

# Directrices para la protección de la información personal infantil.

## Comisionado de Protección de Datos Inglés

### 1. INTRODUCCIÓN

Hasta ahora, nunca se había recopilado tanta información personal sobre los niños. Y dicho volumen está llamado a incrementarse de forma drástica.

La información sobre la infancia, y sobre las personas ligadas a ella, se recopila con las mejores intenciones. Todos deseamos proteger a los niños de abusos y de otros peligros. Todos deseamos ver que el conjunto de los niños alcanza su potencial con la mejor educación y atención sanitaria posibles, así como el óptimo desarrollo social y emocional. Todos deseamos evitar que la infancia se vea abocada al delito y a los comportamientos antisociales.

Existen, y siempre existirán, enconados y a menudo encendidos enfrentamientos sobre la manera de llevar a la práctica dichas elevadas aspiraciones. En concreto, uno de los epicentros se sitúa en el papel de los organismos oficiales implicados en el bienestar de la infancia. Los debates en curso sobre dónde y cómo establecer los límites de la intervención estatal deben ser ampliamente resueltos en los ámbitos político y democrático.

Sin embargo, las iniciativas dentro de este amplio terreno ponen sobre la mesa cuestiones reales de protección de datos y de privacidad que es necesario tratar. El hecho de que la ley de protección de datos (en el ámbito europeo y nacional) no establezca una distinción explícita entre los interesados adultos y aquellos que son niños plantea un relevante horizonte adicional que también debe abordarse. Muchas de las cuestiones relativas al manejo de información sobre niños son complejas y requieren decisiones delicadas. Las respuestas dependerán de la orientación de las políticas teniendo en cuenta notables consideraciones sobre la protección de datos.

Las presentes directrices cubren tres áreas principales: hechos, problemáticas y acciones futuras. La primera área tratada pone de relieve la extensión y el alcance de la información personal recopilada sobre los niños por parte de los organismos oficiales, cómo se usa (y se usará) dicha información y con quién se compartirá. Muchos de los planes existentes y propuestos no serán controvertidos, pero la imagen global y los vínculos crecientes entre los diferentes sistemas pueden sorprender a más de uno.

Por lo tanto, el libro toma distancia para identificar algunas de las cuestiones clave sobre protección de datos así como para plantear preguntas sobre ellas. La claridad de los objetivos, los fundamentos y la autoridad legal son importantes consideraciones a la hora de decidir qué es aceptable y qué no lo es. No obstante, existen otros asuntos prácticos, y tal vez más urgentes, que deben tratarse si se quieren evitar notables riesgos.

El apartado final establece futuras directrices que el Comisario estará en disposición de adoptar. Esto incluye una guía inmediata y futura sobre algunas cuestiones (como el consentimiento) y otras iniciativas basadas en mayor medida en las políticas. Un tema central es ayudar a los diversos organismos oficiales a entenderlo bien, incluido el garantizar la confianza y el apoyo máximos por parte del público en lo que hacen. Por consiguiente, nuestro enfoque es el de un compromiso constructivo y no el de la confrontación escéptica o negativa.

Las presentes directrices se apoyan en un informe de investigación elaborado para la *Information Commissioner's Office* [Oficina del Comisario de Información] por la *Foundation for Information Policy Research* (FIPR) [Fundación para la Investigación de las Políticas de Información]. El informe de investigación se publica simultáneamente y repasa numerosos aspectos de forma mucho más detallada. Las opiniones y conclusiones vertidas en el informe de la FIPR son las de dicha Fundación, y no reflejan las del Comisario o las de su Oficina.

## **2. EL INCREMENTO EN LA INFORMACIÓN ALMACENADA SOBRE LOS NIÑOS – LOS HECHOS**

La investigación de la FIPR ofrece un recuento exhaustivo de la gama de bases de datos que contienen información sobre los niños en los ámbitos de los servicios sociales, la educación, la delincuencia juvenil y la atención sanitaria. Asimismo, repasa el desarrollo de nuevos sistemas fundamentales para favorecer la divulgación de información, como el *Information Sharing Index* [Índice de Difusión de Información]. El informe identifica los objetivos expresados de políticas públicas detrás de cada iniciativa, la gama de información personal almacenada y de qué forma se usa y se divulga en la práctica dicha información. Muestra que, de una forma creciente, la motivación de las iniciativas ha pasado de centrarse en la *protección* infantil a ocuparse más del *bienestar* infantil, incluidas cuestiones como un rendimiento escolar deficiente o la pobreza. Asimismo, hay iniciativas para intentar lidiar con asuntos de mayor relevancia para la comunidad, en sentido amplio. Ello incluye recopilar y analizar factores de riesgo con el fin de intentar identificar a aquéllos que pueden verse implicados en delitos en algún momento posterior de sus vidas.

