Organisation for Economic
Co-operation and Development

DIRECTRICES DE LA OCDE QUE REGULAN LA PROTECCIÓN DE LA PRIVACIDAD Y EL FLUJO TRANSFRONTERIZO DE DATOS PERSONALES

(23 de septiembre de 1980)

ORGANIZACIÓN DE COOPERACIÓN Y DESARROLLO ECONÓMICO

En virtud del artículo 1 del Convenio firmado el 14 de diciembre de 1960 en París, entrado en vigor el 30 de septiembre de 1961, la Organización para la Cooperación y el Desarrollo Económico (OCDE) tiene por objetivo promover políticas dirigidas:

- A conseguir la mayor expansión de la economía y el empleo y una progresión del nivel de vida en los países miembros, manteniendo la estabilidad financiera, y a contribuir así al desarrollo de la economía mundial.

- A contribuir a una sana expansión económica en los países miembros, así como en los países no miembros, en vías de desarrollo económico.

- A contribuir a la expansión del comercio mundial sobre una base multilateral y no discriminatoria, conforme con las obligaciones internacionales.

Los países miembros originales de la OCDE son Alemania, Austria, Bélgica, Canadá, Dinamarca, España, Estados Unidos, Francia, Grecia, Irlanda, Islandia, Italia, Luxemburgo, Noruega, Países Bajos, Portugal, Reino Unido, Suecia, Suiza y Turquía. Los países siguientes se han convertido posteriormente en miembros mediante adhesión en las fechas indicadas: Japón (28 de abril de 1964), Finlandia (28 de enero de 1969), Australia (7 de junio de 1971), Nueva Zelanda (29 de mayo de 1973), México (18 de mayo de 1994), República Checa (12 de diciembre de 1995), Hungría (7 de mayo de 1996), Polonia (22 de noviembre de 1996), Corea (12 de diciembre de 1996) y Eslovaquia (14 de diciembre de 2000). La Comisión de las Comunidades Europeas participa en los trabajos de la OCDE (artículo 13 del Convenio de la OCDE).

NIPO: 326-04-034-7
Catálogo general de publicaciones oficiales
http://publicaciones.administracion.es

Traducción en lengua española realizada de los textos en inglés y/o francés, versiones oficiales de esta publicación, titulados:

OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data

Lignes directrices de l'OCDE sur la protecion de la vie privée et les flux transfrontières de donnes de caractère personnel

RECOMENDACIÓN DEL CONSEJO RELATIVA A LAS DIRECTRICES QUE REGULAN LA PROTECCIÓN DE LA PRIVACIDAD Y EL FLUJO TRANSFRONTERIZO DE DATOS PERSONALES (23 de septiembre de 1980)

EL CONSEJO,

Considerando los artículos 1(c) y 5(b) del Convenio sobre la Organización para la Cooperación y el Desarrollo Económicos de 14 de diciembre de 1860,

RECONOCIENDO:

- que, aunque las leyes y políticas nacionales pueden diferir, los países miembros tienen un interés común en proteger la privacidad y las libertades individuales, así como en reconciliar los valores fundamentales pero contradictorios como la privacidad y el libre flujo de información;
- que el tratamiento automático y los flujos transfronterizos de datos personales crean nuevas formas de relaciones entre los países y requieren la elaboración de normas y prácticas compatibles;
- que los flujos transfronterizos de datos personales contribuyen al desarrollo socioeconómico;
- que la legislación local relativa a la protección de la privacidad y los flujos transfronterizos de personal pueden obstaculizar esos flujos transfronterizos;

decidió fomentar el libre flujo de información entre los Países Miembros y evitar la creación de obstáculos injustificados para el desarrollo de las relaciones socioeconómicas entre los Países Miembros;

Y RECOMIENDA:

1. Que los Países Miembros tengan en cuenta en su legislación interna los principios relativos a la protección de la privacidad y las libertades individuales establecidos en las Directrices contenidas en el Anexo a esta Recomendación y que forma parte del mismo;
2. Que los Países Miembros se esfuercen por eliminar o evitar que aparezcan, en nombre de la protección de la privacidad, obstáculos injustificados para los flujos transfronterizos de datos personales;
3. Que los Países Miembros colaboren en la implantación de las Directrices establecidas en el Anexo;
4. Que los Estados Miembros convengan cuanto antes en los procedimientos específicos de consulta y cooperación para la aplicación de esas Directrices.

Anexo a la Recomendación del Consejo, de 23 de septiembre de 1980, DIRECTRICES QUE REGULAN LA PROTECCIÓN DE LA PRIVACIDAD Y LOS FLUJOS TRANSFRONTERIZOS DE DATOS PERSONALES

PARTE PRIMERA. DEFINICIONES GENERALES

1. Por lo que respecta a estas Directrices:

   a) por "inspector de datos" se entiende una persona que, según la ley del país, es competente para decidir sobre el contenido y el uso de datos personales con independencia de si esos datos son, o no, recogidos, guardados, tratados o divulgados por esa persona o por un representante en su nombre;

   b) por "datos personales" se entiende toda información relativa a un individuo identificado o identificable (sujeto de los datos);

   c) por "flujos transfronterizos de datos personales" se entiende los desplazamientos de datos personales más allá de las fronteras nacionales.

Alcance de las Directrices

2. Estas Directrices se refieren a los datos personales. del sector público o del privado, que, debido al modo en que son tratados, a su naturaleza o al contexto en el que se usan, representan un peligro para la privacidad y las libertades individuales.

3. No se debería interpretar que estas Directrices pueden evitar:

   a) la aplicación, para diferentes categorías de datos personales, de diferentes medidas de protección según su naturaleza y el contexto en el que se recogen, guardan, tratan o divulgan;

   b) la exclusión de la aplicación de las Directrices de los datos personales que no representan ningún riesgo para la privacidad y las libertades individuales; ni

   c) la aplicación de las Directrices sólo al tratamiento automático de datos personales.

4. Las excepciones a los Principios contenidos en las Partes Segunda y Tercera de estas Directrices, incluidas las relativas a la soberanía nacional, la seguridad nacional y la política pública (el "orden público"), deberían ser:

   a) las menos posibles, y

   b) puestas en conocimiento del público.

5. En el caso concreto de los países federales, la observancia de estas Directrices se puede ver afectada por la división de poderes en la Federación.

6. Estas Directrices deberían considerarse como normas mínimas susceptibles de ser complementadas con medidas adicionales para la protección de la privacidad y las libertades individuales.

PARTE SEGUNDA. PRINCIPIOS BÁSICOS DE APLICACIÓN NACIONAL.

Principio de limitación de recogida

7. Debería haber límites a la recogida de datos personales y cualquiera de esos datos debería ser obtenido por medios legales y honestos y, en su caso, con el conocimiento o consentimiento del sujeto de los datos.

Principio de calidad de los datos

8. Los datos personales deberían corresponder a los fines para los que se van a usar y, en la medida en que sean necesarios para esos fines, deberían ser correctos y completos, y estar actualizados.

Principio de especificación de los fines

9. Los fines para los que los datos personales se recogen deberían especificarse en el momento en que se recogen, y su uso posterior estaría limitado al cumplimiento de esos fines o de otros que no sean incompatibles con esos fines y se especifiquen cada vez que haya un cambio de fines.

Principio de limitación de uso

10. Los datos personales no se deberían revelar, poner a disposición del público ni usar para fines que no sean los especificados de conformidad con el apartado 9 anterior, excepto:

    a) con el consentimiento del sujeto de los datos; o

    b) por imperativo legal.

Principio de salvaguarda de la seguridad

11. Los datos personales deberían estar protegidos por las oportunas medidas de salvaguarda contra riesgos como pérdida o acceso no autorizado, destrucción, uso, modificación o revelación de datos.

Principio de transparencia

12. Debería haber una política general de transparencia en lo concerniente al tratamiento, el uso y las políticas relativos a los datos personales. Se deberían poner los medios para establecer la existencia y la naturaleza de los datos personales, así como los fines principales para los que se van a usar, así como la identidad y el domicilio habitual del inspector de datos.

Principio de participación individual

13. Toda persona física debería tener derecho a:

    a) conseguir, a través de un inspector de datos o de otra manera, la confirmación de si el inspector tiene o no tiene datos relativos a su persona;

    b) que se le comunique cualquier dato relativo a ella:

        1.
        - en un plazo de tiempo razonable;

- con una tarifa, en su caso, que no sea excesiva;
- de manera razonable; y
- de forma que pueda entender fácilmente;

2.

c) que se le den las razones de porqué se rechaza una petición hecha de conformidad con lo establecido en los apartados (a) y (b), y poder recurrir ese rechazo;

d) recusar los datos relativos a ella y, si la recusación tiene éxito, hacer que se eliminen, rectifiquen, completen o modifiquen los datos.

Principio de responsabilidad

14. A todo inspector de datos se le deberían pedir responsabilidades por el cumplimiento de las medidas que permiten la aplicación de los principios antes expuestos.

PARTE TERCERA. PRINCIPIOS BÁSICOS DE APLICACIÓN INTERNACIONAL: LIBRE FLUJO Y RESTRICCIONES LEGÍTIMAS

15. Todo País Miembro debería tener en cuenta las implicaciones para los demás Países Miembros del tratamiento nacional y la re-exportación de datos personales.

16. Los Países Miembros deberían tomar todas las medidas oportunas y razonables para garantizar que los flujos transfronterizos de datos personales, incluido el tránsito a través de un País Miembro, sea ininterrumpido y seguro.

