Protección de la Infancia en Línea: Directrices para la industria

www.itu.int/cop

RECONOCIMIENTOS

Esta Guía ha sido preparada por la UIT y un equipo de autores de instituciones destacadas activas del sector de las TIC, y no habría sido posible sin su tiempo, entusiasmo y dedicación.

La UIT expresa su agradecimiento a todos los autores siguientes, que han aportado su tiempo y valiosos análisis: (por orden alfabético)

- Cristina Bueti y Marco Obiso (UIT)
- John Carr (*Children's Charities' Coalition on Internet Safety*)
- Natasha Jackson y Jenny Jones (GSMA)
- Nerisha Kajee y Rob.Borthwick (Vodafone)
- Giacomo Mazzone (UER) basado en los documentos facilitados por Marc Goodchild y Julian Coles (ambos de BBC)
- Michael Moran (Interpol)
- Brian Munyao Longwe (AfrISPA)
- Lorenzo Pupillo y Rocco Mammoliti (Telecom Italia)

Los autores agradecen particularmente los estudios y comentarios detallados de Kristin Kvigne (Interpol).

La UIT da las gracias asimismo a Salma Abbasi de eWWG por su valiosa participación en la iniciativa Protección de la Infancia en Línea (PIeL).

En la dirección http://www.itu.int/cop/ figura información y materiales adicionales sobre este proyecto de guía, que se actualizará periódicamente.

Si tiene algún comentario o desea facilitar información adicional, contacte via la dirección cop@itu.int

Índice

Prefacio

Resumen 1

Directrices para la industria 2

Principales esferas de estudio por toda la industria de TIC
Principales esferas de estudio por los radiodifusores
Principales esferas de estudio por los Proveedores de servicios Internet (PSI)
Principales esferas de estudio por los operadores móviles

1. Antecedentes 6

Colaboración con la Industria

2. Clasificación de contenidos y servicios 8

Radiodifusores

Estudio de caso: *British Broadcasting Company* (BBC) – Reino Unido **10**

Proveedores de servicios Internet

Estudio de caso: Seguridad "Big Six" de MySpace – Prácticas para los servicios de redes sociales **17**

Estudio de caso: Criterios de clasificación de contenido inalámbrico en EE.UU. **19**

3. Mecanismos de control de contenido 21

Radiodifusores
Proveedores de servicios Internet

Estudio de caso: Telecom Italia y la protección de los niños – Italia 26

Operadores móviles
Mecanismos de verificación de edad
Controles parentales

Estudio de caso: Controles parentales de NTT DoCoMo – Japón 31
Estudio de caso: ATT MEdiaTM controles parentales netos – EE.UU. 31

4. Educación y comunicación con los usuarios 32

Radiodifusores
Proveedores de servicios Internet
Utilizar los Términos y Condiciones
Operadores móviles

Estudio de caso: Código de conducta sobre los SMS con recargo de la Asociación de Proveedores de Servicio de Aplicaciones Inalámbricas (WASPA) – Sudáfrica 40
Estudio de caso: "Pistas para padres" de Vodafone – Reino Unido 41
Estudio de caso: Conocimiento de los medios CBBC – Reino Unido 45
Estudio de caso: Érase una vez el ciberespacio, MDA y Okto – Singapur 45
Estudio de caso: Comunicación con los clientes para luchar contra el spam y los SMS fraudulentos 46

5. Contenido ilegal 48

Términos y Condiciones, directrices de usuario

Procesos de señalar y tomar nota

Estudio de caso: Servicio de atención ante abusos y método de señalar y anotar – Telecom Italia **50**

Líneas de ayuda

Colaboración en la industria

6. Otros asuntos 53

Contenido generado por los usuarios: los radiodifusores

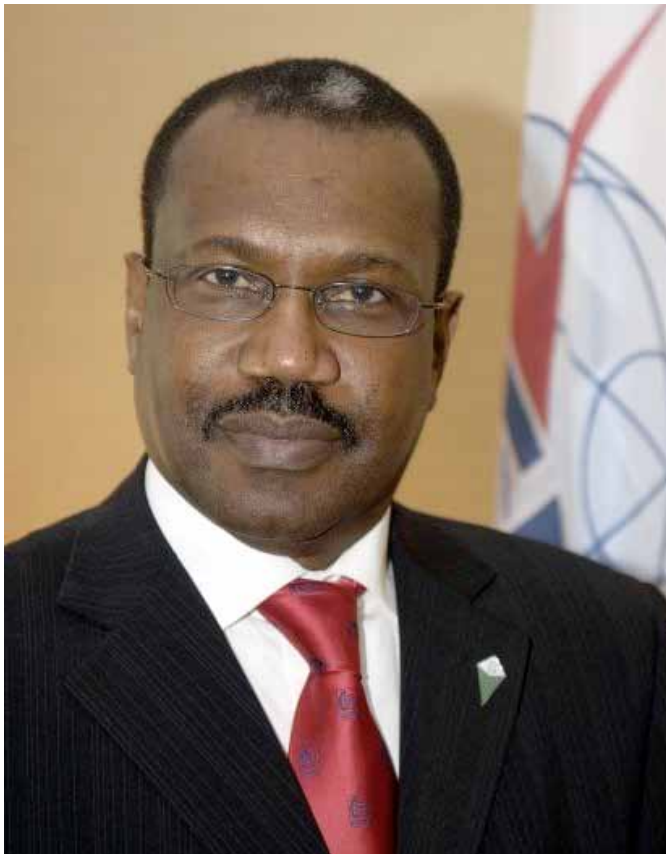
Estudio de caso: Cómo pueden los radiodifusores proteger a los niños contra el material inapropiado externo: el ejemplo de la BBC **55**

7. Conclusiones 56

8. Otra información y referencias 59


“La protección de los niños en línea es un problema mundial que necesita respuesta global”

Prefacio



Ha llegado el momento de presentarles esta Guía preliminar elaborada con la valiosa ayuda de numerosos especialistas.

Con la generalización de Internet de banda ancha, la Protección de la Infancia en Línea es fundamental y exige una respuesta mundial coordinada. Las iniciativas locales e incluso nacionales son muy importantes, pero Internet no tiene fronteras y la cooperación internacional será fundamental para ganar la batalla que debemos librar.

Radiodifusores, PSI y operadores móviles estarán en vanguardia de la lucha contra la ciberdelincuencia y la ciberamenaza, y les agradezco mucho su ayuda.

Dr Hamadoun I. Touré
Secretario General de la Unión Internacional de Telecomunicaciones (UIT)

"La Convención de las Naciones Unidas sobre los Derechos del Niño define niño como cualquier persona menor de 18 años. En estas Directrices se abordan todos los problemas a que se enfrentan las personas menores de 18 años en todo el mundo. Sin embargo, parece poco probable que un joven usuario de Internet de siete años tenga las mismas necesidades o intereses que uno de 12 años que empieza la enseñanza secundaria, o que uno de 17 años a punto de entrar en la edad adulta. En diversas partes de estas Directrices los consejos y recomendaciones se han adaptado a cada uno de esos distintos contextos. Si bien el recurso a categorías amplias puede ser útil como directriz, nunca se debe olvidar que, en último término, cada niño es distinto y las necesidades específicas de cada uno han de ser objeto de un análisis personalizado. Además, hay numerosos factores jurídicos y culturales diferentes, que pueden influir en gran medida en cómo utilizar o interpretar estas Directrices en cada país o región.

Existe hoy en día un gran número de instrumentos jurídicos internacionales que sustentan, y en muchos casos exigen, la toma de medidas de protección de los niños en general y, en particular, en lo que respecta a Internet. Estas leyes e instrumentos son los cimientos de estas Directrices y están ampliamente resumidos en la Declaración de Río de Janeiro y en el Plan de Acción para Prevenir y Eliminar la Explotación Sexual de Niños, Niñas y Adolescentes adoptada por el 3.º Congreso Mundial contra la Explotación Sexual de Niños, Niñas y Adolescentes, celebrada en noviembre de 2008."

Resumen

Estas Directrices se han preparado en el marco de la Iniciativa de la Protección de la Infancia en Línea (PIeL)[1] a fin de sentar las bases de un cibermundo seguro no sólo para los niños de hoy en día, sino también para las generaciones futuras.

La información presentada en estas Directrices ha sido preparada por la UIT, con la colaboración de una serie de autores procedentes de las principales instituciones del sector de TIC y, en concreto, la GSMA, Interpol, Afrispa, la UER, Telecom Italia, la *Children's Charities' Coalition on Internet Safety* y Vodafone.

La diversidad de colaboradores que han participado en la elaboración de este documento es en sí una prueba de los rápidos cambios que ha experimentado Internet como parte de la revolución digital, que prosigue a un ritmo acelerado.

La convergencia es hoy en día una realidad en muchos países y no cabe duda de que está trayendo con ella toda una serie de nuevos retos. La cooperación y la asociación son las claves para el progreso. Ningún sector de la industria tiene el monopolio de los conocimientos o el saber. Todos podemos aprender unos de otros.

La UIT, junto con los otros autores de este Informe, pide a todos los asociados que adopten políticas y normas que protejan a los niños en el ciberespacio y faciliten su acceso seguro a los recursos en línea.

Se espera que, de esta manera, no sólo se consiga construir una sociedad de la información más inclusiva, sino también que los Estados Miembros puedan cumplir sus obligaciones de protección y preservación de los derechos del niño, como se enuncia en el Convenio de las Naciones Unidas sobre los Derechos del Niño, adoptado por la Asamblea General de las Naciones Unidas en su Resolución 44/25 de 20 de noviembre de 1989 y en el Documento de Resultados de la CMSI.

[1] www.itu.int/cop

Directrices para la industria

En esta sección se presentan las directrices de protección de la infancia en línea para la industria. A fin de formular una estrategia nacional centrada en la seguridad de los niños en línea, los líderes de la industria habrán de considerar las siguientes estrategias para cada una de las esferas mencionadas a continuación:

		Principales esferas de estudio
Toda la industria de TIC		Hay una necesidad urgente de tomar medidas comunes más allá de las que cada organización de TIC pueda tomar individualmente, que son:
	1.	Elaboración de normas y recomendaciones conexas para la protección de la infancia en línea. El objetivo es elaborar un método común que pueda aplicar toda la industria.
	2.	Evaluar las opciones y posibilidades existentes de adopción de medidas coordinadas y coherentes en todo el mundo para proteger a los niños en línea. Ha de prestarse atención a la elaboración de las capacidades (por ejemplo, vigilancia y alerta y gestión de incidentes) que podrían facilitar el inventario de amenazas y la compartición de información entre distintos actores.
	3.	Identificar los puntos comunes entre diversos sectores (radiodifusores, Internet, móvil) a fin de elaborar Códigos de Conducta o de práctica que ayuden a los Estados Miembros de la UIT a colaborar más eficazmente con el sector privado/la industria.
	4.	Establecer acuerdos de cooperación entre los gobiernos y el sector privado/la industria para compartir información y desarrollar capacidades específicas destinadas a reducir los riesgos y ampliar la posible utilización de las TIC por parte de los niños.

		Principales esferas de estudio
Radiodifusores	5.	Elaborar normas comunes en materia de sistemas de presentación de reclamaciones. El objetivo es evitar que se dé la situación en que se añadan funciones de reclamación externas a los sistemas internos de los radiodifusores y se pueda crear más confusión entre los usuarios o se corra el riesgo de sobrecargar a la policía u otras entidades con un gran número de reclamaciones para las que sus servicios no están preparados o equipados para contestar.
	6.	Elaborar normas y recomendaciones comunes. El objetivo es crear un método ampliamente compartido de protección de la infancia en línea. Será necesario fomentar su adopción por parte de toda la industria.
	7.	Establecer un proyecto panindustrial para crear procedimientos más sólidos de obtención del consentimiento paterno antes de que los niños puedan acceder a contenidos no autorizados a todos los públicos, al menos a nivel regional.
		Principales esferas de estudio
Proveedores de servicios Internet (PSI)		Las siguientes recomendaciones son orientaciones para la industria de Internet y los proveedores de servicios Internet (PSI) a fin de crear un entorno más seguro para los usuarios jóvenes. Cada uno de los puntos indicados habrá de incluirse dentro de un marco más amplio para la protección de los usuarios por parte de los proveedores en línea responsables.
	8.	El objetivo estratégico de la industria de Internet a la hora de proteger a los niños ha de ser reducir la disponibilidad de contenidos y comportamientos nocivos o ilegales y reducir el acceso a los mismos. Los PSI también habrán de dar a niños y padres información y herramientas de fácil utilización para que puedan gestionar su uso de Internet de tal manera que se minimicen los posibles riesgos.
	9.	El lenguaje y el vocabulario de los sitios Internet y los servicios Web 2.0 habrán de ser accesibles, claros y pertinentes para todos los usuarios, incluidos los niños, los jóvenes, los padres y los cuidadores, en especial en los Términos y Condiciones, la política de privacidad, la información de seguridad y los mecanismos de informe.
	10.	Informar sobre problemas, abusos y comportamientos ilegales: es muy importante que los proveedores de servicio dispongan de procedimientos robustos para la tramitación de reclamaciones. En concreto, las reclamaciones sobre acoso y contenido inadecuado habrán de examinarse prontamente y, si procede, se tendrá que eliminar rápidamente el contenido ofensivo. En la medida de lo posible, los proveedores de servicio deberán considerar la posibilidad de contar con mecanismos, como enlaces para comunicar abusos o marcar perfiles que puedan no ser adecuados o representen un riesgo para niños y jóvenes, y tener la capacidad de llevar tales informes hasta las fuerzas de seguridad, si procede.