Éstas son las bases de datos principales o innovadoras que recopilan (o lo harán en breve) información sobre la infancia en Inglaterra.

DIRECTRICES PARA LA PROTECCIÓN DE LA INFORMACIÓN PERSONAL INFANTIL

Programa	Usado por	Contenido
Índice de Difusión de Información (IS). Se introducirá en 2008.	<i>Dept. for Education and Skills</i> (DfES) [Ministerio de Educación y Cualificaciones] y autoridades locales (LAs).	Información básica que identifique a todos los niños, con datos de contacto de profesionales habilitados e indicadores de interés.
<i>Integrated Children's System</i> (ICS) [Sistema de niños integrados]. Propuesto.	Servicios Sociales.	« <i>Electronic social care record</i> » (ESCR) [Registro electrónico de atención social] para los casos de niños en manos de trabajadores sociales. Almacenaría y analizaría información exhaustiva de niños y sus familias. Descargaría datos de otras bases pero no compartiría a su vez datos de forma automática.
<i>National Pupil Database</i> [Base de datos Nacional de Alumnos] (NPD).	DfES	Amplia información objetiva de cada niño en la enseñanza pública en Inglaterra.
RAISEonline ( <i>Reporting and Analysis for Improvement through School self-Evaluation</i> ) [Información y Análisis para la Mejora mediante la autoevaluación escolar]. Con vistas a la sustitución de un sistema actual similar.	<i>Office for Standards in Education</i> (Ofsted) [Organismo regulador de los centros escolares y escuelas].	Sistema para el análisis de datos en la NPD.
Base de datos « <i>Lost pupil</i> » [«Alumno perdido»].	Autoridades Locales de Enseñanza (LEAs)	Los datos más recientes de las NPD para niños que no estén actualmente en la enseñanza pública en Inglaterra.
ASSET	<i>Young Offenders' Teams</i> (YOTs) [Equipos para la delincuencia juvenil], <i>Youth Inclusion and Support Panels</i> (YISPs) [Paneles de integración y apoyo juvenil] y tribunales juveniles.	Perfiles de jóvenes delincuentes, basados en una variedad de factores, con fines de sentencia y rehabilitación.
ONSET Actualmente en periodo de prueba.	YISPs. Fundado por el <i>Youth Justice Board</i> [Consejo de Justicia Juvenil].	Idéntico a Asset pero para aquéllos sin antecedentes penales. Con el fin de identificar a aquéllos más propensos a incurrir en comportamiento delictivo.

Programa	Usado por	Contenido
RYOGENS	Producido por Esprit y actualmente usado por cinco Autoridades Locales.	Se ocupa de niños y jóvenes vulnerables.
<i>National Register of Unaccompanied Children (NRUC)</i> [Registro Nacional de Niños no acompañados].	Promovido por la <i>Association of London Government</i> [Asociación de Autoridades Locales de Londres]. Usado para intercambiar información entre Autoridades Locales y el <i>Immigration and Nationality Directorate (IND)</i> [Dirección General de Inmigración y Nacionalidad].	Intercambia información entre el IND y las Autoridades Locales sobre solicitantes de asilo menores de 18 años no acompañados. Con el fin de reunir fondos para el cuidado de dicho colectivo y reducir el uso fraudulento de la edad entre los solicitantes de asilo.
NOTIFY	<i>Greater London Authority</i> [Autoridad del Gran Londres] y distritos de Londres.	Localización y movimiento de familias sin hogar.
MERLIN	Policía Metropolitana.	Niños ' <i>Coming to notice</i> ' (CTN) ['puestos en conocimiento'] de la policía.

El **Índice de Difusión y Evaluación de Información (IS)** contiene únicamente la información de contacto para el niño, su colegio, su médico de cabecera y todo aquél que le esté proporcionando servicios públicos. No se incluye información adicional (como expedientes sanitarios o educativos). Si una persona implicada en el bienestar del niño desea hablar con el resto, puede señalar el expediente con una bandera para solicitar que las demás personas se pongan en contacto con ella.

