2009

ingética TECHNOLOGIES

c/ Pablo de Santo Leocadio 7 Entlo 8, Vila-real (Castellón)

Telf. 964 539 154 **www.ingetica.com**

[LA PROTECCIÓN DE DATOS PERSONALES DE LOS NIÑOS (CASO ESPECIAL COLEGIOS)]

El presente documento ha sido extraído del sitio web de la Agencia Española de Protección de Datos, y ha sido ligeramente modificado por Ingética Technologies con el objetivo de adaptarlo para una lectura por parte de responsables de centros públicos y privados de nuestro ámbito geográfico.

El título original del documento es "***Documento de trabajo 1/08 sobre la protección de datos personales de los niños (Directrices generales y el caso especial de los colegios)"***

El Grupo de trabajo al que se hace mención en el documento se creó en virtud del artículo 29 de la Directiva 95/46/CE. Se trata del órgano consultivo independiente de la UE sobre protección de los datos y la vida privada. Sus tareas se definen en el artículo 30 de la Directiva 95/46/CE y en el artículo 15 de la Directiva 2002/58/CE. La secretaría pertenece a la Dirección C (Justicia Civil, Derechos fundamentales y Ciudadanía) de la Comisión Europea, Dirección General de Justicia, Libertad y Seguridad, B-1049, Bruselas, Bélgica, Oficina nº LX-46 06/80.

Los comentarios sobre este Documento de Trabajo deberán enviarse a: Secretaría del Grupo de Trabajo del Artículo 29, Comisión Europea, Dirección General de Justicia, Libertad y Seguridad.
Unidad C.5 – Protección de datos personales
Oficina: LX 46 1/43
B – 1049 Bruselas

Todos los comentarios de sectores públicos y privados se publicarán en la página web del Grupo de Trabajo del Artículo 29, a menos que los encuestados indiquen de manera explícita que desean mantener confidencial información en concreto.

Presidente Peter SCHAAR

1. INTRODUCCIÓN

El objetivo del presente documento consiste en analizar los principios generales pertinentes para la protección de los datos de los niños y explicar su pertinencia en un área crítica específica, a saber, la de los datos de los colegios.

Al hacer esto, pretende identificar las cuestiones importantes para la protección de los datos de los niños en general y ofrecer directrices a aquéllos que trabajan en este campo.

De conformidad con los criterios de los instrumentos internacionales más importantes, un niño es una persona natural con menos de 18 años, a menos que se haya emancipado legalmente antes de dicha edad.

Un niño es un ser humano en el sentido completo de la palabra. Por este motivo, un niño debe gozar de todos los derechos de una persona, incluyendo el derecho a la protección de sus datos personales. No obstante, los niños se encuentran en una situación especial, que debe considerarse desde dos perspectivas: la estática y la dinámica.

Desde el punto de vista estático, el niño es una persona que aún no ha alcanzado la madurez física y psicológica. Desde el punto de vista dinámico, el niño se encuentra en el proceso de desarrollarse física y mentalmente para convertirse en adulto. Los derechos del niño y su ejercicio (incluyendo el de la protección de datos) deben expresarse de manera que se reconozcan ambas perspectivas.

El presente dictamen se basa en la convicción de que la educación y responsabilidad son herramientas cruciales en la protección de los datos de los niños. Examinaremos los principales principios pertinentes para esta cuestión. La mayoría de ellos se refieren a los derechos del niño, pero se examinarán en el contexto de la protección de datos.

Estos principios están incluidos en los instrumentos internacionales aplicables más importantes. Algunos de estos instrumentos se refieren a derechos humanos generales, pero también contienen normas específicas para los niños. Los más importantes son los siguientes:

- Declaración universal de derechos humanos, 10/12/48 - artículos 25, 26, N. 3
- Convención europea para la protección de los derechos humanos y libertades fundamentales 04/11/50 – artículo 8.
- Carta de los derechos fundamentales de la UE, 07/12/00 – Artículo 241

Otros instrumentos que se refieren directamente a los derechos del niño son los siguientes:

- Declaración de Ginebra sobre los derechos del niño, 1923
- Convención de las Naciones Unidas sobre los derechos del niño, 20/11/89
- Convención europea sobre el ejercicio de los derechos de los niños, Consejo de Europa, nº 160, 25/01/932

2. PRINCIPIOS FUNDAMENTALES

A – EN GENERAL

1) - Interés superior del niño

El principio jurídico principal es el del interés superior del niño. La base de este principio es que una persona que aún no ha alcanzado la madurez física y psicológica necesita más protección que otros. Su objetivo es mejorar las condiciones de los niños y pretende reforzar el derecho de los niños al desarrollo de su personalidad. Todas las entidades, públicas o privadas, que tomen decisiones relativas a los niños deben respetar este principio. También se aplica a los progenitores y a otros representantes de los niños, ya sea en el momento de la comparación de sus respectivos intereses o en representación del niño.

Normalmente, los representantes de los niños deberían aplicar este principio, pero cuando haya un conflicto entre los intereses de los niños y sus representantes, los juzgados y tribunales o, si procede, las APD deberán decidir.