		Principales esferas de estudio
	11.	Los proveedores de servicios han de considerar la posibilidad de incorporar por defecto la capacidad de informe en todas sus páginas y servicios web ofrecidos, por medio de un "botón de informe de abuso", en la medida de lo posible. Podría crearse un botón común reconocible, que se encontrase siempre en la misma ubicación en todas las páginas. El mecanismo de informe podría mejorarse ofreciendo soluciones técnicas al usuario, como la capacidad de anexar las pantallas, las estadísticas de conexión, las listas de procesos en curso, etc., además de informar al usuario de la información que ha de incluir con los informes para que sean efectivos.
	12.	Los proveedores de servicio han de considerar la posibilidad de insistir, en un lenguaje accesible y de fácil comprensión, en los comportamientos aceptables y no aceptables dentro del servicio, en especial para los jóvenes usuarios y sus padres o tutores. Se sugiere que esta información se facilite directamente, además de incluirse en los Términos y Condiciones.
	13.	Los proveedores de servicio deberán seguir evaluando la eficacia de las tecnologías de identificación y verificación de la edad de los consumidores. El objetivo ha de ser la aplicación de una solución adecuada a cada servicio (lo que es especialmente importante cuando el servicio en cuestión está sujeto a restricciones jurídicas en función de la edad), en la medida en que tal solución sea jurídica y técnicamente viable y, lo que es más importante, crear servicios Internet más seguros. Tales soluciones podrán impedir a los menores acceder y verse expuestos a contenidos o servicios inapropiados, o que a los servicios destinados a los niños no puedan acceder los adultos.
	14.	Los proveedores de servicio habrán de considerar la posibilidad de comunicarse proactivamente con las fuerzas de seguridad locales o nacionales para informar de abusos ilegales sobre los niños tan pronto como tengan noticia de ello. También habrán de disponer de procedimientos internos que garanticen el cumplimiento de sus responsabilidades en virtud de las leyes nacionales y/o internacionales en materia de contenido ilegal. También habrán de considerar la posibilidad de evaluar el contenido comercial insertado en sus propios servicios (ya sea de sus anunciantes o del contenido de proveedores de contenido terceros) periódicamente, en la medida de lo posible, a fin de garantizar que no se puede acceder a contenidos potencialmente nocivos desde su red. Para asistirles en esta tarea existen programas de escaneado y reconocimiento de imagen.

		Principales esferas de estudio
Operadores móviles		A continuación se presenta una "lista de verificación" de los puntos que los operadores móviles pueden considerar a la hora de proteger a los niños, tanto en términos de creación de un entorno móvil seguro y adecuado para los usuarios jóvenes, como en términos de lucha contra la posible utilización impropia de sus servicios para la distribución y publicación de contenidos ilegales de abuso sexual infantil:
	15.	Si la oferta de contenido y servicios no es apropiada para usuarios de todas las edades, se garantizará que el contenido se clasifica de conformidad con la reglamentación nacional, de forma compatible con las normas existentes sobre medios equivalentes y que se ofrece junto con capacidades de verificación de la edad, si es posible.
	16.	De ser posible, se colaborará con otros operadores del mercado para llegar a un acuerdo sobre compromisos de la industria en materia de ofertas de contenido no apropiado para todas las edades, y se fomentarán tales compromisos.
	17.	Se facilitarán herramientas para permitir el control por parte del usuario o sus padres/tutores del acceso al contenido. También estas herramientas habrán de ser conformes con la reglamentación nacional y las normas sobre medios equivalentes.
	18.	Se señalará claramente la naturaleza del contenido y los servicios ofrecidos de manera que los usuarios puedan tomar, con conocimiento de causa, decisiones sobre el consumo de tal contenido y sobre todo compromiso (por ejemplo, periodo de suscripción mínimo) que puedan adquirir.
	19	Se facilitará a los padres el entendimiento de todos los servicios de contenidos móviles que sus hijos puedan estar utilizando, de manera que puedan guiarlos hacia una utilización apropiada de los mismos.
	20.	Se educará a los clientes sobre la manera de gestionar problemas relacionados con la utilización móvil, en general, incluidos temas como el correo basura, el robo, y los contactos inapropiados, por ejemplo, de intimidación, y se garantizará que los clientes dispongan de un medio para comunicar tales problemas.
	21.	Se utilizarán los Términos y Condiciones de cliente para manifestar explícitamente la postura de la empresa con respecto a la utilización indebida de los servicios para almacenar o compartir contenido de abuso sexual infantil, así como su compromiso para con las investigaciones que lleven a cabo las fuerzas al respecto, de conformidad con la legislación nacional; se dispondrá de procesos Notificación y Bloqueo (NTD) o semejantes; cuando las haya, se prestará apoyo a las líneas de ayuda nacionales o similares.

1. Antecedentes

En la actualidad, lo digital ha transformado el estilo de vida en todo el mundo. Hace tiempo que la industria informática es totalmente digital, la industria de telecomunicaciones casi lo es y el sector de la radiodifusión lleva muy avanzada su conversión de analógico a digital. El acceso permanente a Internet es hoy en día normal, pues las personas cada vez pasan más tiempo consumiendo medios digitales que de cualquier otro tipo.

El estilo de vida se está igualando desde China hasta Italia gracias al SMS, el correo-e, los chats, las citas en línea, los juegos en línea, los mundos virtuales y los multimedios digitales.

Aunque estas tecnologías aportan comodidad y diversión a muchas personas, los reguladores y los usuarios suelen encontrarse siempre un paso por detrás de las rápidas innovaciones que experimenta este campo. Además, a medida que se diversifica el número de canales para la entrega de servicios, las empresas más y menos tradicionales del sector se enfrentan a nuevos dilemas.

Colaboración con la Industria

En el mundo convergente de hoy en día, la tradicional distinción entre distintas partes de las industrias de telecomunicaciones y de telefonía móvil, entre empresas de Internet y radiodifusores, está desapareciendo y ha dejado de ser relevante. La convergencia está aunando los distintos canales digitales en un único flujo que llega a miles de millones de personas de todo el mundo. Es

en este contexto donde la UIT, en colaboración con la GSMA, Telecom Italia, la Unión Europea de Radiodifusión, Interpol, la *Children's Charities' Coalition on Internet Safety*, Vodafone y Afrispa, ha preparado estas Directrices para la Industria en el marco del Programa de Protección de la Infancia en Línea. Su objetivo es asentar un marco común para que todos los participantes de la industria trabajen juntos hacia el objetivo común de que Internet sea lo más seguro posible para los niños y los jóvenes, estableciendo, por ejemplo, códigos de conducta o fuentes autorizadas de asesoría y orientación.

Los proveedores de servicios Internet, en concreto, hace tiempo que han aceptado que tienen una especial responsabilidad con respecto a la protección de la infancia en línea, en gran parte debido a que los PSI son tanto el conducto que ofrece acceso desde y hacia Internet, como un depósito que acoge, reserva y almacena los servicios que ofrecen. Lo mismo ocurre con las redes de telefonía móvil, muchas de las cuales extienden sus funcionalidades mucho más allá del intercambio de voz y datos original. También los radiodifusores desempeñan un gran papel en el espacio Internet, ofreciendo múltiples servicios en línea que antes sólo se asociaban a los PSI o las empresas de servicios en línea. No obstante, dada la enorme cantidad de empresas involucradas, generalmente creadas muchos años antes de que Internet se convirtiera en un producto de consumo masivo, los sitios de los radiodifusores suelen atraer a muchos seguidores.

Cada uno de los sectores que han colaborado en este proyecto ha aportado su propia experiencia y su propia historia. Al colaborar de esta manera, poniendo en común conocimientos y experiencia, toda la industria está encantada de poder avanzar hacia un Internet más seguro para todos, pero sobre todo para los niños y los jóvenes.

2. Clasificación de contenidos y servicios

La noción de que no todos los contenidos y servicios son adecuados para todos los públicos está muy clara en el mundo "fuera de línea". Las películas y juegos, por ejemplo, tienen una clasificación por edades, y los programas de televisión con contenidos violentos o de carácter sexual están sujetos a restricciones horarias.

Cuando el contenido en línea sea exactamente igual al de su versión "fuera de línea" (por ejemplo, un juego o película donde sólo cambia el canal de acceso), será posible reutilizar las clasificaciones existentes. Sin embargo, cuando se trate de contenido nuevo o modificado, tanto el contenido como los proveedores de servicio tendrán que encontrar métodos de indicar la naturaleza de tal contenido y la edad de la audiencia a que está destinado.

En el caso de contenido más tradicional (por ejemplo, vídeos musicales), generalmente es posible aplicar una clasificación por edad estableciendo unas normas de referencia conformes con los marcos nacionales (o regionales, en función del grado de sensibilidad social compartida) aplicables a otros medios, como juegos o películas. Sin embargo, la creciente gama de atractivos servicios interactivos, como tablones de anuncios, salas de charlas, redes sociales y servicios de contenido generado por los usuarios, si bien son más difíciles de "clasificar" de manera tradicional, también pueden presentar riesgos para los jóvenes usuarios, no sólo por el consumo de contenido no adecuado para su edad, sino también por la exposición a conductas (por ejemplo, intimidación) y contactos (por ejemplo, corrupción) impropios.

Todos estos problemas se tratan en las siguientes subsecciones. En el apartado dedicado a los radiodifusores se trata el problema que supone poner a disposición contenido tradicional a través de un nuevo medio. En el apartado de proveedores Internet se observan los problemas de contenido, contacto y conducto en la gestión de servicios en línea no tradicionales. El apartado de operadores móviles presenta la manera en que los operadores de todo el mundo están afrontando el problema de la clasificación y gestión de contenidos y servicios móviles.

Radiodifusores

Los radiodifusores de televisión siempre han sabido aprovechar la naturaleza lineal de la "radiodifusión" de televisión para ocuparse de los problemas relacionados con los contenidos no adecuados para todos los públicos modificando su horario de emisión; por ejemplo, emitiendo el contenido adecuado sólo para adultos o adolescentes a última hora de la tarde o por la noche (después del "toque de queda"), cuando los niños pequeños duermen.

Sin embargo, dado que los radiodifusores con cada vez más frecuencia emiten su contenido en línea de manera no lineal "a la carta", sin seguridad de que haya una supervisión paterna directa y donde no se puede definir el horario de emisión, los radiodifusores han estado buscando maneras de ofrecer su contenido de manera adecuada a la edad de los espectadores.

Las investigaciones muestran que, en general, los padres desean conocer los tipos de contenido que pueden causar problemas (como lenguaje obsceno o violencia), en lugar de que se les ofrezca una simple clasificación por edad.

Por este motivo, algunos radiodifusores han establecido un sistema de etiquetado. Por ejemplo, la BBC ha elaborado el sistema de etiquetado de orientación, 'G', donde aparece este símbolo cuando el contenido incluye material sensible, que se explicita en la sinopsis del programa. La presencia del símbolo 'G' se utiliza para activar los sistemas de control parental con PIN, si están activados.

Nota – A menos que se indique lo contrario, el término "radiodifusores" en este documento se refiere específicamente a los proveedores de contenido de radiodifusión tradicional, en el sentido de que el "radiodifusor" tiene control creativo y editorial sobre el contenido expuesto que se "emita" o, como se observa en este documento, se facilite en línea. Este término no incluye a los proveedores de servicio que permiten la publicación de contenidos creados por terceros. Estas entidades entran dentro de la categoría de proveedores de servicios Internet.

Estudio de caso: British Broadcasting Company (BBC) – Reino Unido

Con su propuesta *iPlayer*, que facilita acceso en línea a la programación de la BBC de forma no lineal (o "a la carta") y también contribuye en un 9% al tráfico total de Internet en Reino Unido, la BBC ha adquirido una importante experiencia en la gestión de la entrega responsable de contenido no adaptado a todos los públicos.

En la actualidad, la instalación del *iPlayer* de la BBC está restringida a los mayores de 16 años. También se informa a los usuarios de la protección mediante PIN durante el proceso de inscripción y ellos deciden si quieren activarlo y cuándo. Si optan por no hacerlo, se les indica cómo hacerlo más adelante. Si el programa no está adaptado a todos los públicos (es decir, para todas las edades), llevará un aviso de orientación, en este caso el símbolo 'G', además de texto explicativo de la naturaleza del contenido, en el momento en que el usuario haya de decidir si descargar el contenido. En el momento de visualización también aparece el texto explicativo y el usuario tendrá que introducir su número PIN, si lo ha activado, antes de poder ver el contenido. Toda persona que utilice el *iPlayer* sin el código PIN correcto recibirá un mensaje indicándole que no tiene el permiso necesario para acceder al contenido marcado con el símbolo 'G'.

En breve, la BBC introducirá la difusión en directo a través del *iPlayer*, donde los programas pertinentes también irán marcados con la 'G' y el texto explicativo antes de que puedan visionarse. Desde el principio se dispondrá de un sistema de protección por PIN y, en la actualidad, la BBC está estudiando maneras de reforzar este sistema aún más, pues la difusión y la descarga estarán integradas en un solo sistema.

