos por su control riguroso, los responsables del tratamiento de datos los favorecerán probablemente en la medida en que les dan un margen de cumplimiento adicional además de ofrecerles una ventaja competitiva.

68. El uso de las BCR como base jurídica de las transferencias internacionales requiere que los responsables del tratamiento de datos demuestren haber aplicado garantías adecuadas, en cuyo caso las autoridades de protección de datos podrán autorizar las transferencias. Este es un campo en que los servicios de certificación podrían ser útiles. Tales servicios analizarían las garantías presentadas por el responsable del tratamiento de datos y, en su caso, expedirían el sello correspondiente. Una autoridad de protección de datos solo podría usar la certificación expedida por un programa de certificación dado, al analizar con arreglo a las BCR, un responsable del tratamiento de datos ha aportado garantías suficientes al objeto de transferencias internacionales de datos, contribuyendo así a racionalizar el proceso de autorización de transferencias internacionales de datos.

IV.7 Regulación de los sistemas de certificación

69. Las mismas razones que favorecen el desarrollo de servicios de certificación apuntalan también la necesidad de regular dichos servicios. En efecto, si dichos servicios se orientan a proporcionar pruebas fiables de la observancia de las normas de protección de datos (a las autoridades de protección de datos, a los responsables del tratamiento y a los consumidores en general) y operan sin fricciones en el mercado interior, parece necesario establecer normas que dispongan la prestación de esos servicios. Las autoridades de protección de datos deben desempeñar un papel clave en el desarrollo de dichas normas (p.ej., parámetros, modelos, etc.) y deben poder ejecutar la aplicación de las mismas. Esto requiere también que cuenten con recursos suficientes. Además, las autoridades de protección de datos deben desempeñar un papel en la certificación de organismos de certificación. Esto puede ser particularmente importante en

materia de transferencias internacionales de datos. Dado que la calidad de los servicios y la necesidad de que estos operen en el mercado interior son un criterio clave, la ley deberá crear las condiciones que los lleven a lograr dicha calidad. No parece posible dejar esto al albur del mercado. La experiencia en otras materias como la certificación de mercancías demuestra una tendencia descendente. La competencia entre prestatarios de servicios puede llevar a una reducción de precios y también a cierta flexibilidad o facilitación de los procedimientos. En resumen, sea o no con una base transfronteriza, parecen necesarias normas que garanticen la buena calidad de los servicios y un terreno de juego equitativo.

70. El Grupo de Trabajo del artículo 29 observa que la legislación sobre acreditación vigente[11] puede ser aplicable en materia de servicios de certificación en el campo de la protección de datos. Dicha legislación ofrece ya la estructura necesaria para establecer normas sobre organización y funcionamiento de organismos de acreditación. Estas normas se aplican a la acreditación voluntaria y también en casos específicos en que la acreditación es obligatoria.

71. Evidentemente, este tipo de servicio debería impulsar la armonización de las normas subyacentes en relación con las cuales se analizaran las actuaciones. Las directrices mencionadas (del Grupo de Trabajo del artículo 29 o de la Comisión) que establecieran programas tipo de cumplimiento de las normas serían muy pertinentes.

V. CONCLUSIONES

72. El desarrollo de nuevas tecnologías y la persistente globalización de la economía y la sociedad han llevado a una proliferación de la información personal que se recoge, clasifica, transfiere o conserva. Consiguientemente los riesgos para dichos datos se multiplican.

73. El Grupo de Trabajo del artículo 29 está convencido de que el aumento no solo de los riesgos sino del valor de los datos personales en sí abundan en la necesidad de reforzar el papel y la responsabilidad de los responsables del tratamiento de datos. Un marco normativo que atienda a esta nueva realidad debe incluir las herramientas necesarias para incitar a los responsables del tratamiento a aplicar en la práctica medidas adecuadas y eficaces que cumplan los objetivos de los principios de protección de datos. Procedimientos para garantizar la identificación de todas las operaciones de tratamiento de datos, para tratar las solicitudes de acceso, para la asignación de recursos, incluida la designación de las personas responsables de la organización del cumplimiento de las normas de protección de datos, son ejemplos de dichas medidas.

[11] Reglamento (CE) nº 765/2008 del Parlamento Europeo y del Consejo, de 9 de julio de 2008, por el que se establecen los requisitos de acreditación y vigilancia del mercado relativos a la comercialización de los productos y por el que se deroga el Reglamento (CEE) nº 339/93.

74. Para estimular en la práctica la protección de datos, el Grupo de Trabajo del artículo 29 sugiere primero y ante todo la inclusión en las propuestas de modificación de la Directiva de protección de datos de una nueva disposición que exija que los responsables del tratamiento de datos apliquen medidas adecuadas y eficaces para garantizar el cumplimiento de los principios y obligaciones de la Directiva de protección de datos, demostrándolo ante las autoridades que se lo soliciten. Estas medidas deben fomentar la observancia de los principios y obligaciones de protección de datos a la vez que minimizan los riesgos de acceso no autorizado, abuso, pérdida, etc. La obligación de demostrar la implantación de las medidas necesarias, si así se solicita, sería una herramienta útil para las autoridades de protección de datos en sus funciones ejecutivas.

75. La obligación de ejecutar dichas medidas debe aplicarse a los responsables del tratamiento de datos de todos los sectores (público y privado) y debe poder modularse de modo que el tipo de medidas responda a los riesgos que representen el tratamiento de datos y la naturaleza de los mismos.

Bruselas, 13 de julio de 2010

Por el Grupo de Trabajo
El Presidente
Jacob KOHNSTAMM