2) – Protección y cuidado necesario para el bienestar de los niños

El principio del interés superior exige una apreciación adecuada de la posición del niño. Ello implica el reconocimiento de dos cuestiones. En primer lugar, la inmadurez del niño le hace vulnerable y ello debe compensarse mediante una protección y cuidados adecuados.

En segundo lugar, el derecho del niño al desarrollo sólo puede disfrutarse adecuadamente con la asistencia o protección de otras entidades y/o personas. Dicha protección es competencia de la familia, la sociedad y el Estado.

Debe reconocerse que, para alcanzar un nivel adecuado de cuidado para los niños, en ocasiones, será necesario tratar sus datos personales de manera exhaustiva y por varias partes. Esto será fundamentalmente en áreas de bienestar: educación, seguridad social, sanidad, etc. Pero ello no es incompatible con una protección de datos adecuada y reforzada en dichos sectores sociales, aunque deberá ejercerse un especial cuidado cuando se compartan los datos sobre niños.

El hecho de compartir puede ocultar el principio de finalidad (limitación de objetivo) y crear el riesgo de que se construyan perfiles sin referencia al principio de proporcionalidad.

3) – Derecho a la intimidad

Como ser humano, el niño tiene derecho a la intimidad. El artículo 16 de la Convención de las Naciones Unidas sobre los Derechos del niño dispone que ningún niño será objeto de injerencias arbitrarias o ilegales en su vida privada, su familia, su domicilio o su correspondencia, ni de ataques ilegales a su honra y a su reputación. Todo el mundo debe respetarlo, incluso los representantes del niño.

4) – Representación

Los niños requieren representación jurídica para el ejercicio de la mayoría de sus derechos. No obstante, ello no significa que la condición jurídica del representante tenga una prioridad absoluta o incondicional sobre el del niño, porque el interés superior del niño puede, en ocasiones, conferirle derechos relativos a la protección de datos que puedan anular los derechos de los progenitores o representantes. La necesidad de representación tampoco implica que no deba consultarse a los niños, a partir de cierta edad, en cuestiones relativas a ellos.

Si el tratamiento de los datos del niño comenzó con el consentimiento de su representante, el niño en cuestión, al alcanzar la mayoría de edad, podrá revocar su consentimiento. Pero si desea que continúe el tratamiento, el interesado deberá dar su consentimiento explícito cuando se exija.

Por ejemplo, si un representante ha dado su consentimiento explícito a la inclusión del niño (el interesado) en un ensayo clínico, al alcanzar la mayoría de edad, el responsable del tratamiento deberá asegurarse de que sigue teniendo una base válida para el tratamiento de los datos personales del interesado. En concreto, deberá considerar la obtención del consentimiento explícito del propio interesado para que continúe el ensayo, ya que están implicados datos sensibles.

En esta cuestión, debe recordarse que los derechos a la protección de datos pertenecen al niño y no a su representante, que se limita a ejercerlos.

5) – Intereses en conflicto: intimidad y el interés superior del niño

El principio del interés superior puede tener una doble función. *Prima facie*, el principio exige que se proteja la intimidad del niño del mejor modo posible, dando efecto en la mayor medida posible a los derechos de protección de datos del niño. No obstante, pueden surgir ocasiones en que el interés superior del niño y su derecho a la intimidad parezcan estar en conflicto. En tales casos, los derechos de protección de datos pueden tener que ceder al principio del interés superior. Éste es el caso en especial de los datos médicos, donde, por ejemplo, un servicio de bienestar juvenil podría necesitar información pertinente en casos de abusos a menores o negligencia. De manera similar, un profesor puede divulgar datos personales de un menor a un trabajador social para proteger al niño, física o psicológicamente.

En casos extremos, el principio del interés superior del niño puede también entrar en conflicto con el requisito del consentimiento de su representante. En este caso, también se elegirá el interés superior del niño (por ejemplo, si está en peligro la integridad física o mental del niño).

6) – Adaptación al grado de madurez del niño

Puesto que el niño es una persona todavía en desarrollo, el ejercicio de sus derechos (incluyendo los relativos a la protección de datos) debe adaptarse a su nivel de desarrollo físico y psicológico. Los niños no sólo se encuentran en proceso de desarrollo, sino que tienen derecho a este desarrollo. El modo en que se gestiona este proceso en los diferentes ordenamientos jurídicos varía de un Estado a otro, pero en cualquier sociedad, los niños deben tratarse de conformidad con su nivel de madurez.

Por lo que respecta al consentimiento, la solución puede variar de la mera consulta al menor, al consentimiento paralelo del niño y el representante, e incluso, al consentimiento único del niño si ya es maduro.

7) – Derecho a ser consultado

De manera gradual, los niños van siendo capaces de contribuir a la toma de decisiones que les afectan. A medida que crecen, se les debe consultar más regularmente sobre el ejercicio de sus derechos, incluyendo los relativos a la protección de datos.

Esta obligación de consulta consiste en tener en cuenta (aunque no someterse necesariamente) las opiniones propias del niño. Este derecho a ser consultado puede aplicarse a muy distintas cuestiones, como la geolocalización, el uso de las imágenes del niño y otros.