17. Todo País Miembro debería evitar el restringir los flujos transfronterizos de datos personales entre él y otro País Miembro, excepto si éste último todavía no respeta sustancialmente estas Directrices o si la re-exportación de esos datos pudiera transgredir su legislación nacional sobre privacidad. Pero un País Miembro puede imponer restricciones respecto de ciertas categorías de datos personales para los que su legislación doméstica sobre privacidad contempla normas concretas dictadas por la naturaleza de esos datos, y para los que los demás Estados Miembros no tienen prevista una protección similar.

18. Los Países miembros deberían evitar el elaborar leyes, políticas y prácticas en nombre de la protección de la privacidad y las libertades individuales que pudieran crear obstáculos a los flujos transfronterizos de datos personales que se excedieran en requisitos para esa protección.

PARTE CUARTA. IMPLANTACIÓN NACIONAL

19. Al implantar a nivel nacional los principios establecido en las Partes Segunda y Tercera, los Países Miembros deberían establecer procedimientos o instituciones legales, administrativos o de otro tipo para la protección de la privacidad y las libertades individuales en relación con los datos personales. Los Países miembros deberían ocuparse en especial de:

a) aprobar la legislación nacional adecuada;

b) fomentar y respaldar la autorregulación, bien en forma de códigos de conducta o de otra manera;

c) facilitar los oportunos medios para que las personas físicas puedan ejercer sus derechos;

d) procurar las oportunas sanciones y soluciones en caso de incumplimiento a través de medidas que pongan en práctica los principios establecidos en las Partes Segunda y tercera; y

e) garantizar que no haya discriminación desleal contra los sujetos de los datos.

PARTE QUINTA. COOPERACIÓN INTERNACIONAL

20. Los Países Miembros deberían poner en conocimiento de otros Países Miembros, cuando así se los pidan, la información relativa a la observancia de los principios establecidos en estas Directrices. Además, los Países Miembros deberían garantizar que los procedimientos relativos a los flujos transfronterizos de datos personales y a la protección de la privacidad y las libertades individuales son sencillos y compatibles con los de los otros Países Miembros que observan estas Directrices.

21. Los Países Miembros deberían establecer procedimientos para facilitar:

- el intercambio de información relativa a estas Directrices, Y
- la ayuda mutua en los asuntos de investigación y procedimiento en cuestión.

22. Los Países Miembros deberían trabajar en la elaboración de principios, nacionales e internacionales, que regulen la ley aplicable en el caso de flujos transfronterizos de datos personales.

MEMORIA EXPLICATIVA - INTRODUCCIÓN

Uno de los rasgos de los países miembros de la OCDE en la pasada década ha sido la elaboración de leyes para la protección de la privacidad. Estas leyes han mostrado una tendencia a asumir diferentes formas según los países, y en muchos de ellos aún se están elaborando. La disparidad de la legislación puede crear obstáculos al libre flujo de información entre países. Dichos flujos se han incrementado en gran manera en los últimos años y están abocados a seguir aumentando debido a la introducción de nueva tecnología informática y de la comunicación. La OCDE, que lleva años con una actitud activa en este campo, decidió ocuparse del problema de separarse de la legislación propia de cada país y en 1976 encargó a un Gripo de Expertos que elaborara unas Directrices sobre las normas básicas que han de regir el flujo transfronterizo y la protección de los datos personales y la privacidad, para así facilitar la armonización de la legislación nacional. El gripo ya ha terminado el trabajo.

Las Directrices son amplias y reflejan el debate y el trabajo legislativo que se ha estado haciendo durante varios años en los países miembros. El Grupo de Expertos que preparó las Directrices ha considerado fundamental el emitir una Memoria Explicativa que acompañe al trabajo. Su objeto es explicar y elaborar las Directrices y los problemas básicos de protección de la privacidad y las libertades individuales. Llama la atención sobre temas clave que han surgido en las discusiones de las Directrices y explica las razones que llevaron a la elección de soluciones concretas.

La Primera Parte de la Memoria da un información básica general sobre el área de interés tal y como la conciben los países miembros. Explica la necesidad de la actuación internacional y resume el trabajo realizado hasta el momento por la OCDE y algunos otros organismos internacionales. Concluye con una lista de los principales problemas con los que el Grupo de Expertos e encontró durante el trabajo.

La Segunda Parte se divide en dos secciones. La primera contiene comentarios sobre ciertos rasgos generales de las Directrices, y la segunda comentarios detallados sobre apartados concretos.

Esta Memoria es un documento informativo, preparado para explicar y describir en general el trabajo del Grupo de Expertos. Queda subordinada a las Directrices y no puede variar el significado de las Directrices, pero se facilita para ayudar a una mejor interpretación y aplicación de las mismas.

I. ANTECEDENTES GENERALES.

Los problemas.

1. La década de los 70 se puede describir como un período de intensificación de las actividades legislativas y de investigación sobre la protección de la privacidad en relación con la recogida y el uso de los datos personales. Numerosos informes oficiales muestran que los problemas se toman en serio a nivel político y al mismo tiempo que la tarea de equilibrar intereses opuestos es delicada y no es probable que se realice de una vez y ya está. El interés público ha tendido a centrarse en los riesgos e implicaciones asociados con el proceso informatizado de los datos personales, y algunos países han optado por promulgar normas legislativas que se refieren exclusivamente a los ordenadores y las actividades informáticas. Otros países han preferido un enfoque más general a los temas de la protección de la privacidad con independencia de la tecnología concreta del proceso de datos utilizada.

2. Las soluciones que se están discutiendo son sobre todo modos de salvaguardar al individuo, lo que evitará que se invada la privacidad en sentido clásico como, por ejemplo, que se usen mal o se difundan datos personales íntimos; pero han quedado a la vista otras necesidades de protección más o menos estrechamente relacionadas. La obligación que tienen los conservadores de los registros de informar al público en general sobre las actividades referidas al proceso de

datos, y los derechos de los sujetos de los datos a que los datos a ellos referidos se completen o modifiquen, son dos ejemplos escogidos al azar. Hablando en términos generales, ha existido una tendencia a ampliar el concepto tradicional de privacidad ("el derecho a que le dejen a uno solo") y a identificar con esta palabra a una síntesis de intereses más compleja que quizá debiera denominarse más correctamente como privacidad y libertades individuales.

3. Por lo que respecta a los problemas legales del proceso automático de datos (PAD, ADP en inglés), la protección de la privacidad y las libertades individuales constituye quizás el aspecto que más se ha debatido. Entre las razones de esa preocupación tan amplia están el uso ubicuo de los ordenadores para procesar los datos personales, las posibilidades – mucho mayores – de almacenar, comparar, enlazar, seleccionar y acceder a los datos personales, y la combinación de los ordenadores con la tecnología de la información que permite poner los datos personales a disposición de miles de usuarios, ubicados en localidades geográficas distantes entre sí, al mismo tiempo, y permite la reunión de datos y la creación de redes complejas de datos tanto nacionales como internacionales. Ciertos problemas exigen una atención especialmente urgente, como es el caso de los relativos a las nuevas redes de datos internacionales, y la necesidad de equilibrar los intereses contrapuestos de privacidad por una parte y libertad de información por la otra, para permitir la plena explotación de las posibilidades que brindan las modernas tecnologías para el proceso siempre que sea razonable.

Actividades a nivel nacional.

4. De los países miembros de la OCDE, más de in tercio han promulgado hasta ahora una o varias leyes que, entre otras cosas, pretenden proteger a los particulares frente al mal uso de datos relativos a ellos y les dan el derecho a acceder a los datos para comprobar su veracidad y corrección. En los Estados federales, podemos encontrar leyes de este tipo tanto a nivel nacional como provincial/estatal. En los diferentes países se hace referencia a estas leyes de distinta manera. En la Europa continental se suele hablar de "leyes sobre los datos" o "leyes sobre la protección de datos", mientras que en los países de habla inglesa se conocen normalmente como "leyes sobre la protección de la privacidad". La mayoría de estar normas legislativas se promulgaron después de 1973 y en el momento actual esta actividad legislativa se ha continuado e incluso ampliado. Los países que ya cuentan con leyes en vigor están interesándose ahora por nuevas áreas de protección o bien han empezado a revisar o complementar las ya existentes. Otros países se empiezan a implicar ahora y tienen proyectos de ley pendientes de aprobación o están estudiando los problemas con vistas a elaborar la oportuna legislación. Estos esfuerzos realizados en cada país, sin olvidar los amplios informes y documentos de investigación elaborados por los comités públicos u organismos similares, contribuyen a aclarar cuáles son los problemas y las ventajas e implicaciones de las distintas soluciones. En la etapa actual, facilitan una base sólida para la actuación internacional.

5. Los planteamientos para la protección de la privacidad y las libertades individuales adoptados por los diferentes países tienen muchos rasgos en común. Así pues, es posible identificar ciertos intereses o valores básicos que normalmente se consideran componentes básicos del área de protección. Algunos principios fundamentales de este tipo son: establecer límites a la recogida de datos personales de acuerdo con los objetivos de quien recoge los mismos y criterios similares; restringir el uso de los datos a los objetivos claramente indicados; crear los medios para que los particulares tengan conocimiento de la existencia y los contenidos de los datos y poder corregirlos; e identificar a los responsables de la adecuación de las leyes y decisiones sobre protección de la privacidad. Hablando en términos generales, las leyes que protegen la privacidad y las libertades individuales en relación a los datos personales intentan cubrir las sucesivas etapas del ciclo que comienza con la recogida inicial de los datos y termina con el hecho de borrar los mismos u otras medidas similares, y garantizar al máximo el conocimiento, la participación y el control individuales.