La 'G' del sistema de orientación de la BBC ha sido adoptada por otros radiodifusores terrenales de Reino Unido, incluidos ITV, *Channel Four* y FIVE para sus ofertas a la carta en línea.

La BBC tiene una estrategia muy clara para la protección de niños y adolescentes de todas las edades a través de tres sitios donde se indican, para cada edad, los niveles de protección, conocimientos informáticos, independencia y madurez adecuados, así como mediante otros servicios educativos ofrecidos a través de *BBC Learning*.

1. Los sitios CBeebies (www.bbc.co.uk/cbeebies) y CBBC (www.bbc.co.uk/cbbc) permiten a los niños y sus padres o tutores interactuar con la BBC y entre ellos de manera segura, fiable y accesible. Estos sitios tienen una alta calidad y contenido y experiencias interactivas, interesantes y atractivos para los niños, y además sirve de trampolín hacia los mejores sitios web externos adecuados para niños de menos de 12 años.

2. El objetivo es dar a los niños el poder y la oportunidad de ahondar su relación con la BBC, sus productos y personajes, aumentando el valor recibido, su sentimiento de propiedad y su participación en CBeebies y CBBC. Para ello, estos sitios ofrecen una serie de herramientas innovadoras e interactivas, así como creativas, destinadas a que todos los niños

británicos, sea cuál sea su origen y capacidad, tengan un espacio para publicar su propio contenido, pensamientos y opiniones. También contiene un servicio de noticias 24 horas al día en línea para niños, como parte de *Newsround*, y a través de la sección *PressPack* los niños pueden participar activamente sobre temas de su interés.

3. *BBC Switch* es un espacio en línea para adolescentes con contenido destinado a los jóvenes sobre sus intereses y que fomenta la interacción. Este sitio contiene programas de televisión y radio además de contenido independiente. (www.bbc.co.uk/switch).

4. *BBC Learning* está dirigido a los niños en edad escolar y aborda una amplia gama de temas vinculados a los estudios o capacidades específicas, entre los que se cuentan:

Bitesize – servicio de revisión y recapitulación de los principales temas para niños entre 5 y 16 años (www.bbc.co.uk/schools/ks3bitesize).

Blast – desarrollo creativo para adolescentes centrado en artes creativas. Está asociado a organizaciones artísticas para jóvenes (www.bbc.co.uk/blast).

Algunos servicios están diseñados para su uso en las aulas y otros para ser utilizados directamente por los alumnos, sin necesidad de tutor, desde casa o en la escuela.

La BBC colabora estrechamente con Ofcom (regulador de medios y telecomunicaciones de Reino Unido) y con una serie de radiodifusores y proveedores de plataformas a fin de fomentar la utilización de prácticas idóneas en materia de marcación. La BBC también participa activamente en el Grupo de Información de Contenido del BSG. La BBC es también miembro asociado de la Asociación de Televisión a la Carta (ATVOD), organismo de autorreglamentación de los servicios a la carta


Social
Networking

Proveedores de servicios Internet

Por norma general, contenido Internet y servicios Web 2.0 son términos relativos a la creciente utilización de Internet por particulares a fin de crear y distribuir su propio contenido en formato escrito y audiovisual. Como ejemplos de servicios Web 2.0 se pueden citar:

- **Contenido generado por el usuario:** sitios como wikis, blogs y de compartición de imágenes, diseñados específicamente para que los usuarios telecarguen, compartan o visualicen el contenido.
- **Sitios de redes sociales** donde los usuarios exponen su "perfil" personal con información como su lugar de residencia, sus intereses y gustos (por ejemplo, música, películas y libros), así como fotografías o vídeos, canciones y enlaces a los perfiles de sus amigos. También pueden contener funcionalidades de charla, compartición de ficheros, creación de blogs y grupos de debate.
- **Comunidades en línea y mundos sociales** donde los participantes seleccionan, personalizan o crean personajes, llamados "avatares". Sus avatares pueden construir viviendas, crear entornos, interactuar con otros e incluso intercambiar dinero virtual al comprar o vender objetos en un mundo virtual con múltiples jugadores.
- **Juegos en línea** donde se puede jugar con otras personas, generalmente en complejos y extensos "mundos lúdicos" donde pueden interactuar y hablar entre ellos durante el juego.

Con frecuencia, estas categorías se superponen y se considera cada vez más que estas redes forman parte de la cultura joven, como se indica en el completo e independiente informe realizado en Reino Unido sobre los riesgos que corren los niños en Internet y los videojuegos.

Puede resultar útil distinguir entre riesgos potenciales basados en "contenidos", "contactos" y "conductas", de acuerdo con la estructura establecida por el proyecto Kids Online de la UE[2]. Gracias a Web 2.0 y a la creciente interactividad resultante, ahora es posible establecer comunicaciones uno a uno, uno a muchos y muchos a muchos. Evidentemente, esto aumenta la posibilidad de establecer contactos no deseados y, en algunos casos, llevar a conductas ilegales. Establecer una distinción entre contacto y conducta es útil para entender las diferencias, coincidencias e identificar las medidas que se pueden tomar. La principal diferencia es que "contacto" se refiere a la situación en que el niño es el receptor de la comunicación/mensaje (la 'víctima'); mientras que por "conducta" se entiende la situación en que el niño es el instigador del comportamiento impropio (el "ejecutante")[3]. Otros organismos han añadido dos categorías que

[2] www.eukidsonline.net/

Nota: En las secciones dirigidas a proveedores de servicios Internet se abordan temas que atañen a toda la industria de Internet, incluidos los proveedores de acceso Internet, así como los proveedores de servicios electrónicos/proveedores de contenido y servicios, a los que se denomina colectivamente en este documento proveedores de servicios Internet (PSI). Por tanto, cabe señalar que no todas las recomendaciones serán de aplicación para todos los PSI.

[3] *Safer Children in a Digital World: the report of the Byron Review* (http://www.dcsf.gov.uk/byronreview/).

conviene recordar: "comercio" –que se refiere a la posible explotación de niños y jóvenes por parte de empresas sin escrúpulos que se aprovechan de su inexperiencia, o a problemas como la peska, ante los cuales los jóvenes pueden ser más vulnerables. Por ultimo, está el problema de la "adicción", que se refiere a la manera en que algunos niños y jóvenes puede llegar a obsesionarse con la tecnología de tal manera que supone un obstáculo o barrera para el desarrollo de relaciones normales con otras personas o para su participación en actividades físicas sanas.

Desde el punto de vista de la industria de Internet, hay tres objetivos estratégicos clave para la seguridad de los niños en Internet, que requieren que la industria y los padres/tutores, adopten conjuntamente la responsabilidad de aumentar la seguridad de los niños en línea:

- **Reducir la disponibilidad**: reducir la disponibilidad de los contenidos, contactos y conductas inadecuados (industria).
- **Restringir el acceso**: dar a los niños y padres las herramientas necesarias para gestionar el acceso al contenido inadecuado (industria y familia).
- **Aumentar la resistencia**: aumentar la resistencia de los niños al material al que pueden verse expuestos; enseñar a los niños cómo reaccionar ante los contenidos y contactos inadecuados y enseñar a los padres a ayudar a sus hijos en tales casos y a evitar que los niños tengan conductas dañinas o inadecuadas (padres).

La naturaleza misma de Internet hace que no haya un único punto evidente donde se pueda ejercer un control editorial, contrariamente a lo que ocurre en los medios de radiodifusión, donde cada canal ejerce tal control. Hay controles editoriales (por ejemplo, moderadores de sitios de contenido generado por el usuario), pero están muy dispersos por la "cadena de producción Internet". En esta cadena hay productores de contenido, agregadores de contenido, proveedores de servicios Internet (PSI) y anfitriones web, proveedores de búsqueda, directorio y web, dispositivos de usuario, etc.

En cada punto de la cadena hay una serie de herramientas técnicas que pueden ayudar a los padres a gestionar el acceso a Internet de sus hijos (por ejemplo, programas de control parental, búsquedas seguras y verificación de edad en sitios web).

Un ejemplo de la función de la industria de Internet en cooperación con las familias es el siguiente:

1. Los sitios web de contenido generado por los usuarios eliminan los contenidos dañinos o inapropiados telecargados en ellos.
2. Los niños y padres indican a los anfitriones la presencia de material dañino o inapropiado en sus sitios, cuando lo encuentran.
3. Los PSI bloquean el acceso a material ilegal, como imágenes pedófilas.
4. Los padres instalan software para filtrar los contenidos dañinos o inapropiados.
5. Los sitios web aconsejan de manera clara y fácilmente visible cómo mantenerse seguro.

6. Los padres hablan con sus hijos, y ellos con sus hermanos y amigos, sobre ciberseguridad.

Reducir la disponibilidad:

Los proveedores de servicio pueden alcanzar el objetivo de reducir la disponibilidad de contenidos, contactos y conductas dañinas o inadecuadas de la siguiente manera:

- Adoptar **un proceso de moderación** efectivo del contenido generado por los usuarios. Por ejemplo, MySpace examina todas las imágenes y vídeos telecargados en su sitio.
- Basar el proceso de moderación en los informes de los usuarios. Responder efectivamente a los informes de más de un usuario y de usuarios continuos (en función de su nivel de actividad o la clasificación o reputación indicada por otros usuarios) puede contribuir a crear una comunidad activa de "autopolicías" que se protejan y protejan a otros en línea.
- Establecer un mecanismo de información de la existencia de contenidos, contactos o comportamientos inapropiados, como se incluye en los términos de servicio, la política de uso aceptable y/o las directrices para el usuario. Estos mecanismos han de ser de fácil acceso para el usuario en todo momento y el procedimiento ha de ser sencillo de entender y estar adaptado a todas las edades. Ha de acusarse recibo de los informes y reaccionar rápidamente. Ha de darse a los usuarios la información que necesitan para elaborar un informe eficaz y, si procede, una indicación de la tramitación normal de los informes.
- Vincular los informes de abuso a los procesos de "notificación y bloqueo", con un acuerdo de nivel de servicio público sobre los tiempos de respuesta o eliminación.
- Evitar la **publicidad en línea de contenido** dañino o inadecuado.

Restringir el acceso:

Se puede lograr el objetivo de restringir el acceso a contenidos inapropiados de las siguientes maneras:

- **Software de control parental**, que permite a los padres administrar el acceso de sus hijos a los recursos Internet.
- **Las herramientas de seguridad en Internet**, incluido el control parental, en el mejor de los casos deberían permitir las listas blancas, el filtrado del contenido, la supervisión de utilización, la gestión de contactos y el establecimiento de límites de tiempo/programas.
- Las computadoras nuevas deberían tener **"por defecto" activado el software de control parental**, mensajes de seguridad que expliquen las funcionalidades por defecto.
- Adoptar la **"búsqueda segura"**: la mayoría de motores de búsqueda ofrecen una opción de búsqueda segura, que no devuelve resultados que contengan imágenes o palabras clave que se puedan considerar inapropiadas para los niños.
- Adoptar métodos adecuados de verificación de edad para impedir que los niños accedan a contenidos inadecuados para

su edad, o a sitios o servicios interactivos, como las salas de chat, etc., donde puede haber riesgo de encontrar contactos y conductas inapropiados.

- **Etiquetado del contenido**: Los proveedores de contenido profesional (es decir, juegos, contenido con control editorial de radiodifusión) deben explicar claramente con una etiqueta externa el contenido de sus sitios para indicar su adecuación para niños.
- **Bloqueo a nivel de red**, donde, de acuerdo con criterios nacionales, ciertos materiales, como las imágenes pedófilas, en Internet es claramente ilegal.

Aumento de la resistencia:

Aumentar la capacidad de los niños para gestionar riesgos es un objetivo importante e interdependiente y complementario de los otros dos objetivos: reducir la disponibilidad y restringir el acceso.

Aunque los padres y niños tienen un papel que desempeñar en la reducción de la disponibilidad de material dañino e inapropiado (por ejemplo, informando de los abusos a los anfitriones), esta tarea corresponde sobre todo a la industria. Y, aunque la industria tiene su función en aumentar la resistencia de los niños (por ejemplo, con avisos de seguridad), son los padres y las personas que trabajan con niños las que tienen más influencia y, por tanto más responsabilidad.

Estos papeles, distintos pero complementarios, de la industria y las familias para la consecución de los tres objetivos, son muy importantes y revelan la necesidad de contar con una estrategia nacional y compartida para la protección de los niños en línea que pueda influir y capacitar tanto a la industria como a las familias.

Al observar los puntos fuertes y débiles de las actuales estrategias para mejorar la seguridad de los niños en Internet, así como las diferentes legislaciones nacionales, la industria de Internet puede elaborar códigos de práctica nacionales autorreglamentados, que serán más transparentes que las directrices prácticas, siempre y cuando el organismo controlador/coordinador realice su función eficazmente y publique los resultados. También pueden elaborarse mecanismos dentro de estos marcos que den cabida a la opinión de padres y niños.

Operadores móviles

A medida que aumenta el número de operadores móviles que ofrecen a sus clientes acceso a una amplia y atractiva gama de servicios de contenido, incluidos juegos, música, vídeos y programas de televisión, éstos se ven enfrentados con el problema que supone gestionar el acceso de los clientes a contenido comercial que estaría sujeto a restricciones de edad, si se facilitase por otros canales.