B – BAJO LA PERSPECTIVA DE LA PROTECCIÓN DE DATOS

1) – Ámbito del marco jurídico existente sobre protección de datos

Las Directivas pertinentes sobre protección de datos, es decir 95/46/CE y 2002/58/CE, no mencionan de manera explícita los derechos a la intimidad de los menores. Estos instrumentos jurídicos se aplican a todas las personas físicas, pero no hay disposiciones específicas relativas a cuestiones concretas de los niños.

No obstante, esto no significa que los niños no tengan derecho a la intimidad y que estén fuera del ámbito de dichas Directivas. De conformidad con la redacción de las propias Directivas, éstas se aplican a cualquier “persona física” y, por consiguiente, incluyen a los niños.

Teniendo en cuenta el limitado ámbito personal y material de la Directiva, siguen sin solucionarse una serie de cuestiones relativas a la protección de la intimidad de los niños dentro del marco de la Directiva. Esto se debe a que la mayoría de las disposiciones no tienen directamente en cuenta las particularidades de la vida de los niños. Surgen problemas en relación con el grado de madurez individual de un niño, así como el requisito de representación en los actos jurídicos.

Las necesidades de protección de datos de los niños deben tener en cuenta dos aspectos principales. Se trata, en primer lugar, de los niveles variantes de madurez que determinan cuándo pueden los menores tratar sus propios datos y, en segundo lugar, la medida en que los representantes tienen derecho a representar a los menores en casos en que la divulgación de datos personales perjudicaría el interés superior del niño.

A continuación, trataremos la cuestión de cómo las normas existentes de la Directiva podrían aplicarse de manera óptima para garantizar que la intimidad de los niños se protege de un modo eficaz y adecuado.

2) – Principios de la Directiva 95/46/CE

a) Calidad de los datos

Los principios generales sobre la calidad de los datos que se disponen en la Directiva 95/46/CE deben adaptarse, naturalmente, de manera adecuada cuando se aplican a los niños. Esto quiere decir:

a.1) ***Lealtad*****.** El deber de tratar los datos personales de conformidad con el principio de lealtad (art. 6a) debe interpretarse de manera estricta cuando se trate de un niño. Como los niños no son completamente maduros, los responsables del tratamiento deben ser conscientes de ello y actuar de buena fe a la hora de tratar sus datos.

a.2) ***Proporcionalidad y pertinencia de los datos*****.** El principio establecido en el artículo 6c) de la Directiva 95/46/CE dispone que sólo se podrán recabar y tratar los datos adecuados, pertinentes y no excesivos. Al aplicar los principios del artículo 6c), los responsables del tratamiento deberán prestar especial atención a la situación del menor, ya que deberán respetar su interés superior en todo momento.

De conformidad con el artículo 6d) de la Directiva 95/46/CE, "los datos exactos y, cuando sea necesario, actualizados; deberán tomarse todas las medidas razonables para que los datos inexactos o incompletos, con respecto a los fines para los que fueron recogidos o para los que fueron tratados posteriormente, sean suprimidos o rectificados;"
Teniendo en cuenta el desarrollo constante de los niños, los responsables del tratamiento deberán prestar especial atención a la obligación de mantener los datos personales actualizados.

a.3) ***Conservación de los datos.*** En este sentido, es necesario tener en cuenta el "droit à l'oubli" que se aplica a cualquier interesado incluyendo, en especial, los niños. El artículo 6e) de la Directiva deberá aplicarse en consecuencia. Puesto que los niños están en continuo desarrollo, los datos relativos a ellos cambian y pueden volverse rápidamente anticuados e irrelevantes en relación con el objetivo principal de su recopilación. Los datos no deberán conservarse cuando ocurra esto.

b) Legitimidad

La Directiva 95/46/CE establece principios fundamentales en materia de protección de datos que los Estados Miembros deben respetar e implementar. En relación con los derechos a la intimidad de los niños, los artículos 7 y 8 son de suprema importancia ya que establecen criterios para hacer legítimo el tratamiento de los datos.

En primer lugar, puede permitirse el tratamiento si la persona en cuestión ha dado su consentimiento inequívoco. El significado del término "consentimiento" se aclara en el artículo 2(h) de la Directiva.

En otras palabras, debe ser libre e informado. No obstante, el consentimiento no es obligatorio en todos los casos. De hecho, el tratamiento también puede ser legítimo si se cumplen otros requisitos legales de conformidad con el artículo 7 (b-f), por ejemplo, puede permitirse el tratamiento si se firma un contrato.

En los casos en que los representantes violan la intimidad de los niños vendiendo o publicando sus datos, se plantea la cuestión de cómo puede protegerse el derecho a la intimidad si los propios niños no son conscientes de la infracción. Los niños necesitan un tutor legal pero, en casos como éste, no pueden ejercer sus derechos. Si el niño es lo bastante maduro para detectar un incumplimiento de su derecho a la intimidad, debe tener derecho a ser escuchado por las autoridades competentes, incluyendo las autoridades de protección de datos.