6. Las diferencias entre los planteamientos nacionales como aparecen actualmente en las leyes, proyectos o proposiciones de ley se refieren a aspectos como el ámbito de la ley, el énfasis que se pone en los diferentes elementos de protección, la puesta en marcha detallada de los amplios principios indicados anteriormente, y la maquinaria de aplicación. Así pues, las opiniones varían en

cuanto a autorizar los requisitos y mecanismos de control en forma de írganos supervisores especiales ("entidades de inspección de datos"). Las categorías de los datos sensibles se definen de otra manera, los medios para asegurar la apertura y la participación individual varían, y esto sólo por dar algunos ejemplos. Naturalmente, las diferencias tradicionales existentes entre los sistemas legales producen disparidad, tanto respecto a los planteamientos legislativos como a la formulación detallada del marco regulador de la protección de los datos personales.

Aspectos internacionales de la privacidad y los bancos de datos.

7. Debido a ciertas razones, los problemas derivados de la elaboración de medidas de protección para los individuos en lo relativo a la manipulación de datos personales no se pueden resolver exclusivamente a nivel nacional. El enorme aumento de flujos de datos a través de las fronteras y la creación de bancos de datos internacionales (conjuntos de datos destinados a su recuperación u otros fines) han puesto de manifiesto la necesidad de una actuación nacional concertada y, al mismo tiempo, de argumentos de apoyo a favor del libre flujo de información que deben ser equilibrado con frecuencia frente a los exigencias de la protección de datos y de las restricciones sobre su recogida, proceso y difusión.

8. Una preocupación básica a nivel internacional es el consenso sobre los principios fundamentales en los que se debe basar la protección del individuo. Ese consenso obviaría o reduciría las razones para regular la exportación de datos y facilitar la resolución de los problemas o conflictos de las leyes. Además, constituiría un primer paso hacia la elaboración de acuerdos internacionales vinculantes y más detallados.

9. Hay otras razones por las que la regulación del proceso de los datos personales debería considerarse en un contexto internacional: los principios implicaban valores de preocupación que muchos países están ansiosos por defender y ver cómo son aceptados por todos; pueden ayudar a ahorrar costes en el tráfico de datos internacional; los países tienen un interés común en evitar la creación de lugares donde las normativas nacionales sobre el proceso de datos se puedan burlar con facilidad; de hecho, a la vista de la movilidad internacional de personas, mercancías y actividades científicas y comerciales, las prácticas comúnmente aceptadas con respecto al proceso de datos, pueden ser ventajosas incluso cuando el tráfico de datos transfronterizo no está directamente implicado.

Actividades internacionales relacionadas.

10. Hay varios acuerdos internacionales sobre distintos aspectos de las telecomunicaciones que, a la vez que facilitan las relaciones y la cooperación entre los países, reconocen el derecho soberanote cada país a regular sus propias telecomunicaciones (Convenio sobre las Telecomunicaciones Internacionales de 1973). La protección de los datos y programas informáticos ha sido investigada, entre otros, por la Organización Mundial de la Propiedad Intelectual que ha elaborado un borrador de disposiciones para las leyes nacionales sobre la protección del software informático. Se pueden encontrar acuerdos especializados tendentes a la cooperación informativa en distintas áreas, como son la aplicación de las leyes, los servicios sanitarios, los servicios estadísticos y judiciales (por ejemplo, respecto a la toma de pruebas).

11. Algunos acuerdos internacionales tratan de un modo más general de temas que actualmente están en discusión, como la protección de la privacidad y la libre difusión de la información. Podemos citar el Convenio europeo de Derechos Humanos de 4 de noviembre de 1950 y el Convenio Internacional de Derechos Políticos y Civiles (Naciones Unidas, 19 de diciembre de 1966).

12. No obstante, a la vista de lo inadecuado de los instrumentos internacionales existentes sobre el proceso de datos y los derechos individuales, algunas entidades internacionales han realizado estudios detallados de los problemas implicados para encontrar mejores soluciones a los mismos.

13. En 1973 y 1974 el Comité de Ministros del Consejo de Europa adoptó dos resoluciones

referentes a la protección de la privacidad de los particulares frente a los bancos de datos electrónicos en los sectores público y privado respectivamente. Ambas resoluciones recomendaban que los gobiernos de los estados miembros del Consejo de Europa tomaran medidas para la aplicación de ciertos principios básicos de protección relativos a la obtención de datos, la calidad de los datos y los derechos de los particulares a ser informados sobre los datos y las actividades de proceso de los mismos..

14. Posteriormente, el Consejo de Europa, siguiendo las instrucciones de sus Comités de Ministros, comenzó a preparar un Convenio internacional sobre protección de la privacidad en relación al proceso de datos en el extranjero y trasfronterizo. También comenzó a trabajar sobre las regulaciones de modelos para los bancos de datos transfronterizos y las normas de conducta para los profesionales del proceso de datos. El Comité de Ministros adoptó el Convenio el 17 de septiembre de 1980. Este convenio persigue el establecimiento de los principios básicos sobre la protección de datos que habrán de aplicarse en los países miembros, la reducción de las restricciones sobre los flujos de datos transfronterizos entre las Partes Contratantes teniendo en cuenta la reciprocidad, el logro de la cooperación entre las autoridades de cada país encargadas de la protección de datos y establecer un Comité Consultivo para la aplicación y el desarrollo continuo del convenio.

15. La Comunidad Europea ha llevado a cabo estudios relativos al problema de armonización de las legislaciones de cada país dentro de la Comunidad en relación a los flujos de datos transfronterizos y las posibles distorsiones de la competitividad, los problemas de la seguridad de los datos y su confidencialidad y la naturaleza de los flujos de datos transfronterizos. A principios de 1978, un subcomité del parlamento Europeo realizó una vista pública sobre el proceso de datos y los derechos de los particulares. Su trabajo se materializó en un informe al Parlamento Europeo en la primavera de 1979. Este informe, que fue adoptado por el parlamento Europeo en mayo de 1979, contiene una resolución sobre la protección de los derechos de los particulares frente a los avances técnicos sobre el proceso de datos.

Actividades de la OCDE

16. El programa de la OCDE sobre los flujos de datos transfronterizos deriva de los estudios sobre la utilización de los ordenadores en el sector público que se inició en 1969. Un Grupo de Expertos, el Jurado/Panel de Banco de Datos, analizó y estudió diferentes aspectos del tema de la privacidad, por ejemplo en relación a la información digital, la administración pública, los flujos de datos transfronterizos y las implicaciones de las políticas en general. Para demostrar la naturaleza de los problemas, el Jurado de Bancos de Datos organizó un Simposium en Viena en 1977 en el que se recogieron opiniones y experiencias de diversos sectores como, entre otros, el gobierno, la industria, los usuarios de redes de comunicación de datos, los servicios de proceso y organizaciones intergubernamentales interesadas.

17. Se elaboraron algunos principios orientadores en un marco general de cara a una posible actuación internacional. Estos principios reconocían (a) la necesidad, en general, de flujos de información continuos e ininterrumpidos entre países, (b) los intereses legítimos de los países en evitar toda transferencia de datos que sea peligrosa para su seguridad o contraria a sus leyes sobre orden público y decencia o que viole los derechos de sus ciudadanos, (c) el valor económico de la información y la importancia de proteger el "comercio de datos" mediante normas aceptadas de leal competencia, (d) la necesidad de garantías de seguridad para minimizar las violaciones de los datos registrados y el mal uso de la información personal, y (e) la significación de un compromiso de los países para establecer un conjunto de principios fundamentales para la protección de la información personal.

18. A principios de 1978 en la OCDE se estableció un nuevo Grupo de Expertos ad hoc sobre las barreras a los Datos Transfronterizos y la Protección de la Privacidad. A este Grupo se le encargó que elaborara unas directrices sobre las normas básicas que regirían el flujo transfronterizo y la protección de los datos personales y la privacidad, para así facilitar la armonización de las diversas legislaciones nacionales sin que ello excluyera el posterior establecimiento de un Convenio

internacional. Este trabajo tenía que llevarse a cabo en estrecha cooperación con el Consejo de Europa y la Comunidad Europea y estar listo el 1º de julio de 1979.