Personal específico y previamente investigado puede tener acceso a la base de datos en diversas agencias implicadas en los servicios a la infancia. En caso de datos especialmente delicados, por ejemplo si un niño ha sido examinado por un especialista en salud mental, el acceso a dicha información está sujeto a una salvaguarda mayor, y sólo estará disponible con consentimiento expreso. La información de contacto de los niños sólo se omitirá del expediente si existe un riesgo real de que su inclusión los ponga en peligro.

La **Base de datos Nacional de Alumnos** contiene la información completa relativa al conjunto de los niños en la enseñanza pública, incluidos resultados de evaluación, orígenes étnicos y si reciben almuerzos escolares gratuitos. **RAISE-online** será usado por el consejo Ofsted de inspecciones escolares así como por las Autoridades Locales de Enseñanza (LEAs) con el fin de analizar los datos de la Base de datos Nacional de Alumnos. Por ejemplo, esto puede revelar que una escuela en particular necesita hacer más por los niños con necesidades educa-

## DIRECTRICES PARA LA PROTECCIÓN DE LA INFORMACIÓN PERSONAL INFANTIL

tivas especiales, o que los niños de un cierto grupo étnico están sufriendo retraso escolar. Asimismo, puede ser usado individualmente por escuelas para anticiparse a los resultados de sus propios alumnos.

**RYOGENS** es un sistema usado por funcionarios de sanidad, de trabajo social y de educación en el seno de Autoridades Locales para tomar nota de problemas generales relativos al bienestar de un niño, como la implicación en *bullying* [acoso], o el hecho de que un niño viva en un área desfavorecida. Si se registran un cierto número de problemas, el sistema lo notificará de forma automática al resto de departamentos relevantes dentro de dicha Autoridad Local. En la fecha de la investigación de la FIPR para su informe únicamente cinco Autoridades Locales estaban haciendo uso de él.

**Notify** es usado por varias autoridades gubernamentales locales en Londres para realizar un seguimiento de los movimientos de familias alojadas en emplazamientos temporales. Se colgarán de la Red informes completos de sanidad, vivienda y servicios sociales, pero este tipo de datos sólo estarán disponibles para profesionales relacionados con dicho aspecto de la atención a las familias.

**MERLIN** es un sistema de la Policía Metropolitana que incluye en su registro a todo niño que haya entrado en contacto con la policía de alguna forma, ya sea en calidad de víctima o de delincuente, porque vivan en el mismo hogar que un infractor o por cualquier otra razón.

La mayor parte de dichas bases de datos sólo otorgan acceso a información dentro del sector relevante, como la educación o la atención social. La principal excepción reside en sistemas que están diseñados para reducir la delincuencia juvenil y el comportamiento antisocial. RYOGENS, por ejemplo, permite la difusión no consentida de información entre servicios sociales, policía, sanidad, educación, vivienda y los equipos YOT.

### 3. PROBLEMAS Y PREGUNTAS

Es necesario un profundo debate sobre la gama y la amplitud de información que se recopila sobre los niños del país. Es difícil imaginar un núcleo familiar con hijos que no hayan sido incluidos en al menos una de las diversas bases de datos que se están elaborando. Mientras éstas pueden ser útiles a los objetivos esenciales de las políticas públicas, la recopilación y uso de cierta información puede estar adentrándose en terrenos que resulten incómodos. La creación del perfil de niños a una edad tan temprana por asuntos circunstanciales y las consecuencias para el resto de sus vidas es un ejemplo de ello.

Las presentes directrices se usarán para aumentar la concienciación de lo que está ocurriendo y generará y articulará debates posteriores. Tal vez aquéllos

que estén más directamente implicados deseen estudiar el análisis más amplio y profundo ofrecido por el informe de la FIPR.

La postura del Comisario de Información debe estar más directamente vinculada con sus responsabilidades en la protección de datos, especialmente para considerar un cierto número de cuestiones clave relativas a la protección de datos generado por la plétora de bases de datos infantiles. Tienen que ver tanto con el diseño como con la implementación y se expresan en términos generales, pero el Comisario es consciente de que algunos promotores y profesionales habilitados para ciertos programas abordan las diferentes problemáticas con más rigor que otros.