En cuanto a las demás condiciones del artículo 7 de la Directiva que hacen el tratamiento de datos legítimo, también deben respetarse los principios del interés superior de niño y de representación. A partir de cierta edad, por ejemplo, los niños son capaces, por ley, de incurrir en obligaciones contractuales, como en el campo del empleo. Pero dichos contratos sólo son válidos si los representantes han dado su consentimiento. Antes de la celebración de un contrato, o durante su ejecución, es posible que la otra parte quiera recabar datos sobre el niño como empleado.

Los representantes facilitan el tratamiento de datos dando su consentimiento. Los progenitores o tutores deben tomar las decisiones basándose en el interés superior del niño. Deben tener en cuenta los modos en que la divulgación de los datos podría suponer una amenaza a la intimidad del niño y a sus intereses vitales, por ejemplo, no divulgando datos médicos. Existen otras áreas en las que se permite a los niños decidir independientemente de sus representantes.

En relación con la condición del artículo 7 e), cabe destacar que el principio del interés superior del niño puede clasificarse, asimismo, como de interés público. Éste puede ser el caso cuando el servicio de bienestar juvenil necesita datos personales del niño para cuidar de él. Por consiguiente, las disposiciones de la Directiva pueden aplicarse directamente a estas circunstancias.

No obstante, se plantea la cuestión de si los niños que, en determinados casos, pueden otorgar actos jurídicos sin el consentimiento de sus representantes (en situaciones en que gozan de derechos parciales) pueden también dar un consentimiento válido al tratamiento de sus propios datos.

De conformidad con las normativas locales aplicables, esto puede ocurrir en casos de matrimonio, empleo, cuestiones religiosas, etc. En otros casos, el consentimiento del niño puede ser válido con la condición de que el representante no se oponga. También está claro que el nivel de madurez física y psicológica del niño debe tenerse en cuenta y que, a partir de cierta edad, es capaz de juzgar cuestiones que le afecten. Esto puede ser importante en casos en que el representante no está de acuerdo con el niño, pero el niño es lo suficientemente maduro para decidir en su propio interés, por ejemplo, en un contexto sexual o médico.

No deben descuidarse los casos en que el interés superior del niño limita o incluso prevalece sobre el principio de representación y se le debe dar una mayor consideración.

El principio más amplio de legitimidad se refiere a los intereses legítimos del responsable del tratamiento o de un tercero (artículo 7 f), salvo cuando quedan anulados por los intereses o derechos y libertades fundamentales del interesado. Al hacer el balance, debe prestarse especial cuidado al estatus de interesado del niño, utilizando su interés superior como guía.

c) Seguridad de los datos

El artículo 17 de la Directiva 95/46/CE establece que “Los Estados miembros establecerán la obligación del responsable del tratamiento de aplicar las medidas técnicas y de organización adecuadas, para la protección de los datos personales contra la destrucción, accidental o ilícita, la pérdida accidental y contra la alteración, la difusión o el acceso no autorizados” y especifica que:

“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.”

Debe prestarse una especial atención y cuidado en relación con los datos de los niños.

d) Derechos del interesado

d.1.) *Derecho de información*

Cabe destacar que el requisito de consentimiento en virtud de la Directiva va de la mano con la obligación de informar adecuadamente al interesado (artículo 10, 11 y 14).

En el contexto de la información a los niños, debe ponerse especial énfasis en dar comunicaciones escalonadas basadas en el uso de un lenguaje sencillo, conciso y educativo de fácil comprensión. En una comunicación más breve debería incluirse la información básica que debe proporcionarse al recabar datos personales directamente del interesado o de un tercero (artículo 10 y 11). Ésta debería ir acompañada de una información más detallada, tal vez a través de un hipervínculo, donde se proporcionen todos los datos pertinentes.

Tal y como ha indicado el Grupo de Trabajo en su recomendación sobre el tratamiento de datos en línea, es fundamental que las comunicaciones se envíen en el lugar y momento correctos, es decir, deben aparecer directamente en la pantalla, antes de recabar la información.

Además de ser un requisito en virtud de la Directiva, es especialmente importante como una herramienta para concienciar al niño de los posibles riesgos y peligros que puedan surgir de las actividades en línea. De hecho, puede argumentarse que en el entorno en línea, al contrario que en el mundo real, ésta es la única oportunidad de informar a los niños de dichos peligros.

d.2) ***Derecho de acceso***

Normalmente, son los representantes quienes ejercen el derecho de acceso, pero siempre en interés del niño. En función del grado de madurez del niño, puede ejercerse en su lugar o junto con él. En algunos casos, el niño puede tener derecho a ejercer sus derechos solo.

Cuando se trate de derechos muy personales (como, por ejemplo, en el campo de la salud), los niños pueden incluso pedir a sus médicos que no divulguen sus datos médicos a sus representantes.

Éste podría ser el caso si un adolescente da datos sexuales a un médico o a una línea de ayuda, excluyendo de manera explícita a sus representantes de dicha información.