19. El Grupo de Expertos, presidido por el Juez Kirby, de Australia, y con la asistencia del Dr. Peter Seipel (Asesor), elaboró diversos borradores y discutió varios informes que contenían, por ejemplo, análisis comparativos de diferentes planteamientos sobre la legislación en este campo. Mostró una especial preocupación respecto a ciertos temas que se indican a continuación.

a) El tema de los hechos sensibles y concretos

Surgió la cuestión de si las Directrices serían de carácter general o si se estructurarían para tratar con diferentes tipos de datos o actividades (por ejemplo, los informes sobre créditos). De hecho, puede que no sea posible identificar un conjunto de datos que se vean universalmente como sensibles.

b) El tema del ADP

El argumento de que el ADP es la causa principal de preocupación es dudoso y, de hecho, puesto en cuestión.

c) El tema de las personas jurídicas

Algunas leyes nacionales, pero ciertamente no todas, protegen los datos relativos a las personas jurídicas de manera similar a como lo hacen con los datos relativos las personas físicas.

d) El tema de las sanciones y recursos
Los planteamientos para controlar los mecanismos varían mucho: por ejemplo, los planes que implican la supervisión y autorización por parte de autoridades especialmente constituidas al efecto podrían compararse a los planes que implican una conformidad voluntaria de los conservadores de registros y una confianza en los recursos judiciales tradicionales de los Tribunales.

e) El tema de la puesta en marcha o de la maquinaria básica
La elección de los principios fundamentales y su nivel de detalle apropiado presenta ciertas dificultades. Por ejemplo, hasta que punto las cuestiones sobre la seguridad de los datos (protección de datos frente a interferencias no autorizadas, incendios y hechos similares) deberían verse como parte del conjunto de la protección de la privacidad es discutible; las opiniones pueden diferir en cuanto a los límites temporales para la retención, o los requisitos para su borrado, de los datos y lo mismo vale para los requisitos sobre datos importantes para fines concretos. Es particularmente difícil trazar una clara línea divisoria entre el nivel de los principios u objetivos básicos y las cuestiones de "maquinaria", de nivel inferior, que deberían dejarse a la puesta en marcha local.

f) El tema de la elección de la ley

Los problemas de la elección de la jurisdicción y la ley aplicable y del reconocimiento de las sentencias extranjeras han demostrado ser complejos en el contexto de los flujos de datos transfronterizos. No obstante, se plantea la cuestión de si y en qué medida debería intentarse en esta etapa el proponer soluciones en las Directrices de carácter no vinculante.

g) El tema de las excepciones

Las opiniones sobre la cuestión de las excepciones también pueden variar. ¿Son necesarias? Si lo son, ¿deberían facilitarse categorías particulares de excepciones o se deberían poner límites generales a las excepciones?.

h) El tema de la predisposición.
Para terminar, existe un interesante conflicto entre la protección y el libre flujo transfronterizo de

datos personales. Se debe hacer hincapié en uno o en otro, y es difícil distinguir entre los intereses de la protección de la privacidad y otros intereses relativos al comercio, la cultura, la soberanía nacional, etc., etc.

20. Durante su trabajo, el Grupo de Expertos mantuvo estrechos contactos con los órganos correspondientes del Consejo de Europa. Se hizo todo lo posible para evitar diferencias innecesarias entre los textos elaborados por los dos organismos; así pues, el conjunto de principios básicos de protección son en muchos aspectos similares. Por otra parte, se dan ciertas diferencias. Para empezar, las Directrices de la OCDE no son legalmente vinculantes, considerando que el Consejo de Europa ha elaborado un convenio que será legalmente vinculante en los países que lo ratifiquen. Esto a su vez significa que la cuestión de las excepciones se ha tratado con más detalle por el consejo de Europa. En cuanto al área de aplicación, el Convenio del consejo de Europa se ocupa en primer lugar del proceso automático de datos personales mientras que las Directrices de la OCDE se aplican a los datos personales que implican peligros para la privacidad y las libertades individuales, con independencia de los métodos y la maquinaria usada en su tratamiento. En lo que se refiere a los detalles, los principios básicos de protección propuestos por los dos organismos no son idénticos y la terminología empleada difiere en algunos aspectos. El marco institucional para la cooperación continua se trata con más detalle en el convenio del consejo de Europa que en las Directrices de la OCDE.

21. El Grupo de Expertos también mantuvo la cooperación con la Comisión de las Comunidades Europeas tal y como requería su mandato.

II. LAS DIRECTRICES

A. FINES Y OBJETIVOS

Aspectos generales.

22. En el Preámbulo de la Recomendación se indican los temas básicos que requieren una actuación. En la Recomendación se afirma el compromiso de los Países Miembros de proteger la privacidad y las libertades individuales y de respetar el flujo transfronterizo de datos personales.

23. Las Directrices expuestas en el Anexo a la Recomendación constan de cinco partes. La Parte Primera contiene una serie de definiciones y en ella se especifica el objetivo de las directrices, indicando que representan normas mínimas. La Parte Segunda contiene ocho principios básicos (Apartados 7 a 14) relativos a la protección de la privacidad y las libertades individuales a nivel nacional. La Parte Tercera se ocupa de los principios de aplicación internacional, es decir principios que tienen sobre todo que ver con las relaciones entre los países Miembros.

24. La Parte Cuarta trata, en términos generales, con los medios para poner en marcha los principios básicos expuestos en las partes anteriores y en ella se especifica que esos principios deberían aplicarse sin discriminaciones. La Parte Quinta se ocupa de asuntos de asistencia mutua entre los países Miembros, principalmente a través del intercambio de información y evitando procedimientos nacionales incompatibles para la protección de los datos personales. Termina con una referencia a temas relativos a la ley aplicable que pueden surgir cuando en el flujo de datos personales intervienen varios países Miembros.

Objetivos

25. El meollo de las Directrices consiste en los principios expresados en la Parte Segunda del anexo. Se recomienda a los países Miembros que se adhieran a esos principios con vistas a: a) conseguir que los países Miembros acepten ciertas normas mínimas de protección de la privacidad y las libertades individuales respecto a los datos personales;
b) reducir todo lo posible las diferencias entre las correspondientes normas locales y las prácticas de los países Miembros;

c) asegurarse de que al proteger los datos personales tienen en cuenta los intereses de otros países Miembros y la necesidad de evitar toda indebida interferencia con los flujos de datos personales entre los países Miembros; y
d) eliminar, en la medida de lo posible, las razones que podrían inducir a los países Miembros a restringir los flujos transfronterizos de datos personales por los posibles riesgos que dichos flujos conllevan.

26. Por último, las Partes Cuarta y Quinta de las Directrices contienen principios tendentes a garantizar:
a) eficaces medidas nacionales para la protección de la privacidad y las libertades individuales;
b) que se evitan las prácticas que implican toda injusta discriminación entre los individuos; y
c) las bases para una cooperación internacional continua y procedimientos compatibles en toda regulación sobre los flujos personales de datos personales.

Nivel de detalle

27. Lo pormenorizadas que puedan ser las Directrices dependiendo de dos factores principales, a saber: a) la amplitud del consenso alcanzado sobre las soluciones planteadas, y b) el conocimiento y la experiencia disponibles que indican las soluciones que se han de adoptar en esta etapa. Por ejemplo, el Principio de Participación Individual (apartado 13) trata concretamente de varios aspectos del hecho de proteger los intereses de un individuo, mientras que la disposición sobre los problemas de elección de la ley y asuntos afines (Apartado 22) simplemente establece un punto de partida para el gradual desarrollo de planteamientos comunes detallados y acuerdos internacionales. En su conjunto, las directrices constituyen un marco general para las actuaciones concertadas de los países Miembros: los objetivos establecidos en las directrices se pueden perseguir de distintas maneras, según los instrumentos legales y estrategias preferidas por los países Miembros para su puesta en marcha. Para terminar, existe la necesidad de una revisión continua de las directrices, tanto por parte de los países Miembros como de la OCDE. A medida que se vaya adquiriendo experiencia, puede que haya que ir revisando y perfeccionando las Directrices.

Países no miembros

28. La Recomendación se dirige a los países Miembros y se traduce en varias disposiciones expresamente limitadas a las relaciones entre los países Miembros (véanse los Apartados 15, 17 y 20 de las directrices). No obstante, es deseable que haya un amplio reconocimiento de las Directrices, y nada en ellas debería interpretarse como algo que puede hacer que los países Miembros vayan a impedir a los países no miembros la aplicación de ciertas disposiciones. A la vista del aumento de los flujos de datos transfronterizos y la necesidad de garantizar soluciones concertadas, se ha hecho lo posible para llamar la atención de los países no miembros y de los oportunos organismos internacionales sobre las Directrices.

Una mayor perspectiva reguladora

29. Anteriormente se ha señalado que la protección de la privacidad y las libertades individuales constituye unos de los muchos aspectos legales, en parte coincidentes, implicados en el proceso de datos. Las Directrices son un nuevo instrumento, añadido a otros instrumentos internacionales afines que rigen temas como los derechos humanos, las telecomunicaciones, el comercio internacional, el derecho de propiedad intelectual y distintos servicios de información. Si fuera necesario, los principios establecidos en las Directrices se podrían revisar y completar en el marco de las actividades desempeñadas por la OCDE en el campo de las políticas sobre información, informática y comunicaciones.

30. Algunos países Miembros han hecho hincapié en las ventajas de un Convenio internacional vinculante de amplia cobertura. El Mandato del Grupo de Expertos le exigía a éstos que elaboraran directrices sobre las normas básicas que rigen el flujo transfronterizo y la protección de los datos personales y la privacidad, y ello sin excluir que en una etapa posterior se establezca un Convenio

internacional de carácter vinculante. Las directrices podrían servir como punto de partida para la elaboración de un Convenio internacional cuando sea necesario.

Personas jurídicas, grupos y entidades similares

31. Algunos países consideran que la protección requerida para los datos relativos a los individuos puede ser de carácter similar a la requerida para los datos relativos a las empresas mercantiles, las asociaciones y los grupos que pueden o no tener personalidad jurídica. La experiencia de ciertos países también indica que es difícil definir claramente la línea divisoria entre datos personales y datos no personales. Por ejemplo, los datos relativos a una pequeña empresa también pueden tener que ver con su propietario o propietarios y dar información personal de carácter más o menos sensible. En esos casos, puede ser aconsejable ampliar a las entidades empresariales la protección ofrecida por las normas sobre los datos personales.

32. También es discutible en qué medida la gente que pertenece a un grupo concreto (por ejemplo, discapacitados mentales, inmigrantes, minorías étnicas) necesitan una protección adicional contra la difusión de información relativa a dicho grupo.