Las cuestiones fundamentales, ampliamente vinculadas con los principios reglamentarios más relevantes en la protección de datos, se incluyen en los siguientes epígrafes:

- Protección de la infancia como prioridad;
- Usos principales y secundarios;
- Tratamiento justo y legítimo;
- Precisión y calidad de la información;
- Seguridad;
- Derechos, especialmente, el acceso a los expedientes.

### **3.1. La protección de la infancia como prioridad**

Siempre debe ser prioritaria la protección de la infancia frente a un riesgo real de daño por abuso o abandono, generalmente por parte de sus progenitores o su cuidador. Está ampliamente aceptado, legal y éticamente, que se puede violar la confidencialidad por sólidos motivos de protección del niño. Durante mucho tiempo, ésta ha sido una parte integrante de las operaciones cotidianas de trabajadores sociales, médicos, docentes, policía y aquéllos que ofrecen consejo sobre cuestiones de manejo de información en el seno de dichos servicios. Al compartir las auténticas problemáticas sobre los niños o la familia, los profesionales están en disposición de elaborar un cuadro más preciso y exhaustivo de la seguridad y el bienestar de un niño. La difusión de la información puede resultar especialmente importante, dadas las situaciones extremas a las que pueden llegar aquellos que abusan para ocultar sus fechorías.

Es importante recalcar que la ley de protección de datos nunca se interpone en el uso o difusión de información personal -sobre los niños o, a veces, sobre terceros- cuando existe una necesidad real. Dañar a los niños mediante abusos o abandono es una actividad delictiva. La ley de protección de datos reco-

noce la importancia de prevenir y detectar el delito así como de perseguir a los infractores. Esto debe ser especialmente importante cuando las víctimas son niños.

La protección de datos nunca debería usarse como una excusa para dejar de proteger a un niño frente a un riesgo real de daño.

Las cuestiones de protección de datos pueden resultar menos claras cuando se centra la problemática en el bienestar de la infancia, en lugar de en su protección. La protección de los niños y su bienestar son temas diferentes. El bienestar de los niños constituye una categoría mucho más amplia, referida a los niños pobres, o infelices, o que viven en comunidades no gratificantes, o que en algún otro sentido están en peligro de no convertirse en adultos plenos con una oportunidad razonable de desarrollar su potencial. Mientras que la protección de la infancia se ocupa de un número relativamente reducido de niños, estimados en Inglaterra en unos 50.000, las problemáticas relativas al bienestar de los niños pueden atañer a tres o cuatro millones.

La agenda *Every Child Matters* [Todos los niños cuentan] amplía la atención social de la protección al bienestar. A pesar de que existan redundancias, este movimiento significa que, en esencia, se recopilará y se compartirá más información sobre una mayor cantidad de niños por diferentes razones. Estos diferentes objetivos suscitan diversas consideraciones desde una perspectiva de protección de datos. Es importante que no se dé por hecho que los enfoques usados en el marco de la protección sean transferibles al contexto del bienestar. La situación se complica todavía más si tenemos en cuenta los difusos límites que lo separan de la prevención de la delincuencia juvenil.

### **3.2. Usos principales y secundarios**

La confusión o la incertidumbre sobre la línea divisoria entre protección y bienestar ilustran bien la importancia de garantizar la claridad en los motivos por los que se recopila y se usa información. Un requisito fundamental y bien establecido de la protección de datos es que la información personal debería usarse con objetivos específicos y no debería tratarse de maneras incompatibles.

Aquéllos que diseñan o usan algún programa que recopila y usa información relativa a la infancia deben ser absolutamente claros en sus planteamientos. Debe existir un grado de especificidad y los límites de los motivos deben quedar claros. Es necesario justificar con claridad todo objetivo secundario. Dichas cuestiones son especialmente importantes cuando la información se difunde de una agencia a otra, en concreto, desde un ámbito a otro. Puede ser necesario preguntar si se requiere un cambio legislativo para permitir una amplia difusión de datos en casos de bienestar infantil así como en casos de protección de los niños. Sin embargo, aunque se creen portales reglamentarios para la difu-

sión de la información, sigue siendo relevante que exista claridad sobre qué información debería usarse para qué objetivo. Esto se debe reforzar mediante la orientación y la formación apropiadas para los profesionales habilitados.