También podría ser el caso si el niño no confía en sus representantes y se pone en contacto con un servicio de bienestar juvenil, por ejemplo, si consume drogas o tiene tendencias suicidas.

Se plantea la cuestión de si los representantes deben tener acceso a dichos datos y si el menor puede oponerse. Para determinar si prevalece el derecho del niño a la intimidad frente al derecho de acceso del representante, deben estudiarse cuidadosamente los intereses de todas las partes implicadas. En este análisis, el interés superior del niño es de especial importancia.

En el caso de acceso a datos médicos, la apreciación del médico puede ser pertinente para evaluar la oportunidad de acceso por parte del representante.

Las prácticas nacionales también ofrecen ejemplos útiles: en el Reino Unido, por ejemplo, los adolescentes mayores de 12 años pueden ejercer su derecho de acceso solos.

En varios países, el derecho de acceso de los representantes a los datos de sus hijas adolescentes está limitado en casos de aborto.

Como comentario general, los criterios para las condiciones de acceso no serán únicamente la edad del niño, sino también si los datos en cuestión fueron proporcionados por los progenitores o por el niño, lo que también es una indicación de su grado de madurez y autonomía.

d.3) ***Derecho de oposición***

El artículo 14 a) dispone que el interesado tiene derecho a oponerse al tratamiento, al menos en los casos mencionados en las letras e) y f) del artículo 7, por razones legítimas. Estas razones pueden ser especialmente imperiosas cuando se refieren a niños. También cabe recordar que el interesado tiene derecho a oponerse, en cualquier caso, al tratamiento de sus datos para fines de prospección (artículo 14 b)).

3. EN EL COLEGIO

En la siguiente sección, el dictamen ilustrará cómo los principios fundamentales recordados anteriormente pueden especificarse en relación con el contexto escolar. De hecho, la vida de un menor se desarrolla tanto en el colegio como en el seno de la familia, por lo que es natural que surjan varias cuestiones de protección de datos en relación con la vida escolar de los niños. Se trata de cuestiones de naturaleza muy diversa y plantean, en consecuencia, diferentes problemas.

1) – Ficheros de alumnos

a) Información

Pueden plantearse cuestiones de protección de datos relativas a los niños (y, en ocasiones, a sus familias) en relación con los ficheros de alumnos desde el momento de su matriculación en el colegio. De hecho, existen países en que la legislación permite a las autoridades escolares exigir formularios, que contienen datos personales, y que deben rellenarse para la creación de ficheros de alumnos, computerizados o de otro tipo.

En dichos formularios, debe informarse a los interesados de que sus datos personales se recabarán, se tratarán y para qué fin, quién es el responsable del tratamiento y cómo pueden ejercerse los derechos de acceso y rectificación. También deberán estar informados, cuando proceda, de a quién podrán divulgarse sus datos.

b) Proporcionalidad

Los datos exigidos no deberán ser excesivos: por ejemplo, los datos sobre los títulos académicos de los progenitores, su profesión o su situación laboral no son siempre necesarios. Los responsables del tratamiento deberán considerar si son realmente necesarios. Debe tenerse especial cuidado, ya que esta información puede ser causa de discriminación.

c) No discriminación

Posiblemente, algunos de los datos incluidos en estos formularios pueden causar discriminación, por ejemplo, los datos relativos a la raza, estado de inmigrante o el hecho de padecer determinadas discapacidades.

Normalmente, esta información se recaba para asegurarse de que el colegio es consciente y presta la atención necesaria a los alumnos con dificultades culturales (por ejemplo, lingüísticas) o económicas.

Los principios del interés superior y el objetivo del principio de limitación deberían ser los criterios en el tratamiento de dicha información. Por ello, debe aplicarse una perspectiva muy estricta en lo que respecta al registro de la religión de los alumnos; esto

sólo puede aceptarse cuando lo justifican la naturaleza (colegio religioso) y fines administrativos y únicamente en la medida estrictamente necesaria.

No deben extraerse deducciones superfluas sobre la religión del alumno cuando los datos sean necesarios únicamente para fines administrativos (por ejemplo, al seguir una clase de religión o al indicar una preferencia en la comida).

La información sobre la riqueza e ingresos la familia de un niño también puede ser una fuente de discriminación, pero puede tratarse en el interés superior del niño, por ejemplo, si los representantes solicitan becas o reducciones de los gastos escolares.

Todos los datos que puedan desembocar en discriminación deben protegerse mediante medidas de seguridad adecuadas, como el tratamiento en ficheros independientes, por personal designado y cualificado, con sujeción al secreto profesional, y otras medidas adecuadas.

El consentimiento al tratamiento de todos los datos que puedan causar discriminación deberá ser claro e inequívoco.

d) Principio de finalidad

d.1) *Comunicación de los datos*

Existen casos en que las autoridades escolares proporcionan los nombres y direcciones de sus alumnos a terceros, con frecuencia para fines de prospección.

Esto ocurre, por ejemplo, cuando se envían datos a bancos o compañías de seguros que desean atraer como clientes a los alumnos, o cuando los datos de los estudiantes se comunican a los representantes electos locales. Esto constituye un incumplimiento del principio de finalidad, ya que los datos para los objetivos del colegio se utilizan para fines incompatibles.