33. Por otra parte, las Directrices reflejan la opinión de que las nociones de integridad individual y privacidad son en muchos aspectos individuales y no deberían tratarse de la misma manera que la integridad de un grupo de personas, o la seguridad y confidencialidad empresariales. Las necesidades de protección son distintas y también lo son los marcos de políticas en los que se han de formular las soluciones y los intereses equilibrados entre sí. Algunos miembros del grupo de expertos sugirieron que se debería prever la posibilidad de ampliar las directrices a las personas jurídicas (empresas, asociaciones). Esta sugerencia no obtuvo el consenso necesario. Así pues, el alcance de las Directrices se limita a los datos relativos a los individuos y se deja a los países Miembros que tracen las líneas divisorias y decidan las políticas en relación a las empresas, los grupos y entes similares (véase el apartado 49 más adelante).

Datos automatizados y no automatizados

34. En el pasado, las actividades de la OCDE sobre protección de la privacidad y campos afines se centró en el proceso automático de datos y en las redes informáticas. El Grupo de Expertos prestó especial atención al tema de si estas directrices deberían o no restringirse al proceso automático y asistido por ordenador de los datos personales. Este planteamiento puede defenderse en relación a varios campos, como los peligros concretos para la privacidad individual provocados por la automatización y los bancos de datos computerizados y el creciente dominio de los métodos automáticos de proceso de datos, especialmente en lo relativo a los flujos de datos transfronterizos, así como el marco concreto de las políticas sobre información, informática y comunicaciones en el que el grupo de Expertos ha previsto cumplir su Mandato.

35. Por otra parte, el Grupo de Expertos ha concluido que limitar las Directrices al proceso automático de datos personales tendría grandes inconvenientes. Para empezar, es difícil, hablando de definiciones, hacer una clara distinción entre el tratamiento de datos automático y no automático. Hay, por ejemplo, sistemas de proceso de datos "mixtos", y etapas en el proceso de datos que pueden llevar o no a un tratamiento automático. Estas dificultades suelen verse complicadas aún más por los permanentes avances tecnológicos, como la introducción de avanzados métodos semiautomáticos basados en el uso del microfilm, o microordenadores que se pueden usar cada vez más para fines privados que son inofensivos e imposibles de controlar. Además, al concentrase exclusivamente en los ordenadores, las Directrices podrían llegar a ser inconsecuentes y tener lagunas, y dar oportunidades a los conservadores de registros de contravenir las normas que ponen en marcha las directrices usando métodos no automáticos para fines que pueden ser delictivos.

36. Debido a las dificultades citadas, las directrices no dan una definición de "proceso automático de datos", aunque se hace referencia al concepto en el preámbulo y en el apartado 3 del anexo. Se puede considerar que en fuentes como glosarios técnicos normales se puede encontrar

orientación para la interpretación de este concepto.

37. Los principios para la protección de la privacidad y las libertades individuales expresados en las Directrices son válidos sobre todo para el proceso de datos en general, con independencia de la tecnología concreta empleada. Por ello las directrices se refieren a los datos personales en general o, más concretamente, a los datos personales que, dada la manera en que son procesados o su carácter o contexto, representan un peligro para la privacidad y las libertades individuales.

38. No obstante, habría que observar que las Directrices no constituyen un conjunto de principios generales sobre la protección de la privacidad; las invasiones de la privacidad por parte de, por ejemplo, la fotografía franca, el maltrato físico o la difamación quedan fuera de su objeto a menos que tales actos tengan que ver de alguna manera con el tratamiento de los datos personales. Así pues, las directrices se ocupan de la construcción y uso de conjuntos de datos organizados para la recuperación, la toma de decisiones, la investigación, los estudios y otros fines similares. Se debería hacer hincapié en que las directrices son neutrales respecto a la tecnología concreta empleada; los métodos automáticos no son más que uno de los problemas planteados en las directrices aunque, especialmente en el contexto de los flujos de datos transfronterizos, es decididamente un problema importante.

B. COMENTARIOS PORMENORIZADOS

Aspectos generales

39. Los siguientes comentarios se refieren a las Directrices indicadas en el anexo a la Recomendación. Intentan aclarar el debate habido en el Grupo de Expertos.

Apartado 1: Definiciones

40. La lista de definiciones se ha quedado corta. La expresión "controlador de datos" es de vital importancia. Trata de definir a un sujeto que, según la ley local, tendría la responsabilidad última de las actividades relativas al proceso de datos personales. Tal y como se define, el controlador de datos es alguien con competencia legal para decidir sobre el contenido y uso de los datos, con independencia de si tales datos son o no recogidos, almacenados, procesados o difundidos por él o por un agente en su nombre. La definición excluye por lo menos a cuatro categorías que pueden tener que ver en el proceso de datos, como a) las autoridades autorizadoras y órganos similares que existen en algunos países Miembros y que autorizan el proceso de datos pero no están facultados para decidir (en el sentido propio de la palabra) qué actividades deberían realizarse y para qué fines; b) las oficinas de servicios de proceso de datos que realizan el proceso de datos en nombre de otros; c) las autoridades de telecomunicaciones y órganos similares que actúan como meros conductos; y d) los "usuarios dependientes" que pueden tener acceso a los datos pero no están autorizados a decidir qué datos habría que almacenar, quién podría usarlos, etc. Al poner en marcha las Directrices, los países pueden elaborar modelos más complejos de niveles y tipos de responsabilidades. En los apartados 14 a 19 de las Directrices se da una orientación sobre lo que se puede hacer en esta dirección.

41. Las expresiones "datos personales" y "sujeto de datos" sirven para subrayar que las Directrices se refieren a personas físicas. La línea divisoria precisa entre los datos personales en el sentido de la información relativa a individuos identificados o identificables y datos anónimos puede resultar difícil de trazar y se debe dejar a la regulación de cada país Miembro. En principio, los datos personales llevan información que por enlaces directos (como un número de registro civil) o indirectos (como una dirección) pueden ser relacionados con una persona física concreta.

42. La expresión "flujos de datos personales transfronterizos" restringe la aplicación de ciertas disposiciones de las directrices a los flujos de datos internacionales y en consecuencia omite los problemas de flujos de datos de los estados federales. Los movimientos de datos tendrán lugar con frecuencia a través de transmisiones electrónicas, pero también pueden emplearse otros

medios de comunicación de datos. Los flujos transfronterizos tal y como se entienden en las Directrices incluyen la transmisión de datos por satélite.

Apartado 2: Área de aplicación

43. La sección de la Memoria que se ocupa del alcance y objeto de las Directrices introduce el tema de su aplicación al proceso automático de datos personales frente al no automático. En el Apartado 2 de las Directrices, que se ocupa de este problema, se basa en dos criterios limitadores. El primero tiene que ver con el concepto de datos personales: las Directrices se refieren a datos que se pueden relacionar con individuos identificados o identificables. No se incluyen las recogidas de datos que no ofrecen esas posibilidades (recogidas de datos estadísticos de forma anónima). El segundo criterio es más complejo y se refiere a un elemento de riesgo concreto de carácter objetivo, es decir que los datos presentan un peligro para la privacidad y las libertades individuales. Estos peligros pueden surgir debido al uso de métodos de proceso automático de datos (la manera en que los datos se procesan), pero también hay otra serie de fuentes de riesgos posibles. Así, los datos que en sí mismos son simples y objetivos pueden ser utilizados en un contexto en el que pasan a ser lesivos para un sujeto de datos. Por otra parte, los riesgos tal y como se expresan en el apartado 2 de las Directrices no se refieren a las recogidas de datos de carácter obviamente inocente (como las libretas personales). Los peligros de los que se habla en el Apartado 2 de las Directrices se referirían a la privacidad y las libertades individuales. No obstante, los intereses protegidos son amplios (véase el punto 2 anterior) y cada país Miembro puede verlos de distinta manera en distintos momentos. En los principios indicados en los Apartados 7 a 13 se da un enfoque básico común y una delimitación en lo referente a las directrices.

44. Como se ha explicado en el Apartado 2 de las Directrices, con ellas se pretende cubrir tanto el sector público como el privado. Los distintos países Miembros pueden definir estas nociones de manera diferente.

Apartado 3: Diferentes grados de sensibilidad

45. No se deberían aplicar las Directrices mecánicamente sin tener en cuenta el tipo de datos y las actividades de proceso de los mismos. El marco facilitado en los principios básicos de la Parte Segunda de las Directrices permite a los países Miembros que ejercen su discreción respecto al alcance de las medidas que han de tomarse. En particular, el Apartado 3(b) permite que muchos casos triviales de recogida y uso de datos personales (véase lo dicho anteriormente) queden completamente excluidos de la aplicación de las Directrices. Es obvio que esto no significa que el Apartado 3 haya de ser visto como un vehículo para echar por tierra las normas establecidas por las Directrices. Pero, hablando en general, las Directrices no presuponen su puesta en marcha uniforme por parte de los países Miembros en todos sus particulares. Se tienen que tener en cuenta, por ejemplo, las diferentes tradiciones y actitudes del público en general. Así pues, en un país los identificadores personales universales se pueden considerar inofensivos y útiles mientras en otro se pueden ver como muy sensibles y su uso estar restringido o incluso prohibido. En un país, se le puede dar protección a datos relativos a grupos y entidades similares mientras que en otro tal protección simplemente no existe, y así sucesivamente. Para terminar, algunos países Miembros pueden encontrar adecuado el restringir la aplicación de las Directrices al proceso automático de los datos personales. En el Apartado 3(c) se indica dicha limitación.