El informe de la FIPR establece que algunos programas recientes y futuros ofrecen ejemplos de dichas problemáticas. Los autores de dicho informe se preocuparon en particular de las bases de datos *Connexions* [Conexiones], cuyo objetivo se define en la *Learning and Skills Act 2000* [Ley de las Competencias y el Aprendizaje de 2000] (s. 114) como '*estimular, permitir o guiar... la participación eficaz de jóvenes en la educación o la formación*'. Sin embargo, los datos de dicho sistema pueden pasarse a otros organismos que participen en alentar a los jóvenes a mantenerse alejados del delito, por ejemplo. Asimismo, el informe subraya el gradual cambio de objetivo de algunas bases de datos a lo largo del tiempo. La Base de datos Nacional de Alumnos pretendía originalmente contener únicamente datos anónimos con objetivos de control, pero en la actualidad incluye datos que pueden usarse (a través de RAISEonline) para tomar decisiones sobre alumnos particulares. RYOGENS, en un principio planteado como una herramienta para la prevención del delito, se usa ahora para compartir problemáticas básicas sobre los niños. En definitiva, los niños y los padres pueden no tener una comprensión clara del alcance de un proyecto o de cómo sus datos podrían usarse en el futuro.

### **3.3. Tratamiento justo y legítimo**

El hilo conductor del informe de la FIPR es que puede no ser fácil justificar como justa y legítima la recopilación y difusión de información sobre la infancia. En concreto, dicho informe se centra en la cuestión de si un niño puede otorgar consentimiento para que sus datos se usen sin remitirse a sus padres. El Comisario de Información reconoce las dificultades que conlleva evaluar si un niño es capaz de dar su consentimiento con plena conciencia, y en todo caso, recomendaría como una buena práctica que se consulte a los padres sobre decisiones importantes que afecten a sus hijos. No obstante, se debe hacer hincapié en que el *Data Protection Act 1998* [Ley de protección de datos personales de 1998] otorga derechos al Interesado, es decir, el niño. Dichos derechos sólo deberían ser ejercidos por otra persona *en su nombre* si los niños en cuestión están capacitados para ejercerlos de forma independiente. Dado el continuo desarrollo de jurisprudencia relativa a la autonomía de un niño, el Comisario considera que sería el momento adecuado para publicar una orientación más avanzada en el contexto de los derechos y obligaciones en la protección de datos. La ICO revisará qué puede hacer para ofrecer una guía más clara para aquellos que tienen que lidiar con difíciles decisiones prácticas.

Sin embargo, el consentimiento no será en todos los casos la única manera de garantizar un tratamiento justo y legítimo. De hecho, dada las complejas cuestiones que se han mencionado, puede ser más seguro para los responsables de

datos confiar en otro criterio para el tratamiento. Sin duda, no es la intención de la Ley de Protección de Datos personales privar a los niños de protección en los casos en que sus padres niegan su consentimiento sin razón. Asimismo, es importante que la búsqueda de consentimiento no se lleve a cabo sobre una base inadecuada, como en los casos en que el tratamiento tiene visos de proseguir con o sin el consentimiento. Los autores del informe de la FIPR también han mostrado su preocupación por las bases legales para el tratamiento y el uso de los llamados «portales reglamentarios» como una alternativa para otorgar el consentimiento cuando es necesaria la difusión de la información. Los portales reglamentarios pueden abarcar desde la autorización en términos de otorgar poderes legales hasta los basados en la coacción. Los efectos en términos de protección de datos varían en función del enfoque adoptado. La coacción puede hacer caso omiso de algunos aspectos de la Ley de Protección de Datos personales mientras que la posibilidad de difusión de información requiere aún un respeto sustancial de la protección de datos. Las cuestiones de difusión de información ya son objeto de un notable trabajo por parte del Gobierno y la ICO también está desarrollando una orientación práctica avanzada, incluido un código de práctica marco para la difusión de información con el fin de ayudar a los profesionales habilitados en un área compleja.

### **3.4. Precisión y calidad de la información**

Resulta indiscutible la importancia de que la información registrada sobre los niños sea precisa y esté actualizada. Casi es secundario que estos sean requerimientos legales. Ningún profesional que trate con un niño desea manejar información imprecisa u obsoleta. Un niño o su familia pueden sufrir graves daños si se registra una información imprecisa.