De conformidad con el artículo 6 1) b) de la Directiva 95/46, los datos de los niños no pueden utilizarse para fines incompatibles con el fin determinado cuando fueron recabados.

Aquí la cuestión no es el problema de que los niños sean destinatarios de fines de prospección, se trata de un problema de protección del consumidor. Lo que se plantea es la recolección de datos personales para enviar a los interesados posteriormente mensajes de prospección. Dicho tratamiento estará siempre sujeto al consentimiento previo de los representantes (y de los niños, en función de su madurez).

En cualquier caso en que una operación de prospección se haya considerado legítima y compatible, dicho tratamiento deberá realizarse siempre de la manera menos intrusiva posible.

d.2) ***Acceso a los datos***

Los datos incluidos en el fichero del alumno deberán estar sujetos a la más rigurosa confidencialidad, de conformidad con el principio general de la Directiva 95/46/CE, artículo 16.

El tratamiento de datos de naturaleza especial deberá estar sujeto a requisitos de seguridad especiales.

Los siguientes son ejemplos de dicho tipo de datos:

- Procedimientos disciplinarios
- Constancia de casos de violencia
- Tratamientos médicos en el colegio
- Orientación escolar
- Educación especial de personas discapacitadas
- Ayudas sociales a alumnos pobres

Deberá proporcionarse acceso a los datos a los representantes de los alumnos (y a los propios alumnos, si ya son maduros). Dicho acceso deberá estar estrictamente regulado

y limitado a las autoridades escolares, inspectores de colegios, personal sanitario y cuerpos y fuerzas de seguridad.

d.3) *Resultados escolares*

Los diferentes países tienen diferentes tradiciones en cuanto a la publicación de los resultados escolares. Existen países con una tradición muy establecida de publicación de los resultados.

El objetivo de este sistema es permitir la comparación de los resultados y facilitar las posibles quejas o recursos.

En otros países, incluso los resultados están sujetos a la norma general de confidencialidad aplicable a los datos del fichero del alumno. En estos casos, los resultados pueden divulgarse a los representantes de los alumnos que ejerzan su derecho de acceso.

En cualquier caso, los resultados escolares deberían publicarse únicamente cuando sea necesario, y sólo después de informar a los alumnos y sus representantes del objetivo de la publicación y de su derecho de oposición.

Supone un problema especial la publicación de los resultados escolares por internet, que es un método cómodo de comunicarlos a las personas interesadas. Los riesgos inherentes a este modo de comunicación exigen que el acceso a los datos sólo sea posible con salvaguardias especiales. Esto puede lograrse utilizando un sitio web seguro o contraseñas personales asignadas a los representantes o, cuando ya sean maduros, a los niños.

Las modalidades del derecho de acceso serán diferentes, en función del grado de madurez del niño. Es probable que, en la escuela primaria, el acceso sea ejercido fundamentalmente por los representantes, mientras que en la escuela secundaria los alumnos del colegio también puedan acceder a los datos ellos mismos.

d.4) *Conservación y eliminación*

El principio general por el que los datos no deben conservarse durante más tiempo del necesario para el fin para el que fueron recabados también es aplicable a este contexto. Por consiguiente, debe estudiarse con cuidado qué datos de los ficheros escolares deben mantenerse, ya sea por motivos educativos o profesionales, y cuáles deben eliminarse, por ejemplo, los relativos a procedimientos disciplinarios y sanciones.

2) – Vida escolar

Surgen cuestiones de protección de datos en relación con la vida escolar diaria en las siguientes áreas.

a) Datos biométricos – acceso al colegio y comedor

A lo largo de los años, se ha producido un incremento en el control del acceso a los colegios por razones de seguridad obvias. Este control de acceso implica la

recopilación, en la entrada, de datos biométricos, como huellas dactilares, iris o contornos de la mano.

En determinadas situaciones, estas medidas pueden ser desproporcionadas para el objetivo, creando un efecto demasiado intrusivo. En cualquier caso, el principio de proporcionalidad debe aplicarse también al uso de estos medios biométricos.

Se recomienda encarecidamente que los representantes legales tengan a disposición un medio sencillo para oponerse al uso de los datos biométricos de sus hijos. Si ejercen su derecho de oposición, deberá darse a los hijos una tarjeta u otro medio para acceder a las instalaciones escolares en cuestión.

b) Circuito cerrado de televisión (CCTV)

Existe una tendencia creciente a usar CCTV en los colegios por motivos de seguridad. No existe una solución válida recomendada para todos los aspectos de la vida escolar y para todas las zonas de los colegios.

La capacidad del CCTV para afectar a las libertades personales supone que su instalación en los colegios exige un cuidado especial. Esto supone que sólo debería instalarse cuando sea necesario y si no está disponible otro medio menos intrusivo de lograr el mismo objetivo. La decisión de instalar un CCTV deberá estar precedida de un debate exhaustivo entre los profesores, los progenitores y los representantes de los alumnos, teniendo en cuenta los objetivos indicados para la instalación y la adecuación de los sistemas propuestos.