La creciente gama de nuevos servicios comunitarios e interactivos a disposición de los usuarios también plantean problemas en cuanto a la edad de estos últimos, por ejemplo, muchos sitios de redes sociales importantes incluyen en sus términos de servicio requisitos mínimos de edad, pues se teme que los usuarios más jóvenes se enfrenten a los riesgos, como el

Estudio de caso: Seguridad “Big Six” de MySpace – Prácticas para los servicios de redes sociales

- **Examen de imágenes y vídeos:** los sitios deberían encontrar la manera de examinar las imágenes y vídeos que acogen a fin de eliminar los que se consideren inapropiados.
- **Examen de grupos de discusión:** las redes sociales deberían examinar los grupos de debate para encontrar temas dañinos, lenguaje ofensivo y comportamientos ilegales y eliminar el contenido que conlleven.
- **Eliminación de agresores sexuales fichados:** las redes sociales deberían impedir a los agresores sexuales fichados que creen cuentas en sus sitios, gracias a tecnología ya existente.
- **Importantes esfuerzos para aplicar los requisitos de edad mínima:** los sitios deberían aplicar sus requisitos de edad mínima y tomar medidas para identificar y eliminar a los usuarios que hayan falsificado información para obtener acceso.
- **Protección de los usuarios más jóvenes contra comunicaciones no deseadas:** las redes sociales han de utilizar una configuración de privacidad por defecto para impedir que los adultos entren en contacto con menores de 16 años a los que no conozcan en la vida real.
- **Cooperación con las fuerzas de seguridad:** todos los sitios deberían tener líneas telefónicas de ayuda disponibles en todo momento para asistir a las fuerzas de seguridad en caso de emergencia y durante las investigaciones rutinarias.

robo de identidad o los contactos inapropiados, que supone facilitar demasiada información sobre uno mismo, etc.

A fin de utilizar un método común y transparente, los operadores móviles y los proveedores de contenido de una serie de países están reaccionando ante la situación trabajando de consuno para elaborar sistemas de clasificación. Los sistemas de clasificación normalmente están diseñados para gestionar contenido móvil comercial, es decir, contenido que producen los operadores móviles mismos o en colaboración con terceros, y se basan en las normas nacionales aceptadas y son coherentes con los métodos aplicados en medios equivalentes (por ejemplo, juegos, películas).

De hecho, siempre que sea posible conviene utilizar las clasificaciones de contenido utilizadas por otras industrias. Como ejemplo puede citarse el caso de las películas, los avances cinematográficos o los juegos de PC (siempre que las imágenes se repitan en la correspondiente versión móvil) a fin de que la percepción del cliente del mismo contenido sea idéntica en todos los medios nacionales.

No obstante, dados los problemas de orden práctico que encuentran los operadores móviles para determinar la edad del usuario, una serie de países (por ejemplo, Australia, Dinamarca, Nueva Zelandia) se han comprometido a establecer un sistema dual, simple, contenido apropiado sólo para adultos y contenido general/de otro tipo.

Por ejemplo, el código australiano divide los criterios y clasificaciones de la actual Junta de Clasificación en las categorías "restringido" (adultos mayores de 18 años) y "no restringido" (general) utilizadas para la telefonía móvil. Por otro lado, los operadores de EE.UU., bajo los auspicios de su asociación de comercio, CTIA, han creado una correspondencia entre las normas existentes para la televisión, las películas, la música y los juegos y las categorías "celular accesible" (general) y "celular restringido" (mayores de 18 años), cuyos resultados la CTIA resume de la siguiente manera:

Este método binario permite la venta de una amplia gama de contenido comercial legal por parte de los operadores móviles y terceros, al tiempo que se superan las pruebas nacionales de aceptabilidad. Se garantiza la gestión del contenido de mayor riesgo, además de que es en la mayoría de edad cuando resulta más práctico verificar la edad (por ejemplo, mediante la posesión de una tarjeta electoral o una tarjeta de crédito).

Otros países, sin embargo, optan por un método más detallado. Alemania ha adoptado un sistema que clasifica el contenido comercial en tres categorías y se basa ampliamente en el sistema de clasificación de películas, "FSK" de ese país:

- Servicio/contenido general: disponible para todos por defecto.
- Servicio/contenido para mayores de 16 años: disponible para todos por defecto. Los padres pueden optar por imponer un bloqueo.
- Servicio/contenido para mayores de 18 años: bloqueado para todos por defecto. Los adultos han de someterse a la verificación de edad.

Estudio de caso: Criterios de clasificación de contenido inalámbrico en EE.UU.

En Francia, en octubre de 2006 se anunció la imposición de un sistema de clasificación recomendado con cuatro categorías ("todos los usuarios", "mayores de 12 años", "mayores de 16 años" y "mayores de 18 años), creado en colaboración con numerosos interesados bajo los auspicios del Foro sobre los derechos de Internet. Los cuatro niveles diferentes facilitarán la resolución de problemas relativos a la gestión del acceso a los servicios interactivos y al contenido generado por los usuarios, gran parte del cual es aceptable para los adolescentes de más edad, pero no es "sólo para adultos" ni adecuado para los más jóvenes y los niños.

Para acceder al contenido para mayores de 18 años, los usuarios habrán de verificar su edad. Las categorías para mayores de 12 y 16 años corresponden a los dos siguientes niveles de control parental:

El contenido móvil puede clasificarse en contenido de operador restringido o contenido de operador generalmente accesible, en función de los criterios utilizados para clasificar películas, programas de TV, música y juegos.

El contenido se suele considerar "restringido" si contiene una o más de las siguientes características:

Contenido restringido por el proveedor:

- Insultos de carácter religioso.
- Violencia excesiva.
- Actividad o comportamiento sexual explícito: desnudez.
- Lenguaje ofensivo.
- Consumo ilegal de droga explícito.
- Otras actividades prohibidas por ley a los adultos mayores de 18 años, como juegos de azar y bingo.

El contenido no clasificado como "restringido" se considerará "generalmente accesible" y estará a disposición de todos los consumidores.

Pueden encontrarse más detalles sobre las Directrices de contenido inalámbrico en el sitio web de la CTIA: http://www.ctia.org/advocacy/index.cfm/AID/10394

- Control parental de primer nivel: bloquea el acceso al contenido comercial para mayores de 16 años, a servicios generados por usuarios/interactivos que facilitan encuentros (por ejemplo, sitios de citas) y a Internet.
- Control parental reforzado: bloquea el acceso al contenido para mayores de 12 y 16 años, todos los servicios generados por usuarios/interactivos y a Internet.

Los sistemas de clasificación del contenido están definidos por los operadores o por organizaciones terceras con la experiencia suficiente. En muchos países (incluidos Dinamarca, Malasia, Singapur y Nueva Zelandia, por ejemplo) simplemente se han definido los límites de la clasificación dentro del Código de Práctica nacional o como apéndice al mismo.

En otros países, incluido Francia, los criterios de clasificación han sido definidos por una organización independiente. El sistema dual de Reino Unido fue creado por el Órgano de Clasificación Móvil Independiente, creado por la industria (IMCB: http://www.imcb.org.uk/) en 2005. Además de formular los criterios de clasificación, el IMCB puede dar asesoramiento o ejercer de árbitro en caso de controversia (caso extremadamente raro) en materia de clasificación de un contenido particular.

Cabe señalar que no todos los sistemas de clasificación del contenido se basan en la edad: Malasia y Singapur utilizan un sistema binario basado en las normas nacionales en vigor, basado en contenido "aceptable" e "inaceptable" y no realiza distinciones en función de la edad.

La existencia de un sistema de clasificación de contenido común facilita la autoclasificación del contenido y, por tanto, reduce los costos y aumenta la eficacia de toda la industria, además de hacer que el sistema de clasificación sea más transparente para los clientes, en especial en el caso de servicios de terceros independientes del portal del operador (por ejemplo, en revistas) y permite la introducción coherente de herramientas como códigos cortos predeterminados para servicios SMS para adultos, lo que facilita la aplicación de controles de edad.

3. Mecanismos de control de contenido

Los proveedores de servicios y contenido en línea están elaborando una serie de métodos para permitir la aplicación de controles de edad al contenido en línea en todo el mundo. Entre ellos se incluyen mecanismos para restringir el acceso al contenido hasta que el usuario haya demostrado su edad ("verificación de edad"), así como controles disponibles para que los padres impongan restricciones al consumo que hacen sus hijos de contenido y servicios en línea.

Radiodifusores

Los radiodifusores ofrecen una serie de servicios y contenidos en línea, algunos de los cuales sólo son apropiados a partir de una determinada edad mínima. Para asegurarse de que los usuarios más jóvenes sólo acceden a los contenidos y servicios que les corresponden por edad, los radiodifusores emplean una serie de técnicas como:

- Procesos de inscripción única – Por ejemplo, en los servicios en línea de la BBC, cuando un niño se inscribe en el tablón de anuncios, ha de indicar su fecha de nacimiento. Esto se utiliza para determinar si tiene edad suficiente para acceder al servicio, y no pueden modificar su fecha de nacimiento más adelante, cuando descubren que no pueden acceder al contenido por motivos de edad.

Nota 1 – Los mecanismos para combatir la presencia de contenido ilegal en línea, en particular contenido pedófilo, se tratan detalladamente en la siguiente sección.

Nota 2 – En la sección 6 se presenta información más detallada sobre el contenido generado por los usuarios y los radiodifusores.

- Control parental por correo-e – Por ejemplo, la BBC está realizando una serie de pruebas para examinar la utilización del consentimiento parental por correo-e y un sistema de registro que permita a los padres decidir las actividades en que pueden participar sus hijos en los sitios web PSB, así como la información que desean recibir. La BBC está también estudiando las reglas que se aplicarían a los adolescentes de hasta 16 años, y si éstos deberían poder acceder a mayores niveles de interacción antes de necesitar el consentimiento paterno".

- Muchos radiodifusores del servicio público que, por el momento, están esperando una mejor reglamentación[4], han adoptado un método más drástico en la web que en sus emisiones de TV. La RAI italiana, por ejemplo, tiene una política restrictiva y no publica en sus sitios web contenido que no haya recibido la clasificación "apto para toda la familia" (marcado con una mariposa blanca). El contenido marcado con una mariposa amarilla (para adultos) o una mariposa roja (exclusivamente para adultos) no está disponible en Internet.

Proveedores de servicios Internet

Es importante que los proveedores de servicios Internet ofrezcan controles que impidan el acceso a determinados servicios o contenidos.

En muchos países, la legislación nacional especifica que determinados contenidos o servicios no han de ponerse a disposición de los niños (es decir, aquellos usuarios que no hayan llegado a la mayoría de edad/edad adulta). Cuando un PSI ofrezca tales servicios o contenidos de manera comercial, ha de emplearse un método de verificación de la edad. Por el contrario, cuando la ley no requiere tal control, se puede esperar razonablemente que no se permita a los niños acceder a los contenidos para adultos. Por ello, es posible que los PSI y otros interesados quieran considerar la posibilidad de crear o utilizar sistemas de verificación de la edad para garantizar el cumplimiento de la ley.

Los proveedores de servicios Internet han de tener en mente que la simple confirmación de edad, en la que con un clic un usuario declara ser mayor de 18 años, no es un método fiable, pues se basa exclusivamente en la integridad del usuario.

Sin embargo, también es importante recordar que incluso las soluciones para confirmar la edad de los usuarios, por ejemplo, solicitando datos de tarjetas de crédito o de identificación, no están totalmente garantizadas: un problema subyacente a todos los métodos es que la verificación de la identidad en Internet es difícil, porque es virtualmente imposible

[4] Conviene recordar que la BBC ha expresado su preocupación por la manera en que se ha de permitir a los usuarios activar un "botón rojo" si encuentran material dañino, explícito o preocupante. El principal problema es que, al disponer de demasiadas opciones, podría dirigir a los usuarios hacia otros sitios menos regulados y de peor reputación. Es fundamental que los radiodifusores mantengan su reputación de entorno seguro y, por tanto, garantizar que todas las alertas de seguridad están justificadas.


“La industria demuestra su compromiso para hallar la manera de que los niños puedan utilizar responsablemente las TIC y las comunicaciones en líneaions”

saber si el usuario está facilitando realmente la información que le pertenece. Aunque un usuario facilite determinada información al registrarse en un sitio web, no se garantiza que lo haya hecho honestamente. Por ejemplo, no se puede confiar en la utilización de tarjetas de identidad nacionales asociadas a un PIN para verificar la edad, pues se trata de información que generalmente conocen otras personas (por ejemplo, miembros de la familia).

Estos métodos también pueden infringir el derecho del usuario a la privacidad. Por ejemplo, las tarjetas de identidad contienen detalles personales (por ejemplo, la fecha de nacimiento), que van más allá de lo estrictamente necesario para confirmar que un usuario es mayor de edad.

Los PSI son cada vez más creativos para solucionar el problema del contenido no apto para todas las edades. Por ejemplo, MySpace exige en sus Términos y Condiciones que todos los usuarios sean mayores de 13 años. A fin de evitar que se dé el caso en que un usuario menor de 13 años mienta sobre su edad, emplea un algoritmo de búsqueda utilizando términos comúnmente utilizados por tales usuarios a fin de encontrar y eliminar sus perfiles. El sitio de MySpace se escanea en busca de tales términos y la base de datos de términos de búsqueda se actualiza para reflejar los cambios en el comportamiento y la terminología de los usuarios.