Apartado 4: Excepciones a las Directrices

46. Dar formalmente las excepciones a las Directrices que son parte de una Recomendación no vinculante puede parecer superfluo. Pero el Grupo de Expertos consideró oportuno incluir una disposición sobre este tema en la que se manifiesta que dos criterios generales deberían guiar las políticas nacionales al limitar la aplicación de las Directrices: cuanto menos excepciones hayas, mejor será, y las que haya se darán a conocer al público (por ejemplo, mediante su publicación en un diario oficial del gobierno). El conocimiento general de la existencia de ciertos datos o archivos sería suficiente para cumplir con el segundo criterio, aunque los detalles relativos a datos

concretos, etc. pueden tener que mantenerse en secreto. La fórmula indicada en el Apartado 4 pretende cubrir muchos tipos diferentes de temas y factores limitadores, ya que está claro que no fue posible facilitar una lista exhaustiva de excepciones, de ahí el decir que incluyen la soberanía nacional, la seguridad nacional y la política pública ("el orden público"). Otro asunto nacional decisivo sería, por ejemplo, los intereses financieros del Estado ("el crédito público"). Además, el Apartado 4 permite que las Directrices se pongan en marchas de maneras diferentes. Habría que tener siempre presente los países Miembros están en la actualidad en diferentes etapas de desarrollo respecto a las normas e instituciones para la protección de la privacidad y es probable que actúen a ritmos diferentes, aplicando distintas estrategias como, por ejemplo, la regulación de ciertos tipos de datos o actividades comparadas con la regulación de carácter general ("planteamiento para todo").

47. El Grupo de Expertos reconoció que los países Miembros podrían aplicar las Directrices de manera diferente según los tipos de datos personales. Puede haber diferencias en la frecuencia de inspección permisible, en la forma de equilibrar los intereses encontrados como la confidencialidad de los informes médicos frente al derecho de toda persona a inspeccionar los datos que a ellas se refieren, y así sucesivamente. Algunos ejemplos de áreas que pueden ser tratadas de manera diferente serían los informes sobre créditos, la investigación sobre delitos y las actividades bancarias. Asimismo, los países Miembros pueden optar por diferentes soluciones respecto a las excepciones que tengan que ver, por ejemplo, con la investigación y la estadística. No es necesario ni posible dar una lista exhaustiva de todas esas situaciones. Algunos de los siguientes Apartados de las Directrices y los comentarios relativos a los mismos nos aclaran algo el área de aplicación de las Directrices y de los temas estrechamente relacionados como la forma de equilibrar los intereses contrapuestos (compárese con los Apartados 7, 8, 17 y 18 de las Directrices). Resumiendo, el Grupo de Expertos asume que las excepciones se limitarán a las necesarias en una sociedad democrática.

Apartado 5: Países federales

48. En los países federales, la aplicación de las Directrices está sujeta a distintas limitaciones constitucionales. Así pues, el Apartado 5 sirve para subrayar que no existen compromisos para aplicar las Directrices más allá de los límites de competencia constitucional.

Apartado 6: Normas mínimas

49. Primero, el Apartado 6 describe las Directrices como normas mínimas para su adopción en la legislación local. Segundo, y en consecuencia, se ha convenido en que las directrices pueden ser completadas por medidas adicionales para la protección de la privacidad y las libertades individuales tanto a nivel nacional como internacional.

Apartado 7: Principio de limitación de recogida

50. Como comentario introductor de los principios establecidos en los Apartados 7 a 14 de las Directrices, cabría señalar que estos principios están relacionados entre sí y coinciden en parte. Así pues, las distinciones entre las diferentes actividades y etapas que intervienen en el proceso de datos que se asumen en los principios son un poco artificiales y es fundamental que los principios se traten a la vez y se estudien en su conjunto. El Apartado 7 se ocupa de dos temas, a saber: (a) los límites a la recolección de datos que, por la manera en que han de ser procesados, su naturaleza, el contexto en el que se van a usar u otras circunstancias, se ven como especialmente sensibles; y (b) los requisitos relativos a los métodos de recogida de datos. Es frecuente que se expresen opiniones distintas sobre el primer tema. Se podría argumentar que es tanto posible como deseable enumerar los tipos de categorías de datos que son sensibles por sí mismos y cuya recogida debería restringirse o incluso prohibirse. Hay precedentes al respecto en la legislación europea (raza, creencias religiosas, antecedentes penales, por ejemplo). Por otra parte, se puede afirmar que ningún dato es intrínsicamente "privado" o "sensible" pero puede llegar a serlo por su contexto y uso. Esta opinión se refleja, por ejemplo, en la legislación de Estados Unidos sobre privacidad.

51. El Grupo de Expertos discutió una serie de criterios de sensibilidad, como el riesgo de discriminación, pero no le fue posible definir ningún conjunto de datos que pudieran verse universalmente como sensibles. En consecuencia, el Apartado 7 contiene meramente una afirmación general e el sentido de que deberían ponerse límites a la recogida de datos personales. Por una cosa, esto representa una recomendación afirmativa a los legisladores de que decidan los límites que pondrían fin a la recogida indiscriminada de datos personales. La naturaleza de los límites no se indica pero se entiende que los límites pueden referirse a:

1.

- los aspectos de la calidad de los datos (es decir, que de los datos recogidos debería sacarse información de alta calidad, que los datos deberían recogerse en un marco informativo adecuado, etc.);

- los límites relativos al objeto del proceso de datos (es decir, que sólo se deben recoger ciertas categorías de datos y, posiblemente, que la recogida de datos debería estar restringida a la mínima necesaria para satisfacer el fin específico);

- "destinar" los datos especialmente sensibles según las tradiciones y actitudes existentes en cada país Miembro;

- los límites a las actividades de recogida de datos de ciertos controladores de datos;

- los temas de derechos civiles.

52. La segunda parte del apartado 7 (métodos de recogida de datos) se dirige contra las prácticas que implican, por ejemplo, el uso de dispositivos de registro de datos ocultos como magnetófonos, o engañar a los sujetos de datos para que suministren información. El conocimiento o consentimiento del sujeto de los datos es una regla fundamental, siendo el conocimiento el requisito mínimo. Por otra parte, no siempre se puede imponer el consentimiento, y ello por razones prácticas. Además, el Apartado 7 contiene un recordatorio ("cuando sea adecuado") de que hay situaciones en las que por razones prácticas o de políticas el conocimiento o consentimiento del sujeto de los datos no se pueden considerar necesarios. Las actividades de investigación sobre delitos y la actualización rutinaria de las listas de correo se pueden mencionar como ejemplos. Por último, el Apartado 7 no excluye la posibilidad de que un sujeto de los datos sea representado por otra parte, por ejemplo en el caso de que sea una persona mentalmente incapacitada, etc.

Apartado 8: Principio de la calidad de los datos

53. Los requisitos de que los datos sean oportunos se pueden ver de distintas maneras. De hecho, algunos miembros del Grupo de Expertos dudaron de si esos requisitos realmente encajan en el marco de la protección de la privacidad. Sin embargo, la conclusión del Grupo fue que los datos habrían de referirse al fin para el que se vayan a utilizar. Por ejemplo, los datos relativos a las opiniones pueden ser engañosos si se utilizan para fines con lo que no guardan relación, y lo mismo vale para los datos interpretativos. El Apartado 8 también se ocupa del hecho de que los datos sean precisos, completos y estén actualizados, todos ellos elementos importantes del concepto de cualidad de los datos. Los requisitos a este respecto están vinculados a los fines de los datos, es decir, no se pretende que tengan más alcance del necesario para los fines para los que se van a usar. Así pues, es frecuente que se tenga que recoger o retener datos históricos; es lo que pasa con la investigación social, que implica los llamados estudios longitudinales de hechos sociales, la investigación histórica y las actividades de archivo. El "test de fines" suele implicar el problema de si se va a dañar o no a los sujetos de datos si los datos no son precisos ni completos o no están actualizados.

Apartado 9: Principio de especificación de los fines

54. El Principio de especificación de los fines guarda una estrecha relación con los dos principios más cercanos, es decir el Principio de la calidad de los datos y el Principio de la limitación de uso. Básicamente, el Apartado 9 implica que antes, y en cualquier caso nunca después, del momento de la recogida de los datos, se podría identificar los fines para los que esos datos se van a usar, y que un posterior cambio de fines también debería indicarse. Esa especificación de fines se puede hacer de ciertos modos complementarios o alternativos, por ejemplo mediante declaraciones públicas, información a los sujetos de datos, legislación, decretos administrativos y autorizaciones dadas por los órganos de supervisión. Según lo indicado en los Apartados 9 y 10, los nuevos fines no se deberían introducir de manera arbitraria; la libertad para hacer cambios debería implicar compatibilidad con los fines originales. Por último, cuando los datos ya no sirven a un fin, y si resulta factible, puede ser necesario destruirlos (borrarlos) o darles una forma anónima. La razón es que se puede perder el control sobre los datos cuando éstos ya no tienen interés, y ello puede acarrear riesgos de robo, copiado no autorizado y cosas por el estilo.