Existen lugares donde la seguridad es de la mayor importancia, por lo que puede justificarse más fácilmente la instalación de CCTV, por ejemplo, en las entradas y salidas de los colegios, así como otros lugares donde circulan las personas (no sólo la población del colegio, sino también personas que visitas las instalaciones escolares por el motivo que sea).

La elección de la ubicación de las cámaras de CCTV deberá ser siempre pertinente, adecuada y no excesiva en relación con el objeto del tratamiento. Por ejemplo, en algunos países, el uso de cámaras de CCTV fuera del horario escolar se consideró adecuado en relación con los principios de protección de datos.

Por otro lado, en la mayoría de las demás partes del colegio, el derecho a la intimidad de los alumnos (así como el de los profesores y otros trabajadores del colegio) y la libertad esencial a la enseñanza, prevalecen sobre la necesidad de vigilancia por CCTV permanente.

Éste es especialmente el caso en las aulas, donde la vigilancia por video puede interferir no sólo en la libertad de los alumnos de aprender y expresarse, sino también en la libertad de enseñar. Lo mismo se aplica a las zonas de ocio, gimnasios y vestuarios, donde la vigilancia puede interferir con el derecho a la intimidad.

Estas observaciones también se basan en el derecho al desarrollo de la personalidad, que poseen todos los niños. De hecho, la concepción en desarrollo de su propia libertad puede verse comprometida si asumen desde una edad temprana que es

normal estar vigilado por CCTV. Esto es aún más cierto si se utilizan webcams o dispositivos similares para la vigilancia remota de los niños durante sus horas de colegio.

En cualquier caso en que esté justificado el uso de CCTV, los niños, el resto de la población del colegio y los representantes deberán estar informados de la existencia de la vigilancia, del responsable del tratamiento y de sus objetivos. La información dirigida a los niños deberá ser adecuada a su nivel de entendimiento.

Las autoridades escolares deberán revisar regularmente la justificación y la pertinencia del sistema de CCTV para decidir si debe mantenerse o no. Los representantes de los niños deberán estar informados en consecuencia.

c) Condiciones de salud

Los datos sobre la condición de salud de los niños son datos sensibles. Por este motivo, su tratamiento deberá adherirse estrictamente a los principios del artículo 8 de la Directiva. Dichos datos sólo deberán tratarlos médicos, o aquéllos que "cuiden" directamente a los alumnos, como profesores y otro personal del colegio sujetos a la ética del secreto profesional.

El tratamiento de datos de este tipo depende o bien del consentimiento de los representantes de los niños o de los intereses vitales relacionados con el colegio o con la vida educativa.

d) Sitios web de los colegios

Un número creciente de colegios crean sitios web dirigidos a los alumnos/estudiantes y sus familias, y dichos sitios web se convierten en la herramienta principal para las comunicaciones externas.

Los colegios deben ser conscientes de que divulgar información personal justifica un cumplimiento más riguroso de los principios fundamentales de protección de datos, en concreto, la proporcionalidad y minimización de los datos; adicionalmente, se recomienda la puesta en marcha de mecanismos de acceso restringido con vistas a proteger la información personal en cuestión (es decir, conexión con nombre de usuario y contraseña).

e) Fotos de los niños

Con frecuencia, los colegios están tentados de publicar (en la prensa o en internet) fotos de sus alumnos. Debe prestarse especial atención a la publicación por parte de los colegios de fotos de sus alumnos en internet. Siempre debe hacerse una evaluación del tipo de foto, la pertinencia de su publicación y su objetivo. Los niños y sus representantes deben ser conscientes de su publicación y deberá obtenerse el consentimiento previo del representante (o del niño, si ya es maduro).

Pueden aceptarse excepciones en el caso de fotos colectivas, a saber, de acontecimientos escolares si, por su naturaleza, no permiten una identificación fácil de los alumnos.

f) Tarjetas de alumno

Para el control de acceso y vigilancia de las compras: Muchos colegios están utilizando tarjetas de alumnos no sólo para controlar el acceso al colegio, sino también para vigilar las compras realizadas por los alumnos. Es cuestionable si el segundo objetivo es totalmente compatible con la intimidad del niño, en especial después de cierta edad.
En cualquier caso, las dos funciones deberían ser independientes, ya que la segunda puede plantear problemas de intimidad.

Para la localización de alumnos: Otro medio de control utilizado en algunos colegios (con tarjeta o sin ella) es la localización de alumnos mediante etiquetas RFID. En este caso, la pertinencia de este sistema deberá estar justificada en relación con los riesgos específicos en cuestión, en especial cuando hay métodos de control alternativos disponibles.

g) Videoteléfonos en los colegios

Los colegios pueden desempeñar un papel fundamental en el establecimiento de precauciones para el uso de MMS, grabación de audio y vídeo cuando se trata de datos personales relativos a terceros sin el conocimiento de los interesados. Los colegios deberían advertir a los estudiantes de que la circulación no limitada de grabaciones de vídeo, grabaciones de audio y fotografías digitales puede causar infracciones graves del derecho a la intimidad de los interesados y la protección de datos personales.