Muchos de los principales proveedores de acceso a Internet ofrecen ahora soluciones de control parental que ayudan a los padres a decidir a qué sitios, contenidos y servicios pueden acceder sus hijos.

Además, Telecom Italia, a fin de ajustarse a la muy restrictiva legislación italiana[7] en materia de protección de menores, y para garantizar que se da una respuesta global a la seguridad de las personas que utilizan sus servicios comerciales, ha lanzado un programa en colaboración con la policía italiana y con el Centro Nacional de lucha contra la pornografía infantil en línea (CNCPO)[8], que utiliza una infraestructura tecnológica muy especializada y un sistema de filtrado para bloquear los sitios indicados por el CNCPO.

Además, para impedir y prevenir la difusión de contenido pedófilo (pornografía infantil), y proteger a los niños, Telecom Italia ha establecido en su sitio web un mecanismo de información/ línea de ayuda para que los usuarios puedan dar cuenta

Estudio de caso: Telecom Italia y la protección de los niños – Italia

Para que los niños y adolescentes puedan navegar por Internet de manera segura, Telecom Italia ha tomado medidas para prohibir el contenido que pueda atentar contra su integridad psicofísica, como se describe en el portal del Grupo[5], y ofrece a sus clientes servicios e instrumentos de protección que garantizan la navegación segura[6].

Para los niños, la herramienta más importante es el **Escritorio Mágico de Alice**, que es un sistema operativo simplificado que funciona en los PC normales. El Escritorio Mágico de Alice permite a los niños utilizar los PC y las funcionalidades permitidas de Internet de manera segura, divertida y educativa, bajo el estrecho control de sus padres. Este servicio está destinado a los niños menores de 10 años.

Las principales características del producto son:

- **Protección del PC** contra una utilización indebida por parte de los niños (evita dañar los ficheros, configuraciones, software instalado por los padres, etc.).
- **Navegación por Internet segura**, basada en una lista blanca de sitios web preferidos establecida por los padres.
- **Cliente de correo-e**, específico para niños, con una interfaz de usuario gráfica especial y una lista de contactos predefinida por los padres.
- **Juegos y herramientas web** para niños, diseñados para jugar, aprender y utilizar una gran cantidad de material instructivo.
- Interfaz de **control parental global**, que permite a los padres controlar y definir el "jardín vallado" de los niños.

Los niños pueden utilizar este entorno seguro con facilidad, con diferentes temas de escritorio, un navegador Internet personalizado ("Mi primer navegador") con el que sólo pueden visitar los sitios "preferidos" aprobados por los padres; un programa de correo-e Mágico donde los correos recibidos desde direcciones desconocidas van a una carpeta de "cuarentena" para que los padres los verifiquen antes de comunicarlos al niño.

Source: Telecom Italia

de los contenidos ilícitos que encuentren navegando por Internet. Estos informes, que pueden ser anónimos y se realizan rellenando un formulario predefinido, se analizan y remiten inmediatamente a la policía postal (CNCPO), que investigará los supuestos delitos, pues las investigaciones son cometido exclusivo de las fuerzas del orden.

Aunque los métodos de control parental mejoran sin cesar, no se puede esperar que ofrezcan total seguridad. Sin embargo, si al mismo tiempo se enseña a los niños las prácticas responsables en Internet (véase Educación y comunicación con los usuarios a continuación), los controles parentales pueden lograr que los usuarios más jóvenes puedan interactuar en línea de manera segura.

[5] www.telecomitalia.com, Sustainability->Hot Topics-> Protection of Children and Abuse

[6] *Alice Total Security y Alice Magic Desktop*, http://adsl.alice.it/servizi/index.html *Guidelines for Industry.*

Operadores móviles

Los mecanismos de control del acceso a contenido restringido se pueden dividir en dos grandes categorías:

- Mecanismos de verificación de edad.
- Controles parentales.

Mecanismos de verificación de edad

Las herramientas de "verificación de edad" disponibles para los minoristas y radiodifusores tradicionales no se pueden utilizar directamente para el contenido móvil. Por ejemplo, con el contenido móvil no hay posibilidad de realizar una verificación visual en el "punto de venta", como se hace en los cines y tiendas; y, dada la naturaleza individual de los dispositivos móviles, los operadores móviles no pueden confiar en la supervisión parental, como sí pueden los radiodifusores de televisión tradicionales.

Sin embargo, una serie de operadores de todo el mundo está poniendo fin a este problema creando sistemas de verificación de edad. Hasta la fecha, éstos se centran en verificar la condición de adulto de los usuarios que desean tener acceso total a todos los contenidos y servicios. Cabe señalar que, cuando los operadores ofrecen servicios y contenidos comerciales sujetos a restricciones de edad impuestas por ley, dicha verificación reviste una especial importancia.

Cada operador tiene un método para verificar la edad, basado en las diferentes opciones existentes:

- Tarjetas nacionales de identificación.
- Tarjetas de crédito.
- Códigos fiscales.
- Tarjetas electorales.
- Verificación de identidad visual en tiendas o, por ejemplo, en la oficina postal.
- Contratos/pago de facturas.

Una vez constatada su condición de adultos, los usuarios reciben un "PIN adulto", necesario cada vez que se quiere acceder a contenido o servicios para adultos, o un "perfil adulto" adosado a su cuenta, de la que se eliminan las restricciones sobre servicios y contenidos.

Dada la dificultad que supone verificar la edad en el entorno virtual/en línea, los operadores permiten a los padres controlar el acceso de los usuarios más jóvenes a los servicios y contenidos mediante la aplicación de controles parentales, en lugar de intentar verificar la edad de todos y cada uno de los usuarios.

Controles parentales

Si los mecanismos de verificación de edad suponen que los operadores aplican proactivamente sistemas para asegurarse de que todos los usuarios tienen la edad mínima necesaria para acceder a determinados contenidos, los controles parentales se basan en

[7] Ley de Italia 38/2006, de lucha contra la explotación sexual de los menores y la pornografía infantil, incluso en Internet; Decreto Legislativo de Italia 70/2003, que regula el comercio electrónico y pide a los operadores de telecomunicaciones, como Telecom Italia, que informen a las autoridades competentes de los ciberdelitos perpetrados en la infraestructura de red y de todo abuso sexual de menores. Convenio sobre Ciberdelitos de la UE, firmado en el Consejo de Europa el 23 de noviembre de 2001, ratificado en Italia mediante la Ley 48/2008.

[8] http://www.poliziadistato.it/articolo/10232-Centro_nazionale_per_il_contrasto_alla_pedopornografia_sulla_rete

que los padres tomen la iniciativa y los apliquen como les parezca adecuado para sus hijos.

Muchos operadores de una serie de países ya han introducido sistemas de control parental, algunos de los cuales se basan simplemente en bloquear el acceso a contenidos comerciales inapropiados, mientras que otros se combinan con otras funcionalidades, como controles de tiempo y gastos.

Con algunas excepciones, incluidos los operadores franceses, que ya permiten dos niveles de acceso, y otros pocos operadores de todo el mundo que disponen de controles parentales en varios grados, la mayoría de estos sistemas sólo ofrecen las opciones "activado" o "no activado", que bloquean el acceso a unos determinados contenidos o servicios sensibles (por ejemplo, para mayores de 16 o 18 años) cuando están activados.

La mayoría de sistemas de este tipo se centran únicamente en los contenidos comerciales, aspecto sobre el que el operador tiene el mayor grado de control y, por ende, de responsabilidad. Los operadores de Japón utilizan las listas blancas/negras de sitios web cuando se aplican controles parentales y algunos operadores de otros mercados disponen de sistemas de filtrado, pero la mayoría aún está por incluir el filtrado en sus propuestas de control parental.

Como medida intermedia, una serie de operadores simplemente bloquean el acceso a Internet cuando los controles parentales están activados.

No obstante, es probable que la utilización de los móviles para acceder a servicios de Internet acelere la implantación de herramientas de filtrado.

Naturalmente, dada la responsabilidad que recae en padres y tutores para aplicar los controles, es fundamental dar a conocer y fomentar esta opción para que sea eficaz a la hora de proteger a los usuarios más jóvenes. Del mismo modo, los operadores han de asegurarse de que los padres entienden que sólo pueden controlar el contenido que se encuentra en sus redes.

Entre las demás opciones que se pueden considerar, se encuentra la de que los operadores móviles instalen controles parentales en los dispositivos de marca por defecto y, posiblemente, que los fabricantes de teléfonos móviles incluyan en ellos software que permita a los padres controlar y restringir los contactos entrantes y salientes de sus hijos.

Estudio de caso: ATT MEdia™ controles parentales netos – EE.UU.

La propuesta de control parental de AT&T se ofrece a los clientes gratuitamente y permite a los padres restringir el acceso de sus hijos a contenidos para adultos vía móvil, además de ofrecer la opción de restringir la compra de descargas de juegos y tonos.

Controlar el contenido: los padres pueden "activar" y "desactivar" los filtros de contenido. Cuando están activados, queda restringido el acceso a sitios de contenido adulto (por ejemplo, chat, citas) del portal AT&T's MEdia™ Net, y se anula el acceso a la web móvil mediante la función de búsqueda. Cuando están desactivados, no hay restricciones y se puede acceder y ver todo el contenido. La opción por defecto es "desactivado".

Controlar compras en MEdia™ Net: los padres pueden "activar" o "desactivar" el bloqueo de compras. Cuando está activado, los niños no pueden adquirir contenido, como tonos, descargas, juegos y gráficos. La opción "desactivado" permite todas las compras y es la opción por defecto.

Estudio de caso: Controles parentales de NTT DoCoMo – Japón

DoCoMo ofrece varios niveles de filtrado del contenido (por ejemplo, el filtrado i-mode 'Kids' y el filtrado i-mode) más una opción de "restricción de tiempo" que puede utilizarse por separado o en paralelo a otros niveles de filtrado. Las tres opciones ofrecidas son gratuitas:

1. Filtrado i-mode Kids: permite acceder a sitios sólo desde el menú i-mode (los proveedores de contenido del menú i-mode tienen prohibido por contrato ofrecer "contenido dañino", incluido el contenido sensible o para adultos, juegos de dinero, violencia, servicios de citas, chat y foros de debate); el " i-menú Kids"", que contiene sitios específicamente diseñados para niños, es la configuración por defecto.
2. Filtrado i-mode: permite el acceso a sitios del menú i-mode y a sitios independientes que no contengan contenido dañino.
3. Restricción de tiempo: impide el acceso a cualquier sitio (sea i-mode o independiente) entre las 22:00 horas y las 06:00 horas.

4.

Educación y comunicación con los usuarios

Para que los usuarios puedan tomar con conocimiento de causa decisiones sobre los servicios y contenidos que quieren utilizar, y permitir a los padres y educadores orientar a los niños y adolescentes hacia una experiencia segura, responsable y adecuada en línea, las empresas de telecomunicaciones y contenido están realizando cada vez mayores inversiones en programas de educación y comunicación.

En esta sección se presentan los métodos que pueden adoptar los proveedores de servicios y contenidos en línea.

Radiodifusores

Los radiodifusores que realizan programas populares entre niños y adolescentes probablemente tengan la misma audiencia "en línea", por lo que tienen una responsabilidad particular a la hora de fomentar que el entorno en línea sea seguro.

Los radiodifusores están también bien situados para explotar la popularidad de sus contenidos para transmitir mensajes simples que ayuden a los usuarios más jóvenes a luchar contra problemas como la "ciberintimidación" y la invasión de la privacidad.

Los radiodifusores pueden emplear otros métodos como fomentar que los niños pidan el consentimiento paterno antes de utilizar determinados servicios. Cuando, al crear una cuenta de usuario, se puede aconsejar al niño que pida el permiso de sus padres y que se asegure de que los padres saben que va a utilizar servicios como tablones de mensajes. En los Términos y Condiciones también se puede dejar claro que los niños deberán tener el permiso de sus padres o tutores antes de utilizar esos servicios.

Si un niño envía un mensaje que sugiere que sus padres no saben o no quieren que utilice servicios como las comunidades en línea de los radiodifusores, normalmente el webmaster indicará claramente al usuario que debe contar con el permiso de padres o tutores para utilizar el tablón.

Algunas organizaciones requieren que el consentimiento paterno se envíe por correo-e para mayor seguridad. Sin embargo, las pruebas realizadas por la BBC, por ejemplo, sugieren que muchos niños utilizan las direcciones de correo-e de sus padres, lo que menoscaba la eficacia del sistema, y que una parte de la audiencia de la BBC sólo accede a CBBC a través de los ordenadores del colegio, ya sea porque no les dan permiso en su casa o porque carecen de acceso a Internet.

Por consiguiente, los métodos de verificación por un clic o un correo-e no bastan para asegurarse de que hay realmente un padre/tutor/profesor al tanto de las actividades del niño y no es de gran ayuda para los niños que se encuentran en el peor lado de la brecha digital. Convendría que toda la industria participase en la búsqueda de sistemas de consentimiento parental aplicables a todas las sociedades y que no permitiesen el abuso.