Aunque éste no sea un aspecto que se haya explorado completamente en el informe de la FIPR, el incremento de bases de datos que acumulan información sobre niños aumenta los riesgos de forma notable. La recopilación de más información aumenta la posibilidad de realizar errores mientras que la introducción (o la falta de actualización) de información y su uso y difusión generalizados magnifican el efecto potencial de dichos errores. Surgen otros riesgos desde el momento en que una base de datos comparte información con otra, especialmente cuando las actualizaciones no siguen el protocolo de transferencia inicial de datos. La fluidez de la vida moderna, con frecuentes cambios de domicilio y de composición familiar, exacerba los problemas en mayor grado.

La necesidad de calidad va más allá de la calidad de los datos en sí mismos. Además, suscita preguntas sobre la calidad de los sistemas para estructurar, acceder y buscar la información. En concreto, si demasiada información se hace impenetrable, los riesgos de pasar por alto los indicadores verdaderamente importantes magnifican el problema de «buscar una aguja en un pajar».

He aquí algunos ejemplos de los riesgos en los que se puede incurrir:

- Identidad errónea;
- Información imprecisa, incompleta u obsoleta sobre las circunstancias o características del niño o de la familia;
- Información imprecisa, incompleta u obsoleta sobre el contacto entre el profesional y el niño;
- «Alarmas perdidas» (Climbié) y «falsas alarmas» (Orkney) – la baja calidad de datos empeorará de forma simultánea ambos indicadores;
- Deducciones incorrectas sacadas de información ambigua, incompleta o que induce a error.

### **3.5. Seguridad**

Toda base de datos que contenga información personal requiere estar protegida con la seguridad adecuada. La Ley de Protección de Datos personales requiere que el nivel de seguridad tome en consideración el daño que un individuo puede sufrir como resultado de una falla en la seguridad. Las consecuencias de que la información más personal de miembros vulnerables de la sociedad caiga en manos equivocadas, como en las de aquéllos que pudieran intentar vivir a costa de niños, podrían resultar extremadamente graves.

El nivel de seguridad tendrá que tener en cuenta dicha posibilidad de daño y mantenerse en un nivel adecuadamente alto. Esto no se puede dejar al azar y requiere el diseño de sistemas desde los principios fundamentales y reforzados por los sistemas de trabajo que rodean su manejo. Los sistemas claramente establecidos diseñados para que numerosos individuos los consulten requieren rigurosos controles de acceso. De forma similar, el elemento humano es especialmente importante cuando la información puede compartirse entre profesionales habilitados desconocidos entre sí. Es esencial que las siguientes áreas se aborden de forma adecuada:

- Seguridad física, incluido el emplazamiento de equipo informático y el acceso físico a éste, en concreto, los dispositivos transportables como los ordenadores portátiles;
- Seguridad lógica, incluidas claves y niveles de acceso diferenciados en función de las necesidades del usuario;
- Procedimientos técnicos y de gestión para garantizar una seguridad eficaz así como el control del acceso, por ejemplo, mediante el uso de pistas de auditoría;

- Formación de personal para garantizar que la información no se usa de forma incorrecta ni se difunde erróneamente a terceros, respaldada por una medida disciplinaria adecuada cuando dicho personal incumpla a sabiendas los procedimientos de seguridad.

El Comisario ya ha solicitado sanciones más duras para aquéllos que, de forma deliberada, intenten usar incorrectamente información personal, y la posibilidad de que los datos de los niños caigan en manos de personas que puedan dañarlos pone de relieve la necesidad de sanciones penales eficaces para disuadir y castigar.

### **3.6. Derechos de acceso**

Una de las características clave de la legislación para la protección de datos consiste en el derecho de acceso otorgado a los individuos. Algunas bases de datos que pueden incluir perfiles de predicción, así como de otros tipos, pueden afectar a la forma en la que un individuo es tratado por aquéllos que entran en contacto con él. Es fundamental que los individuos puedan comprobar sin dificultad la amplitud, naturaleza y precisión de la información personal almacenada sobre ellos o sus hijos, en los casos en los que dichos niños sean incapaces de ejercer los mencionados derechos por sí mismos.

Es esencial que se pongan en marcha procedimientos apropiados para asegurar que se cumple con dicho derecho de acceso dentro del plazo reglamentario (40 días). Cuando se ven implicados niños, puede ser necesario juzgar si el niño es capaz de ejercer sus derechos por sí mismo o si resulta adecuado que un progenitor o un tutor a su cargo lo hagan en su nombre.