3) – Estadísticas escolares y otros estudios

En la mayoría de los casos, no son necesarios datos personales para la obtención de estadísticas (no obstante, puede ocurrir en casos excepcionales, por ejemplo, cuando se elaboran estadísticas sobre integración profesional).

De conformidad con el artículo 6 e) de la Directiva, los resultados estadísticos no deben dar lugar a la identificación de los interesados, ya sea directa o indirecta.

Con frecuencia, se llevan a cabo estudios que utilizan datos personales sobre alumnos, obtenidos a partir de cuestionarios más o menos detallados. La recopilación de estos datos debe estar autorizada por los representantes (en particular, si se trata de datos sensibles) y los representantes deben estar informados del objetivo y los destinatarios del estudio.

Además, siempre que sea posible llevar a cabo estudios sin identificar a los niños, se deberá seguir este procedimiento.

4. CONCLUSIÓN

1) Derecho

El presente dictamen muestra que las disposiciones establecidas en el marco jurídico actual, en la mayoría de los casos, garantiza eficazmente la protección de los datos de los niños.

No obstante, un requisito previo para la protección eficaz de la intimidad de los niños es que las disposiciones se apliquen de conformidad con el principio del interés superior del niño. La aplicación debe tener en cuenta la situación específica de los menores y la de sus representantes. Las Directivas 95/46/CE y 2002/58/CE deberán interpretarse y aplicarse en consecuencia.

En casos de conflictos de intereses, puede buscarse una solución interpretando las Directivas de conformidad con los principios generales de la Convención de las Naciones Unidas sobre los Derechos del Niño, a saber, el interés superior del niño, y también remitiéndose a los demás instrumentos jurídicos ya mencionados.

Se anima a los Estados Miembro a adaptar sus legislaciones a la interpretación arriba mencionada tomando las medidas necesarias. Asimismo, a nivel comunitario, serán bienvenidas las recomendaciones u otros instrumentos adecuados que traten este tema.

Tal y como se dijo anteriormente, el presente dictamen contiene únicamente los principios generales de intimidad y protección de datos que son pertinentes a los datos de los niños y su aplicación al importante campo de la educación. Otras áreas específicas podrían merecer su estudio por parte de este Grupo de Trabajo en el futuro.

2) Práctica

El presente dictamen establece las cuestiones y consideraciones generales relacionadas con cuestiones de protección de datos e intimidad en relación con los niños. El Grupo de Trabajo ha escogido el campo de la educación como un primer paso para tratar esta cuestión debido a la importancia de la educación en la sociedad. Tal y como puede verse, el enfoque para proteger la intimidad de los niños se basa en la educación (por parte de las familias, colegios, autoridades de protección de datos, grupos de niños y otros) y sobre la importancia de la protección de datos y la intimidad y las consecuencias de dar datos personales si no es necesario.

Si nuestras sociedades van a luchar por una auténtica cultura de protección de datos en particular, y por la defensa de la intimidad en general, es necesario empezar por los niños, no sólo como un grupo que precisa protección, o como sujetos de los derechos que hay que proteger, sino también porque deben ser conscientes de sus obligaciones de respetar los datos personales de otros.

Para lograr este objetivo los colegios deben desempeñar una función clave. Los niños y alumnos deber ser educados para convertirse en ciudadanos autónomos de la Sociedad de la Información. Para ello, es fundamental que aprendan desde una edad temprana la importancia de la intimidad y la protección de datos. Estos conceptos les

permitirán tomar decisiones informadas posteriormente sobre qué información desean divulgar, a quién y en qué condiciones. La protección de datos debería incluirse sistemáticamente en los planes escolares, en función de la edad de los alumnos y la naturaleza de las asignaturas impartidas.

No debería darse nunca el caso de que, por razones de seguridad, los niños se enfrenten a una vigilancia excesiva que reduzca su autonomía. En este contexto, en necesario hallar el equilibrio entre la protección de la intimidad y la intimidad de los niños y su seguridad.

Los legisladores, los líderes políticos y las organizaciones educativas deberían, en sus respectivas áreas de competencia, tomar medidas eficaces para tratar estas cuestiones.

La función de las autoridades de protección de datos tiene cuatro vertientes: educar e informar, en especial a los niños y a las autoridades responsables del bienestar de los jóvenes; influir a los responsables de las decisiones para que tomen las decisiones adecuadas en materia de niños y intimidad; concienciar a los responsables del tratamiento de sus obligaciones; y utilizar sus poderes contra aquéllos que no observan la legislación o no se adhieren a los códigos de conducta o las mejores prácticas en esta área.

Una estrategia eficaz, en este contexto, puede ser la formulación de acuerdos entre las APD, Ministerios de Educación y otros organismos responsables, definiendo condiciones claras y prácticas de cooperación mutua en esta área para fomentar la noción de que la protección de datos es un derecho fundamental.

Se debería concienciar a los niños, en concreto, de que ellos mismos deben ser los primeros protectores de sus datos personales. Ésta es un área donde puede demostrarse la eficacia de la potenciación.