Proveedores de servicios Internet

La industria de Internet tiene la responsabilidad de examinar la función e importancia de la comunicación con los clientes en términos de:

- **Claridad** sobre la naturaleza del contenido, los Términos y Condiciones y las Políticas de uso aceptable.
- **Conocimiento**, gracias a partes específicas de la web dedicadas a las amenazas de Internet y a las herramientas disponibles para la protección de los niños.
- **Colaboración**, mediante los formularios de información en línea.
- **Información** para padres y profesores sobre la seguridad de los niños.
- **Educación** de los niños para utilizar Internet de manera segura.

Estos puntos se desarrollan a continuación.

Claridad – *sobre la naturaleza del contenido, los Términos y Condiciones y las políticas de uso aceptable:*

Los PSI son cada vez más conscientes de la importancia de comunicar claramente la naturaleza de los contenidos y servicios, de manera que todos los usuarios, incluidos los más jóvenes, puedan tomar, con conocimiento de causa, decisiones sobre su consumo.

Claridad para la industria de Internet significa:

- Marcar el contenido no apto para todos los públicos.
- Comunicar el precio del contenido, las condiciones de abono, de cancelación de abonos, etc.
- Definición y comunicación de políticas de uso aceptable y de Términos y Condiciones.
- Definición y actualización de las políticas para ajustarse al código nacional pertinente relativo a la seguridad de niños y adolescentes en Internet.

Conocimiento – *gracias a partes específicas de la web dedicadas a las amenazas de Internet y a las herramientas disponibles para la protección de los niños:*

Los PSI pueden facilitar el conocimiento de la protección de los niños exponiendo clara y visiblemente la información sobre la utilización segura de Internet y sobre las herramientas para la protección de los niños de su sitio web. Tal parte del sitio estará destinada a:

- Fomentar el conocimiento y el debate sobre las amenazas de Internet y la protección de los niños, y sobre las herramientas a su disposición, como la configuración de bloqueo y privacidad.
- Intercambiar consejos de seguridad en línea para los usuarios.
- Contener recursos educativos.
- Describir las condiciones reglamentarias nacionales e internacionales.
- Dar a los clientes información sobre las herramientas de protección de los niños disponibles (control parental, etc.).

Los PSI también pueden aumentar el conocimiento de los clientes adoptando un código de autorregulación que permita la protección de los menores mediante la aplicación de normas y herramientas específicas al tiempo que se utiliza una marca visible que certifique la adhesión a dicho código.

Colaboración – *mediante formularios de información en línea:*

Para luchar y prevenir los contenidos pedófilos y proteger a los niños, los PSI deberían:

- Reservar espacio en la web para dar cuenta de los contenidos ilegales que encuentran los usuarios al navegar por Internet. Tales informes deberán realizarse anónimamente rellenando un formulario predefinido.
- Dar a los clientes detalles de cómo realizar un informe de seguridad.
- Contactar inmediatamente a las fuerzas del orden pertinentes, que investigarán los supuestos delitos. Los servicios de atención al cliente de los PSI deberán poder tramitar y remitir los informes de los clientes a las autoridades pertinentes.

Información *para padres y profesores:*

Los proveedores de servicio se están dando cuenta de lo importante que es dar a padres y profesores la información necesaria para entender cómo los niños utilizan los servicios de TIC (por ejemplo, también problemas como el acoso) y estar preparados para orientarlos hacia una utilización responsable.

- Los padres y profesores han de conocer todos los riesgos que supone Internet para poder proteger mejor a los niños. Los mensajes han de ser positivos y permitir a los padres tomar medidas.
- Esta información se transmitirá por múltiples medios, pues muchos padres no utilizan servicios Internet, por ejemplo colaborando con los colegios para dar material educativo e informativo a padres y niños. Siempre que sea posible, los PSI fomentarán la existencia de servicios nacionales de apoyo donde los padres y tutores puedan informar de casos de abuso y explotación y recibir apoyo.

Los padres y profesores deben:

- Informarse sobre Internet y la manera en que lo utilizan los niños, y sobre la tecnología en general.
- Estudiar y evaluar la eficacia de las herramientas tecnológicas disponibles para sus hijos y su contexto familiar, y adoptar las que sean más convenientes.
- Participar e interesarse por la utilización que hacen sus hijos de Internet.
- Ser consciente de los riesgos a que se enfrentan los jóvenes para ayudar a sus hijos a comprender y utilizar las tecnologías.
- Estar atentos a los niños en situación de riesgo en su comunidad y al grupo de amigos de sus hijos.
- Reconocer cuándo han de solicitar ayuda externa.

Educación *de los niños sobre la utilización segura de Internet:*

Para los "navegantes principiantes", el mundo virtual es un recurso útil y divertido, pero también un lugar desde el que pueden acceder a material no adecuado para ellos.

La utilización que los niños hacen de Internet varía con la edad y el nivel de desarrollo. Solos, los más jóvenes no pueden entender las ventajas y peligros que supone navegar por la web, por lo que es preferible que lo hagan acompañados en todo momento de un adulto (padre y/o profesor) que pueda ayudarlos y orientarlos en su elección de contenido, así como a imponer las reglas

de comportamiento adecuadas que habrán de seguir.

Para los adolescentes, no obstante, la tarea es más difícil. Son más independientes y están más informados de las oportunidades que ofrece la web, a menudo mucho más que sus padres y profesores en lo que respecta a Internet, la mensajería instantánea, los chats, los juegos en línea, etc. Sin embargo, conviene que los padres establezcan una reglas y les enseñen a estar alerta, ser educados y responsables al navegar.

También es muy importante que los PSI faciliten directamente a los niños información sobre la utilización segura de Internet. Los niños han de estar educados para poder detectar y reaccionar ante comportamientos inapropiados. A continuación se presenta una lista de consejos para que los PSI den esta información a los más jóvenes usuarios:

- "Nunca facilitar datos personales".
- "Nunca aceptar encuentros con personas que sólo se conocen en línea, especialmente sin consultarlo antes con un adulto".
- "No responder a mensajes inapropiados (acoso, obscenos o insultantes) y guardar las pruebas, no eliminarlas".
- "Decir a un adulto cuando algo o alguien te haga sentir triste o incómodo".
- "Nunca dar tu nombre de usuario o contraseña y tener en cuenta que otros pueden dar información falsa sobre su vida real".

Siempre que sea posible, los PSI han de fomentar la existencia de servicios de ayuda nacionales donde los niños puedan dar estas informaciones y buscar ayuda en caso de abuso o explotación.

Utilizar los Términos y Condiciones

Es muy importante que los PSI y la industria de Internet en general pongan de manifiesto los "Términos y Condiciones" de sus servicios Internet, con una política clara en cuanto a las infracciones de los mismos. Por ejemplo, en los Términos y Condiciones típicos se insiste en que los usuarios no han de utilizar el sitio web o el servicio para:

- Telecargar, colgar, transmitir, compartir, almacenar o poner a disposición contenido que pueda ser dañino, ilegal, difamatorio, delictivo, abusivo, vulgar, obsceno, contrario a la privacidad o los derechos públicos, violentos o racistas.
- Hacerse pasar por otra persona o entidad, dar información falsa sobre la edad o relación con otra persona o entidad.
- Telecargar, colgar, transmitir, compartir, almacenar, poner a disposición en los sitios web información privada de un tercero, incluida la dirección, número de teléfono, dirección de correo-e, número de tarjeta de crédito.
- Solicitar información personal de los menores de 18 años, incluidos, aunque no únicamente, el nombre, la dirección de correo-e, la dirección postal, el número de teléfono o el nombre de su colegio.
- Telecargar, transmitir, compartir material portador de virus.
- Telecargar, colgar, transmitir, compartir o poner a disposición contenido que pueda constituir un delito, de pie a una instrucción criminal, violar los derechos de otra persona física o violar las leyes locales, estatales, nacionales o internacionales.
- Dañar o explotar en modo alguno a los niños.
- Acosar, difamar, defraudar, intimidar, degradar a una persona o grupo de personas por cualquier motivo, incluida su edad, sexo, discapacidad, etnia, raza, religión u orientación sexual.

Los Términos y Condiciones han de ir acompañados por una clara declaración de la política de la empresa con respecto a las infracciones, con mensajes como:

- [La empresa X] ha adoptado una política de anulación de las cuentas de los clientes que cometan repetidas infracciones. Se reserva el derecho de examinar y anular servicios y contenidos creados por los usuarios a discreción y sin previa notificación y de eliminar los contenidos y cuentas.
- [La empresa X] podrá también, con total discreción, limitar el acceso a los sitios o anular la condición de miembro de los usuarios que infrinjan las normas.

Los PSI deberán repetir los mensajes de sus Términos y Condiciones con un lenguaje claro en sus directrices y "recordatorios" dentro del servicio, por ejemplo, recordando a los usuarios los tipos de contenido que se consideran inadecuados en el momento en que vayan a telecargarlos.

Operadores móviles

La educación y comunicación con los usuarios tienen un papel fundamental a la hora de garantizar que los niños y jóvenes pueden tener una segura y adecuada experiencia móvil.

Estudio de caso: Código de conducta sobre los SMS con recargo de la Asociación de Proveedores de Servicio de Aplicaciones Inalámbricas (WASPA) – Sudáfrica

El Código de la WASPA contiene una serie de compromisos específicos para la clara comunicación con los clientes, ejemplos de los cuales son:

- **El material promocional para todos los servicios de abono ha de identificarse clara y explícitamente como "servicios de abono".**
- **Una vez abonado el cliente al servicio, se le ha de enviar un mensaje con la siguiente información:**

a) El costo del servicio de abono y la frecuencia de facturación.

b) Instrucciones claras y concisas para anular el abono.

c) La información de contacto del miembro.

- **Se ha de enviar a los clientes abonados un recordatorio mensual con la información indicada en a, b y c *supra*.**

Los operadores son cada vez más conscientes de la importancia de comunicar claramente la naturaleza de los contenidos y servicios que ofrecen, de manera que todos los usuarios, incluidos los más jóvenes, puedan tomar con conocimiento de causa decisiones sobre su consumo, lo que incluye marcar los contenidos no aptos para todos los públicos, pero también indicar claramente el precio del contenido, los términos de abono y cancelación de abonos, etc., especialmente porque la falta de claridad absoluta a este respecto puede hacer que los usuarios más jóvenes se inscriban involuntariamente a un servicio, por ejemplo, cuando lo que realmente querían era adquirir un único tono.

Como ocurre en otros medios, los operadores móviles no pueden asumir la entera responsabilidad de garantizar que los niños y adolescentes utilizan los dispositivos móviles adecuadamente. También los padres, tutores y profesores tienen una función que desempeñar. El problema es que suele pasar que los padres conocen menos las capacidades de los nuevos dispositivos móviles que los niños mismos, por lo que es fundamental educarlos en este sentido.

Para ello, una serie de operadores está invirtiendo en programas de educación y directrices dirigidas a los padres y que abordan toda una serie de temas pertinentes como:

- Contenidos y servicios: se explica a los padres los tipos de servicios disponibles en la actualidad (por ejemplo, explicar qué son las redes sociales, los servicios basados en la ubicación y cómo se puede acceder a Internet vía móvil) y, cuando proceda, las opciones disponibles para aplicar controles;

Estudio de caso: "Pistas para padres" de Vodafone – Reino Unido

- Contactos inapropiados: cómo evitar el "peligro de extraños", qué hacer si su hijo se ve sometido a "ciberintimidación" por Internet o SMS.
- Medidas que hay que tomar si le roban el teléfono o el niño recibe spam.
- Gestión de la privacidad – no compartir información en línea, mantener privados los perfiles en SNS, etc.

Al educar a los padres, los operadores les dan la capacidad de orientar a los niños hacia una utilización responsable de los servicios móviles. Algunos operadores se han asociado con otros participantes en el mercado para elaborar y fomentar guías para padres (por ejemplo, Francia[9], Irlanda[10]), mientras que otros elaboran sus pro-

Como parte de sus iniciativas educativas sobre la seguridad de los niños, Vodafone ha creado una guía de bolsillo con "pistas" para padres. En esta guía se dan recomendaciones sobre determinados temas, como los chats, los juegos, los servicios con recargo y el acoso.

Las siguientes "pistas" se refieren a la descarga de contenido en móviles:

- **Hablar con los niños sobre los servicios que utilizan en sus móviles, por ejemplo, descarga de tonos, fondos de pantalla o juegos directamente desde el móvil.**
- **Averiguar si quieren compartir el contenido descargado con amigos.**
- **Hablar sobre los tipos de contenido que no quiere que se descargue, reciba o comparta con otros.**
- **Subrayar la importancia de no contestar a mensajes de extraños, o mensajes raros, o que ofrecen productos a bajo precio. Se trata siempre de "demasiado bueno para ser cierto'.**
- **Asegurarse de los niños no pueden acceder a la barra de control parental de ningún teléfono.**
- **Se puede recuperar la barra de control de contenido llamando al servicio de atención al cliente de Vodafone al número 191, visitando una tienda de Vodafone o en línea en la dirección www.vodafone.co.uk**

Es posible descargar las pistas de la "Staying in Touch: A Parent's Guide to Mobile Phones" desde la dirección: http://online.vodafone.co.uk/dispatch/Portal/SimpleGetFileServlet?dDocName=VD007645&revisionSelectionMethod=latestReleased&inline=0

[9] http://www.sfr.fr/media/pdf/offre-sfr/maj-240107/att00013578/701.09Guideparents2007.pdf
[10] http://www.vodafone.ie/download?id=ICIA_PARENTS_GUIDE.PDF

pias guías destinadas específicamente a sus clientes.