Apartado 10: Principio de la limitación de uso

55. Este apartado se ocupa de los distintos usos, incluido el revelado, que implican desviaciones de los fines concretos. Por ejemplo, los datos pueden ser transmitidos de un ordenador a otro donde se pueden usar para fines no autorizados sin pasar por ninguna inspección y así ser revelados en el sentido propio de la palabra. Como norma, los fines indicados inicialmente o a posteriori deberían ser decisivos para el uso que se le puede dar a los mismos. El Apartado 10 contempla dos excepciones generales a este principio: el consentimiento del sujeto de datos (o su representante - véase el Apartado 52 más adelante) y la autoridad de la ley (como, por ejemplo, autorizaciones otorgadas por órganos de supervisión). Por ejemplo, se puede dar que datos que hayan sido recogidos para fines de toma de decisiones administrativas se faciliten para investigación, estadística y planificación social.

Apartado 11: Principio de garantía de la seguridad

56. Seguridad y privacidad no es lo mismo. Sin embargo, las limitaciones sobre el uso y revelación de datos se debería reforzar con garantías de seguridad, en forma de medidas físicas (puertas cerradas con llave y tarjetas de identificación, por ejemplo), medidas de organización (como niveles de autoridad respecto al acceso a los datos) y, en particular en los sistemas informáticos, medidas ad hoc (como el cifrado y la vigilancia disuasoria de actividades inusuales y las respuestas a las mismas). Se debería hacer hincapié en que entre las medidas de organización se incluye la obligación de que el personal de proceso de datos mantenga la confidencialidad de los mismos. La cobertura del Apartado 11 es amplia. Los casos mencionados en sus disposiciones son en cierta medida parcialmente coincidentes (por ejemplo, acceso/revelación). En la "pérdida" de datos se incluyen casos como su borrado accidental, la destrucción de los medios de almacenaje (y con ello la destrucción de los datos) y el robo de datos así como el "uso" para cubrir el copiado no autorizado.

Apartado 12: Principio de la transparencia

57. El Principio de la transparencia se puede ver como una condición previa para el Principio de participación de los individuos (Apartado 13); para que el último principio sea efectivo, en la práctica debe ser posible adquirir información sobre la recogida, el almacenaje o el uso de los datos personales. La información regular y voluntaria de los controladores de datos, y el registro en organismos públicos son algunos, aunque no todos, de los modos para hacerlo. Cuando se habla de medios que son "de disponibilidad inmediata" ello implica que los individuos deberían poder conseguir información sin excesivo esfuerzo en cuanto al tiempo, el conocimiento, los desplazamientos, etc., etc., y sin costes elevados.

Apartado 13: Principio de la participación individual

58. El derecho de todo individuo a acceder a los datos personales y a recusarlos se ve en general quizá como la mayor garantía de protección de la privacidad. Esta opinión es compartida por el Grupo de Expertos que, aunque sabe que el derecho al acceso y a la recusación no puede ser

absoluto, ha optado por expresarlo en un lenguaje claro y bastante específico. Con respecto a los subapartados, son necesarias las siguientes explicaciones:

59. Como norma, el derecho de acceso debería ser sencillo de ejercer. Esto puede significar, entre otras cosas, que debería ser parte de las actividades cotidianas del controlador de datos o de su representante y no debería implicar ningún proceso legal ni otras medidas similares. En algunos casos lo mejor sería facilitar el acceso inmediato a los datos como, por ejemplo, en el área médica, cuando un profesional médico puede servir como intermediario. En algunos países, los órganos de supervisión, como las autoridades de inspección de datos, pueden prestar servicios similares. La necesidad de que los datos se comuniquen en un plazo razonable se puede satisfacer de distintas formas. Por ejemplo, un controlador de datos que facilita información a los sujetos de los datos periódicamente puede quedar exento de la obligación de responder de inmediato a las peticiones individuales. Normalmente, el tiempo debe contarse desde la recepción de una petición. Su duración puede variar en cierta medida según las situaciones dependiendo de la circunstancias como la naturaleza del proceso de datos. La comunicación de esos datos "de manera razonable" significa, entre otras cosas, que se debe prestar atención a los problemas de distancia geográfica. Además, si se prescriben intervalos entre los plazos en que las peticiones de acceso se deben cumplir, esos intervalos han de ser razonables. En que medida los sujetos de los datos deberían poder conseguir copias de datos relativos a ellos es un tema que hay que dejar a la decisión de cada país Miembro.

60. El derecho a que se le den a uno explicaciones (razones) que se contempla en el Apartado 13(c) se limita a situaciones en las que las peticiones de información han sido rechazadas. El Grupo de Expertos veía con buenos ojos que se ampliara este derecho a las decisiones adversas en general basadas en el uso de los datos personales. Pero tras un estudio más profundo, se llegó a la conclusión de que un derecho de este tipo sería demasiado amplio como para insertarlo en el marco de privacidad constituido por las Directrices. No quiere decir que el derecho a recibir explicaciones por una decisión adversa no sea adecuado, por ejemplo, para informar y advertir a un sujeto sobre sus derechos de manera que pueda ejercerlos eficazmente.

61. El derecho a la recusación contemplado en el Apartado 13(c) y (d) tiene un alcance amplio e incluye recusaciones en primera instancia a los controladores de datos y posteriormente en los tribunales, órganos administrativos u otras instituciones, según las normas locales de procedimiento (compárese con el apartado 19 de las Directrices). El derecho a la recusación no implica que el sujeto de los datos pueda decidir qué solución o satisfacción corresponde (rectificación, anotación de que los datos están en litigio, etc.): esas materias se decidirán mediante los procedimientos legales y la ley local. Hablando en términos generales, los criterios que deciden el resultado de una recusación son los establecidos en otra parte de las Directrices).

Apartado 14: Principio de la responsabilidad

62. El controlador de datos decide sobre lo datos y las actividades de proceso de datos. El proceso de datos se realiza en su beneficio. Así pues, es fundamental que la ley local le exija al controlador la responsabilidad de cumplir con las normas y decisiones sobre la protección de la privacidad; y el hecho de que el proceso de datos lo realice otra persona, como una oficina de servicios, en su nombre, no debería bastar para que el controlador de datos quedara libre de esta obligación. Por otra parte, nada de lo expuesto en las Directrices evita que el personal de las oficinas de servicios, los "usuarios dependientes" (véase el Apartado 40) y otros sean considerados igualmente responsables. Por ejemplo, se pueden aplicar sanciones por violaciones de la obligación de mantener la confidencialidad a cualquiera a quien se le hubiera confiado el tratamiento de información personal (apartado 19 de las Directrices). La responsabilidad tal y como se contempla en el Apartado 14 se refiere a la responsabilidad cuya falta conlleva sanciones legales, así como a la responsabilidad establecida por los códigos de conducta, por ejemplo.

Apartados 15 a 18: Principios básicos de aplicación internacional

63. Los principios de aplicación internacional están estrechamente relacionados entre sí. Hablando

en términos generales, el Apartado 15 establece el respeto de los países Miembros por el interés de los demás en proteger los datos personales y la privacidad y las libertades individuales de sus ciudadanos y residentes. El Apartado 16 trata de temas de seguridad en un sentido amplio y se puede decir que corresponde, a nivel internacional, al Apartado 11 de las Directrices. Los Apartados 17 y 18 se ocupan de las restricciones sobre el libre flujo de datos personales entre los países Miembros; básicamente, por lo que respecta a la protección de la privacidad y las libertades individuales, esos flujos se deberían admitir en cuanto los requisitos de las Directrices para la protección de estos intereses se hayan cumplido adecuadamente. La cuestión de otras posibles bases para la restricción de los flujos transfronterizos de datos personales no se contempla en las Directrices.

64. En cuanto al proceso local, el Apartado 15 tiene dos implicaciones. La primera se dirige contra las políticas liberales que son contrarias al espíritu de las Directrices y que facilitan los intentos de burlar o violar la legislación protectora de otros países Miembros. Sin embargo, esa burla o violación, aunque condenada por todos los países Miembros, no se menciona específicamente en este Apartado pues algunos países ven como inaceptable que a un país Miembro se le exigiera directa o indirectamente que aplicara, extraterritorialmente, las leyes de otros países Miembros. Cabría observar que la disposición menciona explícitamente la reexportación de datos. A este respecto, los países Miembros deberían tener siempre presente la necesidad de respaldar los esfuerzos de cada uno de los demás para garantizar que los datos personales no se quedan sin protección como resultado de su transferencia a territorios e instalaciones para el proceso de datos en los que el control es escaso o inexistente.

65. La segunda, que se anima implícitamente a los países Miembros a que consideren la necesidad de adaptar las normas y las prácticas para el proceso de datos a las circunstancias concretas que pueden presentarse cuando se trata de datos extranjeros y datos no nacionales. Como ejemplo, citemos que se puede presentar una situación en la que den accesibles datos sobre ciudadanos extranjeros para fines que sirvan a intereses particulares de su país natal (como el acceso a direcciones de ciudadanos que viven en el extranjero).