## **4. ACCIONES FUTURAS DE LA ICO**

La prioridad inmediata del Comisario consiste en garantizar que las cuestiones suscitadas en el presente libro alcancen a un amplio público, incluidas las personas que elaboran políticas, los organismos que recopilan y usan información sobre los niños, así como todos aquéllos que estén preocupados por la forma de proteger los derechos de privacidad de la infancia.

Se pueden identificar varias directrices más específicas:

### **4.1. Orientación desde la ICO**

Está claro que los que elaboran políticas y los profesionales habilitados necesitan y agradecerían una orientación práctica desde la oficina del Comisario sobre cuestiones relativas a las bases de datos de los niños.

#### **4.2. Consentimiento**

La orientación sobre cuestiones de consentimiento constituye una prioridad y, en el momento adecuado, se publicará una nota técnica de orientación al respecto. La ICO también está inmersa en el proceso de preparar un código de práctica marco para dar asistencia a las organizaciones del sector público a la hora de establecer los programas de difusión de información.

#### **4.3. Plantillas**

Asimismo, la ICO explorará el valor de elaborar una guía de fácil lectura con formato de plantilla, que puedan usar los servicios sociales para explicar las cuestiones básicas de protección de datos a sus clientes. Esto tomará la forma de una plantilla que permitirá a los profesionales habilitados y los estimulará, posiblemente en asociación con terceros, a confeccionar dicha plantilla con el fin de explicar su propio enfoque y ofrecer una orientación directamente a las familias afectadas. Incluirá asuntos como la cláusula de autoexclusión y los derechos de acceso. Puede existir margen para adoptar un enfoque similar para los profesionales de la enseñanza y la sanidad.

#### **4.4. Solicitudes de acceso del interesado**

La ICO valorará si es necesaria una mayor orientación para responder a las solicitudes de acceso del interesado con el fin de ayudar a las organizaciones a decidir cuándo es adecuado responder a dichas solicitudes realizadas en nombre de un niño, por ejemplo, por sus progenitores, y cuándo debe ser el niño el que ejercite los derechos por sí mismo.

#### **4.5. Jóvenes**

La ICO tendrá en cuenta intereses relevantes con el fin de diseñar un programa para preparar una nueva orientación destinada específicamente a los jóvenes, en concreto, a aquéllos en una franja de edad comprendida entre los 12 y los 18 años. Esto puede abordarse tanto de forma general (el conjunto de los niños) como selectiva (por ej., aquéllos en contacto con servicios sociales o la policía). Todo ello reflejará cómo valoran los niños su propia privacidad y confidencialidad y los ayudará a comprender cuál es la forma óptima de salvaguardar sus propios intereses. La ICO está especialmente preocupada por trabajar conjuntamente con organismos como los *Children's Commissioners* [Comisarios de la Infancia], que comparten un interés común en muchas de las cuestiones recogidas en el presente libro.

#### **4.6. Compromiso constructivo con el gobierno y funcionarios encargados de la elaboración de políticas**

En un espíritu de compromiso constructivo, el Comisario debatirá cuestiones relativas a las bases de datos de niños con los ministerios gubernamentales

*DIRECTRICES PARA LA PROTECCIÓN DE LA INFORMACIÓN PERSONAL INFANTIL*

encargados de la educación, la sanidad y la delincuencia juvenil. Las prioridades particulares incluirán:

- Minimizar los riesgos en la creación de perfiles: cuando se clasifica a un niño en una categoría de riesgo, se hace muy difícil para él que lleguen a verlo de una forma diferente aquéllos que entren en contacto con él en el futuro, independientemente de cómo se comporte el niño en cuestión. Esta forma de estigmatización corre el riesgo de convertirse en una profecía autocumplida para los niños afectados.
- Garantizar que están en marcha los mecanismos adecuados para reflejar las opiniones de progenitores e hijos al obtener información, incluido el asegurar que se busca el consentimiento cuando sea necesario y no se usa de una forma inadecuada.
- Establecer la manera más apropiada de difundir la información.
- Calidad de los datos.
- Seguridad.
- Establecer el valor de las 'Evaluaciones de Impacto sobre la Privacidad'.
- La participación de la ICO en el desarrollo de políticas futuras.

V. 1.0

22 de noviembre de 2006