Del mismo modo, es fundamental saber que existen herramientas de control parental, en especial en los mercados donde no se aplican por defecto. Sabiendo esto, los operadores cada vez dan más a conocer las opciones de control parental en los sitios web, las tiendas y en las facturas; y se ofrecen estos controles en los puntos de venta como parte del proceso de venta.

Los operadores también se dirigen directamente a los más jóvenes mediante programas educativos y asociaciones con ONG en sus mercados locales, así como indirectamente, dando a los profesores los recursos para educar e informar a los alumnos sobre la utilización apropiada –véase, por ejemplo, el sitio web Teach Today (www.teachtoday.eu), creado por un consorcio de proveedores Internet de Europa.

A medida que mejoran los servicios y el contenido, los usuarios seguirán recibiendo consejos y recordatorios sobre la naturaleza del servicio que están utilizando y sobre cómo hacerlo de manera segura. Por ejemplo, muchos operadores incorporan directrices comunitarias en sus servicios interactivos (por ejemplo, salas de chat), que recuerdan a los usuarios que no deben comunicar sus datos, etc. (véanse más ejemplos en el apartado "Educar a los niños" de la sección para Proveedores de Internet). Del mismo modo, como práctica idónea, muchos operadores envían regularmente recordatorios a los usuarios de servicios basados en la ubicación, que indican dónde se encuentran, haciéndoles saber que el servicio está activado y recordándoles cómo pueden modificar su perfil o desactivar el servicio.

Estudio de caso: Conocimiento de los medios CBBC – Reino Unido

CBBC (BBC de los niños) tiene una sección formativa llamada *Stay Safe*, presentada por un conejo de dibujo animado llamado Dongle. Los estudios demuestran que los niños de primaria responden bien al personaje. Esta sección contiene un cuestionario interactivo, un "vídeo pop" y enlaces a otros recursos como "thinkuknow" (crees que sabes). Se aborda la seguridad móvil y en línea y todo el contenido se organiza alrededor de las reglas de seguridad "smart" (listo):

S = Mantente seguro.
M = No te reúnas.
A = Aceptar correos-e puede ser peligroso.
R = ¿Fiable? Las personas pueden no ser quien dicen.
T = Habla con un adulto si te sientes asustado o incómodo.

La sección *Stay Safe* está vinculada a todas las páginas de la comunidad y los anfitriones refuerzan el mensaje al insistir en lo que se considera un comportamiento aceptable, pero es importante señalar que, aunque las reglas SMART son utilizadas y apreciadas, existen varias versiones diferentes, lo que puede confundir a los niños.

Estudio de caso: Érase una vez el ciberespacio, MDA y Okto – Singapur

La Autoridad de Desarrollo de los Medios de Singapur (http://www.mda.gov.sg/) ha fomentado la creación de una serie de animación de seis capítulos que emite el canal *MediaCorp's Okto* a lo largo de seis semanas, destinada a dar a conocer los beneficios de Internet y los nuevos medios, al tiempo que se insiste en la necesidad de tener precaución en línea. Esta iniciativa va en el sentido del movimiento de educación pública sobre ciberbienestar y ciberseguridad del gobierno.

Los dibujos se dirigen a los niños entre 10 y 14 años con personajes de cuentos conocidos, pero con decorados actuales y guiones que tratan de Internet y los nuevos medios.

Por ejemplo, en el primer episodio, Caperucita Roja y la mensajería instantánea, Caperucita Roja encuentra un mensaje de una niña desconocida que vive en otra parte del bosque. Caperucita empieza a chatear con la niña y acaba diciéndole que va a visitar a su abuelita, e incluso le da la dirección de la abuelita. Al final se descubre que la "niña" es en realidad el Lobo Feroz disfrazado.

Pueden encontrarse resúmenes de los otros cinco episodios – Blancanieves y los juegos en línea, Pinocho tiene una cita a ciegas, Los tres cerditos y el ataque del virus de Internet, la Bella durmiente y su teléfono móvil, y El Ogro matón– en el sitio web de MDA: http://www.mda.gov.sg/wms. file/mobj/mobj.1334.Annex.pdf

Estudio de caso: Comunicación con los clientes para luchar contra el spam y los SMS fraudulentos

Los clientes, incluidos los niños y jóvenes adolescentes, pueden recibir dos tipos de SMS posiblemente fraudulentos que, con la información correcta, son fáciles de contrarrestar.

Se pueden utilizar los SMS para enviar un mensaje que invita a devolver una llamada o un mensaje a un servicio con recargo. El mensaje típico es del tipo: "Enhorabuena. Ha Ganado usted un premio. Llame al XXX XXX XXX [número con recargo] para obtener más detalles". Este tipo de timo o "microfraude" quiere obtener dinero de la cuenta o tarjeta de prepago del usuario del teléfono.

En una variante de peska, también es posible que se intente robar la identidad del usuario a través de su móvil. Por ejemplo, un usuario puede recibir un mensaje de texto o voz de su inspector fiscal indicándole que tiene un pago pendiente y, cuando el cliente devuelve la llamada, le inducen a desvelar todos sus datos bancarios.

Para casos como éste, los operadores han de lanzar campañas educativas para que los clientes sepan reconocer tales timos y no se dejen engañar (por ejemplo, conociendo los números nacionales con recargo y que no deben llamar a números así en respuesta a un mensaje desconocido). Siempre que sea posible, los operadores han de facilitar información actualizada sobre los timos corrientes, como, por ejemplo, *SCAMwatch* (http://www.scamwatch.gov.au/), de la Comisión de Consumo y Competencia de Australia, que quiere "ayudar a reconocer los timos, dar medios de información y protección contra los mismos", y tiene una sección específicamente dedicada a "timos por teléfono móvil".

La otra forma de abuso más importante son los SMS con recargo utilizados para ofrecer servicios de abono. Los servicios de abono son legítimos cuando ofrecen transacciones repetidas, como la compra del mismo servicio de información cada semana. Los SMS de abono son un abuso cuando un proveedor de servicios de información da al cliente la impresión de que sólo se le cobrará una vez, pero en realidad se hará periódicamente.

Un ejemplo de ello puede ser un anuncio en una revista, donde se da la impresión de que sólo se hará un único pago, pero en realidad se trata de un abono al servicio. Los clientes han de poder cancelar los pagos ulteriores al servicio.

Cuando los clientes se encuentren con un timo de SMS, tienen que poder presentar una queja a su operador de red y/o al regulador de comunicaciones nacionales o con recargo, por ejemplo, reenviando el SMS a un número móvil específico. Las repetidas quejas contribuirán a identificar a los proveedores deshonestos y a tomar las medidas necesarias, hacienda, en último término, que tales prácticas no resulten rentables.

Al indicar estos tipos de mensajes a sus clientes, los operadores pueden ayudarles a protegerse del spam y de los timos por SMS:

- No contestar a invitaciones de llamada a números con recargo – las personas que envían SMS para que los llamen utilizan números normales. Incluso si no se reconoce el número móvil llamante, se pueden evitar los timos identificando y recordando los números con recargo en su país (suelen empezar por 09).
- Los organizadores de concursos no envían notificaciones aleatoriamente – si no reconoce el concurso de que se trata, probablemente es un timo.
- Si compra un tono u otro servicio y ve que le envían tonos repetidamente, probablemente haya caído en un timo de SMS de abono. Cancele los pagos ulteriores (a partir del anuncio original) y presente una queja a su operador y al regulador nacional pertinente.
- Del mismo modo, cuando el operador disponga de otros mecanismos para dar cuenta del spam, habrán de comunicarse a los clientes. Los operadores móviles franceses, por ejemplo, utilizan un código corto SMS para que los clientes puedan informar del spam por SMS, que tiene su propia página web: http://www.33700-spam-sms.fr/

5. Contenido ilegal

Teniendo en mente las mismas prioridades, los operadores móviles de más de 70 países, que representan a más de 900 millones de usuarios, que se han adherido al Código de Práctica de la GSMA, se comprometen todos a garantizar "que sus procesos para obtener el consentimiento [para recibir un mensaje publicitario] son claros y transparentes" y a dar a sus clientes "medios evidentes, claros y eficaces para rechazar la recepción de comunicaciones publicitarias de los operadores por SMS o MMS".

La comunicación es, evidentemente, un proceso bidireccional, y muchos operadores dan a sus clientes la opción de contactarlos para comunicarles problemas, estén relacionados con el descubrimiento de contenidos o contactos inapropiados en un servicio móvil, con el robo del teléfono, la recepción de spam o para solicitar la aplicación/eliminación de controles parentales, con personal formado para responder eficazmente.

Como se verá más adelante, la correcta tramitación de los informes de clientes sobre contenidos posiblemente ilegales es un factor fundamental en la lucha contra la presencia de contenido ilegal, incluida la pedofilia, en el entorno móvil.

Todos los proveedores Internet (tanto fijos como móviles) han de trabajar con las fuerzas del orden para cumplir con sus obligaciones legales con respecto al contenido ilegal. No obstante, muchos proveedores de servicios Internet utilizan otros métodos para luchar contra la utilización impropia de sus servicios para almacenar o distribuir contenidos ilegales, incluida la pedofilia (pornografía infantil). Entre estas medidas las mas comunes son:

- Términos y Condiciones y "directrices de usuario", donde se prohíben explícitamente las actividades ilegales.
- Procesos de notificación y bloqueo (NTD) o "cesar y anular".
- Colaboración con líneas de ayuda nacionales.

Términos y Condiciones, directrices de usuario

Los proveedores Internet que ofrecen servicios interactivos que permiten a los usuarios almacenar y compartir contenido (por ejemplo, álbumes de fotos, redes sociales) pueden utilizar los Términos y Condiciones de los contratos con sus clientes para dejar clara su postura sobre la utilización impropia de sus servicios para almacenar o distribuir contenido ilegal, a fin de subrayar su compromiso con las fuerzas del orden y reservarse todos los derechos, incluido el de eliminar los contenidos ilegales y congelar las cuentas de los usuarios.

Muchos proveedores Internet también insisten en sus Términos y Condiciones con un lenguaje fácilmente comprensible, dentro de unas "directrices de usuario" donde se señala el comportamiento que se espera que sus usuarios tengan en el servicio. Normalmente, se puede acceder a estas directrices directamente desde el servicio en cuestión o en el momento de crear una cuenta.

Los proveedores de servicios también pueden evaluar activamente el contenido comercial incluido en sus servicios (ya sea propio o contratado por terceros) de manera periódica para garantizar que no se puede acceder a través de su red a contenidos ilegales o potencialmente dañinos.

Procesos de señalar y tomar nota

Sea voluntaria u obligatoriamente, los procesos de "notificación y bloqueo" (NTD) o de "cesar y anular" son fundamentales para que los proveedores de servicios y los operadores mantengan sus servicios libres de contenidos ilegales: en cuanto los proveedores reciben la alerta de que sus servicios se utilizan para almacenar contenidos ilegales, toman las medidas necesarias para eliminarlo.

Para que el NTD funcione adecuadamente, debe estar legalmente muy clara la naturaleza del contenido que se considera ilegal, y las fuerzas del orden (u organizaciones delegadas) han de poder confirmar la ilegalidad de los contenidos.

Los operadores y proveedores de servicio pueden disponer o utilizar Oficinas de Abusos de Internet, líneas de ayuda o sitios web especializados para gestionar, reducir o eliminar los ciberdelitos o el material ilegal presente en sus sitios web o infraestructuras. Así, los clientes, el público en general, las fuerzas del orden o las líneas

Estudio de caso: Servicio de atención ante abusos y método de señalar y anotar – Telecom Italia

De conformidad con las leyes nacionales y europeas aplicables en materia de protección de la infancia, prevención de ciberdelitos y lucha contra los contenidos pedófilos (pornografía infantil), Telecom Italia ha creado centros operativos para tratar los abusos, conocidos como Oficinas de Abusos (especializadas para cada tipo de cliente, particular, empresa o privilegiado). Estos centros son la interfaz entre los usuarios de los servicios (en general de Internet) y la empresa para la gestión de abusos y utilización indebida de los servicios.

Gracias al trabajo especializado de los operadores de la Oficina de Abusos, Telecom Italia puede gestionar distintos tipos de ciberdelitos y dar cuenta de todos los hechos pertinentes o significativos a las autoridades locales, como la presencia de contenidos pedófilos en las redes o sitios del Grupo.

Se utilizan dos importantes programas de prevención: primero, el mecanismo NTD (notificación y bloqueo), donde los usuarios o la policía notifica a la Oficina de abusos que se han de eliminar contenidos o sitios ilegales; segundo, un sistema de filtrado web, que utilizan todas las redes de Telecom Italia, basado en el filtrado DNS e IP, capaz de denegar el acceso a determinados sitios o direcciones IP. En Italia las listas DNS o IP que se han de bloquear proceden del CNCPO (Centro Nacional de lucha contra la Pornografía Infantil en línea). Estas listas se descargan automáticamente todos los días.