66. Por lo que respecta a las Directrices, el hecho de fomentar los flujos internacionales de datos personales no es una meta incontestable en sí misma. En la medida en que esos flujos tengan lugar deberían ser, según el Apartado 16, ininterrumpidos y seguros e decir, estar protegidos contra el acceso no autorizado, la pérdida de datos y hechos similares. Esa protección también deberían tenerla los datos en tránsito, es decir los datos que pasan por un país Miembro sin que se los use o almacene con vistas a su uso en ese país. En lo que respecta a las redes informáticas, el compromiso general que se contempla en el Apartado 16 debería verse teniendo en cuenta los antecedentes del Convenio Internacional sobre Telecomunicaciones de Málaga-Torremolinos de 25 de octubre de 1973. Según ese convenio, los miembros de la Unión Internacional de Telecomunicaciones, incluidos los países Miembros de la OCDE, han acordado, entre otras cosas, garantizar el establecimiento, en las mejores condiciones técnicas, de los canales e instalaciones necesarios para realizar el rápido e ininterrumpido intercambio de telecomunicaciones internacionales. Además, los miembros de la UIT han acordado tomar todas las medidas posibles que sean compatibles con el sistema de telecomunicaciones utilizado para garantizar el secreto de la correspondencia internacional. En cuanto a las excepciones, queda reservado el derecho a suspender los servicios internacionales de telecomunicaciones y se tiene derecho a comunicar la correspondencia internacional a las autoridades competentes para garantizar la aplicación de las leyes internas o la ejecución de convenios internacionales de los que los países Miembros de la UIT formen parte. Estas disposiciones se aplican cuando los datos se desplazan a través de las líneas de telecomunicaciones. En su contexto, las directrices constituyen una garantía complementaria de que los flujos internacionales de datos personales serían ininterrumpidos y seguros.

67. El apartado 17 refuerza lo dicho en el apartado 16 en lo relativo a las relaciones entre los países Miembros. Se ocupa de los intereses opuestos a los libres flujos transfronterizos de datos personales pero que pueden constituir las bases legítimas para restringir esos flujos entre países Miembros. Un ejemplo típico sería el de los intentos de burlar la legislación nacional mediante el

proceso de datos en un país Miembro que aún no observa las Directrices plenamente. El Apartado 17 establece una norma de protección equivalente en la que la protección es sustancialmente similar en sus efectos a la del país exportador, pero que no tiene que ser idéntica en la forma ni en todos sus aspectos. Como en el Apartado 15, la reexportación de datos personales se menciona específicamente, y en este caso con vistas a evitar todo intento de burlar la legislación local sobre privacidad de los países Miembros. La tercera categoría de bases para legitimar las restricciones mencionadas en el Apartado 17 sobre los datos personales de naturaleza especial cubre situaciones en las que se podrían ver afectados importantes intereses de los países Miembros. Sin embargo, hablando en términos generales, el apartado 17 está sujeto al Apartado 4 de las Directrices que dice que las restricciones sobre flujos de datos personales se deben mantener al mínimo.

68. El Apartado 18 intenta garantizar que existe un equilibrio entre los intereses de la protección de la privacidad y los intereses de los flujos transfronterizos de datos personales. Está dirigido en primer lugar contra la creación de barreras a los flujos de datos personales que resultan artificiales desde el punto de vista de la protección de la privacidad y las libertades individuales y cumplen los fines restrictivos de otros tipos que no están abiertamente anunciados. Sin embargo, el Apartado 18 no tiene como objeto el limitar los derechos de los países Miembros a regular los flujos transfronterizos de datos personales en áreas relativas al libre comercio, los aranceles, el empleo, y las condiciones económicas relativas al tráfico comercial internacional. Estos son temas que no fueron tratados por el Grupo de Expertos, al estar fuera de su Mandato.

Apartado 19: Puesta en marcha nacional

69. La puesta en marcha detallada de las Partes Segunda y Tercera de las Directrices se deja en primer lugar a los países Miembros. Variará según los distintos ordenamientos y tradiciones legales y por ello el Apartado 19 sólo intenta establecer un marco general que indique a grandes rasgos qué tipo de maquinaria nacional se contempla para la aplicación de las Directrices. La afirmación inicial muestra los diferentes planteamientos que podrían adoptar los países, pero en general y con respecto a los mecanismos de control (órganos de supervisión ad hoc, facilidades de control ya existentes como tribunales, organismos públicos, etc.).

70. En el apartado 19(a) se invita a los países a que adopten una legislación local adecuada, subyaciendo en la palabra "adecuada" lo que en cada país se considere adecuado o no respecto a las soluciones legales. El Apartado 19(b) relativo a la auto-regulación, se ocupa principalmente de los países de derecho común en los que la puesta en marcha no legislativa de las Directrices complementaría la actuación legislativa. El punto (c) daría una interpretación amplia, incluyendo medios como el consejo de los controladores de datos y la previsión de asistencia incluida la ayuda legal. El punto (d) contempla diferentes planteamientos para el tema de los mecanismos de control: en pocas palabras, tanto el establecimiento de órganos especiales de supervisión como la confianza en los medios de control existentes, bien en forma de tribunales, organismos públicos o de otra manera. El punto (e) trata de la discriminación y va contra las malas prácticas pero deja abierta la posibilidad de una "discriminación benigna" para ayudar, por ejemplo, a los grupos en inferioridad de condiciones. La disposición v contra la discriminación injusta en aspectos como la nacionalidad y el domicilio, el sexo, la raza, los credos o la afiliación a algún sindicato.

Apartado 20: Intercambio de información y procedimientos compatibles

71. Aquí se tratan dos grandes problemas, a saber: (a) la necesidad de asegurarse de que se puede obtener información sobre normas, regulaciones, decisiones, etc. que pongan en marcha las Directrices, y (b) la necesidad de evitar que los flujos transfronterizos de datos personales sean obstaculizados por un innecesario marco complejo y dispar de procedimientos y requisitos de adecuación. El primer problema surge a causa de la complejidad de la regulación sobre la protección de la privacidad y las políticas sobre datos en general. Suele haber varios niveles de regulación (en sentido amplio) y muchas normas importantes no se pueden dictar permanentemente en forma de disposiciones estatutarias detalladas; han de mantenerse bastante abiertas y dejarse a la discreción de los órganos de toma de decisiones de nivel inferior.

72. La importancia del segundo problema es, hablando en términos generales, proporcional al número de leyes nacionales que afectan a los flujos transfronterizos de datos personales. Incluso en la etapa actual, es obviamente necesario que se coordinen disposiciones especiales en las leyes de cada país sobre el flujo transfronterizo de datos personales, incluidas medidas especiales relativas al control de adecuación y, en caso necesario, autorizaciones para operar sistemas de proceso de datos.

Apartado 21: Maquinaria para la cooperación

73. La disposición sobre procedimientos nacionales asume que las directrices formarán una base para la cooperación continuada. Las autoridades y los organismos especializados sobre protección de datos que se ocupan de los temas de políticas en la información y las comunicaciones de datos son interlocutores obvios en esa cooperación. En particular, el segundo propósito de esas medidas, que aparece en el apartado 21(II) (ayuda mutua en temas de procedimiento y peticiones de información) está encaminado al futuro: su significación práctica parece aumentar a medida que las redes de datos internacionales y las complicaciones que conllevan se hacen más numerosas.

Apartado 22: Conflictos de leyes

74. El Grupo de Expertos ha prestado una gran atención a los temas de los conflictos de leyes, y en primer lugar a cuestiones como qué tribunales deberían tener jurisdicción sobre temas específicos (elección de la jurisdicción) y qué sistemas legales deberían regir temas específicos (elección de la ley). La discusión de las diferentes estrategias y los principios propuestos ha confirmado la opinión de que en este momento, con el advenimiento de cambios tecnológicos tan rápidos, y dada la naturaleza no vinculante de las Directrices, no se intentará establecer soluciones concretas y detalladas. Van a surgir dificultades en relación a la elección de un modelo regulador teóricamente sólido y la necesidad de una mayor experiencia sobre las implicaciones de las soluciones que en sí mismas son posibles.

75. En cuanto a la cuestión de la elección de la ley, un modo de plantearse estos problemas es identificar uno o más factores relacionados que, poniéndonos en lo mejor, indican una ley aplicable. Esto es especialmente difícil en el caso de las redes informáticas internacionales donde, debido a su ubicación dispersa y el rápido desplazamiento de los datos, así como de las actividades de proceso de datos dispersos geográficamente, se podrían dar varios factores de relación, de manera compleja, que implicarían elementos de novedad legal. Además, no es evidente qué valor se atribuiría en estos momentos a las normas que mediante la aplicación de mecanismos establecen qué ley nacional concreta se va a aplicar. En un sentido, lo adecuado de esa solución parece depender de la existencia de conceptos legales similares y estructuras normativas, y del compromiso vinculante de las naciones de respetar ciertas normas sobre la protección de datos personales. A falta de estas condiciones, se podría intentar formular principios más flexibles que impliquen la búsqueda de una "ley oportuna" y estén ligados al objetivo de garantizar una eficaz protección de la privacidad y las libertades individuales. Así pues, en una situación en las que se pueden aplicar varias leyes, se ha sugerido que una solución podría ser el dar preferencia a la ley nacional que ofrezca la mejor protección a los datos personales. Por otra parte, se puede aducir que soluciones de este tipo dejan mucha incertidumbre, no sólo desde el punto de vista de los controladores de datos que pueden querer saber , en caso necesario por anticipado, por qué ordenamientos legales nacionales se va a regir el sistema de proceso de datos internacional.

76. A la vista de estas dificultades, y teniendo en cuenta que los problemas de conflictos de leyes podrían manejarse mejor dentro del marco total de datos personales y no personales, el Grupo de Expertos decidió contentarse con una manifestación que señala simplemente los temas y recomienda a los países Miembros que trabajen para encontrar esta solución.

Seguimiento

77. El Grupo de Expertos llamó la atención sobre los términos de la Recomendación 4 a las directrices que sugiere que los países Miembros se pongan de acuerdo cuanto antes sobre los procedimientos concretos de consulta/asesoramiento y cooperación para la aplicación de las Directrices.