Líneas de ayuda

Hacia 1995, a medida que Internet ganaba popularidad, la industria, así como los gobiernos y fuerzas del orden, se dieron cuenta de que Internet se estaba utilizando para publicar e intercambiar contenido ilegal, en particular, contenido pedófilo. Se debatieron diversos medios para luchar contra este problema, incluida la creación de líneas de ayuda para que los particulares pudieran denunciar la existencia de contenidos ilegales en línea.

La primera línea de ayuda para denunciar contenidos pedófilos se creó en los Países Bajos en junio de 1996, gracias a una iniciativa conjunta de la industria, el gobierno y las fuerzas del orden. A esta siguieron iniciativas similares en Noruega, Bélgica y Reino Unido.

Desde entonces, muchos países han creado líneas de ayuda y la INHOPE (Asociación Internacional de Líneas de Ayuda Internet), organización general de líneas de ayuda, cuenta ahora con unos 30 miembros en todo el mundo.

Además de los métodos NTD para gestionar el contenido ilegal presente en los propios servicios de los operadores, el respaldo y fomento de las líneas de ayuda da a los clientes y al público en general un medio de dar cuenta del contenido ilegal de ayuda pueden notificarles la presencia de contenido ilegal (ver *infra*). Si los informes proceden del público (por ejemplo, a través de la atención al cliente), los operadores/PSI transmiten la información a las fuerzas del orden o líneas de ayuda nacionales, según proceda, para, por ejemplo, confirmar que el contenido es ilegal o adoptar las medidas jurídicas del caso.

que encuentren, por lo que es una importante medida en la lucha contra contenidos ilegales, incluidos los pedófilos.

Colaboración en la industria

Hay también una serie de iniciativas de colaboración de la industria, como la Coalición Tecnológica, la Coalición Financiera contra la Pornografía Infantil y la Alianza Móvil contra los Contenidos Pedófilos, en curso. Estas iniciativas reúnen a los principales representantes de cada industria para que compartan conocimientos y encuentren nuevos medios técnicos para luchar contra la presencia de contenido pedófilo en toda la industria, incluso, por ejemplo, bloqueando el acceso a URL que se sabe exponen tal contenido.

6. Otros asuntos

Contenido generado por los usuarios: los radiodifusores

En esta sección se abordan los métodos que pueden adoptar los radiodifusores con respecto al contenido generado por los usuarios en sus servicios.

Para garantizar que no se publica contenido inapropiado en los tablones de mensajes, se recomienda que los radiodifusores utilicen una serie de procedimientos para proteger a los usuarios en línea contra el contenido generado por los usuarios inadecuado. Éstos son:

a) Filtros automáticos – es posible bloquear palabras inadecuadas de nombres de usuarios y mensajes en el momento de su publicación. Este filtro comprende insultos, términos sexuales y racistas o lenguaje homófobo. También se pueden bloquear URL ajenas y direcciones de correo-e.

b) Moderación previa – por ejemplo, es posible moderar todos los tablones de mensajes gracias a un equipo de moderadores especializados en niños, que examinan el contenido que va en contra de las normas de publicación de la casa. Se verifican todos los mensajes antes de su publicación y los moderadores también pueden aislar y marcar a los usuarios sospechosos, así como a los que se encuentran en peligro.

c) Anfitriones – además de los moderadores, puede haber anfitriones comunitarios que gestionan los tablones de mensajes desde el punto de vista del público y son el primer punto de contacto con los moderadores cuando hay problemas con un usuario.

Todo tipo de moderación habrá de ser realizada por un equipo interno, al que se someterá a una verificación detallada para comprobar que carecen de antecedentes penales. Esta verificación dependerá de un único organismo. Además, los equipos de moderación pueden aplicar las siguientes reglas:

- No se permitirá el teletrabajo para garantizar que nadie tiene acceso a la información de los niños.
- La moderación se hará en equipo, de manera que todos conozcan los problemas relativos a puestos o usuarios y conozcan su comportamiento en grupo.
- La moderación seguirá unas estrictas directrices, que se elaborarán con el tiempo.
- Los moderadores tendrán un horario definido, que será el de funcionamiento de los tablones de mensajes. Así, se garantiza que siempre habrá un moderador en activo mientras funciona el tablón.

No obstante, se trata de un proceso muy laborioso y, cuanto más éxito y popularidad tiene una comunidad, más recursos se necesitan para moderarla.

La mayor sanción consiste en bloquear a los usuarios que repetidamente infringen las reglas de la casa. Sin embargo, en el futuro es posible que los radiodifusores quieran adoptar un sistema basado en la "confianza y reputación" para fomentar el buen comportamiento y que los usuarios se enseñen las prácticas idóneas mutuamente con el ejemplo.

Los pilares de la comunidad recibirán una recompensa por su buen comportamiento y a los miembros problemáticos se les retirarán los privilegios. Todo el contenido generado por los usuarios habrá de someterse a moderación antes de su difusión.

Las sesiones de chat premoderadas exclusivas con, por ejemplo, los autores y presentadores favoritos de los niños, son un incentivo que ya se utiliza para que un grupo de edad determinado participe en las comunidades en línea de los radiodifusores. Estos eventos exclusivos y otros contenidos con recargo desalientan a los usuarios a mentir sobre su edad e inscribirse a servicios destinados a usuarios de más edad.

Con cada vez más frecuencia, los servicios en línea de los radiodifusores alientan a los usuarios a enviar fotos, vídeos y textos. Estos servicios habrán de verificarse previamente para garantizar que el material es adecuado para su publicación en los sitios web de los radiodifusores y que los niños no dan a conocer información personal suya o de otros, por ejemplo, nombres de escuelas, calles, números de portal, que podrían suponer un peligro, por ejemplo, 'jigsaw id' (llegar a conocer una identidad a partir de datos sueltos).

En particular, cuando los niños presentan vídeos, los radiodifusores habrán de exigir el número de teléfono del padre o tutor para obtener su consentimiento antes de la publicación (de conformidad con las políticas de televisión y protección de los niños contra, por ejemplo, su localización por padres que han perdido su custodia).

Estudio de caso: Cómo pueden los radiodifusores proteger a los niños contra el material inapropiado externo: el ejemplo de la BBC

Todos los contenidos externos vinculados a Cbeebies y CBBC son aprobados previamente por un experto editorial y se ponen en la lista "verde", donde se pueden realizar búsquedas desde el servicio de búsqueda de la BBC.

Cbeebies busca específicamente el contenido del sitio Cbeebies y aprueba los sitios subsidiarios creados por productores independientes para su propia programación Cbeebies.

La herramienta de búsqueda de CBBC es más compleja para que los usuarios puedan encontrar el mejor contenido de CBBC y *Newsround*, y además se seleccionan cuidadosamente sitios de toda la BBC y toda la web. Todos los sitios han de tener valor editorial e interés para los niños entre 7 y 12 años de Reino Unido y no deben:

- **Contener, vincular o anunciar material pornográfico o sexualmente explícito (a menos que forme parte de programas de educación sexual para este grupo de edad).**
- **Contener, vincular o anunciar contenido de violencia explícita o comportamiento que incite a la violencia (incluidos juegos y análisis de juegos con luchas, armas de fuego o de otro tipo).**
- **Incitar a cometer actos ilegales**
- **Incluir discriminación de ningún tipo.**
- **Fomentar hábitos malos para la salud/la alimentación.**
- **Utilizar lenguaje inapropiado.**
- **Existir únicamente para vender productos o servicios**
- **Fomentar los juegos de dinero.**
- **Restringir sus servicios a los abonados**

La BBC no permite vínculos a redes sociales en el sitio CBBC. Si alguno de los sitios externos incluye tablones, han de estar sometidos a moderación previa en todo momento. No es posible vincular salas de chat en directo a los sitios para niños de la BBC.

La base de datos de búsqueda de CBBC se verifica constantemente con una herramienta automática que "barre" todos los sitios de la base de datos buscando cambios, de acuerdo con palabras clave como "tablón" o "chat". Si se detectan cambios se remite el sitio a un investigador que vuelve a comprobar su adecuación y lo elimina de la base de datos, de ser necesario.

Del mismo modo, *PSB Switch* aplica una política rigurosa de protección de los usuarios frente a contenidos inapropiados en línea. Si bien la presencia de *Switch's* en el sitio de un tercero es parte fundamental de la oferta a adolescentes, permitiéndole llegar a un público que no siempre está familiarizado con la oferta PSB, todos los sitios en este espacio están moderados y cuidadosamente controlados. La BBC incluye enlaces evidentes a información sobre seguridad en línea, siempre que es posible, y nunca vincula *Switch* a salas de chat en directo.

7. Conclusiones

Para que los PSI y otros proveedores en línea participen efectivamente en la Iniciativa de Protección de la Infancia en Línea, es fundamental que entiendan claramente cómo se clasifican los servicios y contenidos dentro del marco jurídico que les corresponde.

La colaboración con los radiodifusores locales debería ser muy útil para llegar a tal comprensión. También es importante entender cómo la legislación local percibe la "ubicación" del contenido y determina el "lugar" en que el servicio se entrega o recibe.

Todos los países tienen la responsabilidad de crear sus propias leyes aplicables al contenido y los servicios Internet dentro de su jurisdicción.

Por desgracia, tal y como han demostrado varios estudios, los países carecen de legislación adecuada o suficiente para solucionar el problema de la protección de la infancia en línea.

Además, cada país tiene su opinión al respecto, y tales diferencias pueden explotarse o aprovecharse en detrimento de los niños. Los delincuentes y pedófilos sabrán qué países tienen las leyes más laxas o mecanismos menos desarrollados a este respecto y, naturalmente, se aprovecharán de ello a menos que se tomen las medidas apropiadas.

Dadas las incoherencias en los marcos políticos y legislativos de los distintos países, es imperativo que la industria de Internet en su conjunto siga directrices de prácticas idóneas y adopte normas y códigos de práctica mundiales que les permitan cumplir con su responsabilidad social para con la protección de la infancia en línea.

En muchos países del mundo, la industria está tomando la iniciativa de adoptar métodos voluntarios y autorregulados que demuestran su compromiso con la elaboración de un método adecuado para que los niños utilicen las comunicaciones y TIC en línea. Va en interés de la industria tomar medidas y estar en la vanguardia, no sólo porque es lo correcto desde el punto de vista moral, sino también porque, a la larga, logrará así que los usuarios tengan confianza en Internet como medio de comunicación.

Sin esa confianza, la tecnología nunca podrá desarrollar todo su potencial para enriquecer y capacitar a todas las personas y, además, contribuir a la prosperidad económica y bienestar de cada país.

8. Otra información y referencias

Colaboración en el seno de la industria

European Framework for Safer Mobile Use by Younger Teenagers and Children: http://www.gsmeurope.org/documents/safer_ children.pdf

Enlaces a Códigos de Práctica nacionales para la utilización segura de los móviles de los operadores móviles europeos (en inglés e idioma original): http://www.gsmeurope.org/safer_mobile/national.shtml

GSMA, Code of Practice on Spam: http://www.gsmworld.com/ our-work/public-policy/protecting-consumers/mobile_spam.htm

Programa una Internet más segura: Empowering and Protecting Children Online, http://ec.europa.eu/information_society/activities/sip/ index_en.htm

Telecom Italia sobre protección de la infancia: www.telecomitalia.com, *Sustainability->Hot Topics-> Protection of Children and Abuse*

Estudio sobre *Safer Internet Program Benchmarking of Filtering software and services*: http://ec.europa.eu/information_society/activities/sip/projects/ targeted/filtering/sip_bench/index_en.htm

Home Office: Internet Taskforce for Child Protection (Reino Unido) – industry good practice documents: http://police.homeoffice.gov.uk/ operational-policing/crime-disorder/child-protection-taskforce

Clasificación del contenido

Organismo Independiente de Clasificación Móvil de la Industria de Reino Unido: http://.www.imcb.org.uk/

Proyecto de la UE *Kids Online*: http://www.eukidsonline.net/

Safer Children in a Digital World: Informe de la Byron Review: http://www.dcsf.gov.uk/byronreview/

Educación y comunicación con los clientes

Recurso de la Industria para que los docentes ayuden a los jóvenes a utilizar la tecnología: http://www.teachtoday.eu/

Contenido ilegal

International Association of Internet Hotlines: https://www. inhope.org/

Alianza móvil contra el contenido pedófilo

http://www.gsmworld.com/mobilealliance

Coalición financiera contra la pornografía infantil

http://www.missingkids.com/missingkids/servlet/ PageServlet?LanguageCountry=en_US&PageId=3703

Autorregulación de los medios

Todos los servicios en línea de la BBC están sujetos a las Directrices editoriales de la BBC (http://www.bbc.co.uk/guidelines/editorialguidelines/edguide)

y las Directrices de servicios en línea de la BBC (http://www.bbc.co.uk/guidelines/editorialguidelines/onguide)

Informes nacionales

Reino Unido: Safer Children in a Digital World: Informe de la Byron Review, (http://www.dcsf.gov.uk/byronreview/

Unión Internacional de Telecomunicaciones
Place des Nations
CH-1211 Ginebra 20
Suiza
www.itu.int/cop

Impreso en Suiza
Ginebra, 2011

En colaboración con:

TELECOM ITALIA

AfrISPA
African Internet Service

EBU·UER

GSMA

CHIS

vodafone