

Directrices sobre Protección de la Infancia en Línea para los encargados de formular políticas



www.itu.int/cop

Notificación legal

El presente documento puede ser actualizado en cualquier momento.

Las fuentes externas se mencionan, en su caso. La Unión Internacional de Telecomunicaciones (UIT) no se hace responsable del contenido de las fuentes externas, incluidos los sitios web externos mencionados en la presente publicación.

Ni la UIT ni ninguno de sus representantes será responsable de la utilización de la información contenida en la presente publicación.

Descargo de responsabilidad

La mención de países, empresas, productos, iniciativas o directrices específicos, o las referencias a los mismos, no implican en modo alguno que las apoyen o recomienden la UIT, los autores o cualquier otra organización a la cual estén afiliados los autores antes que otras de carácter similar que no se mencionen.

Las solicitudes de reproducción de extractos de la presente publicación pueden enviarse a: jur@itu.int

© Unión Internacional de Telecomunicaciones (UIT), 2009

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 Sandra Pandí (UIT)
- John Carr (*Children's Charities' Coalition on Internet Safety*)
- Raoul Chiesa y Francesca Bosco (Instituto Interregional de las Naciones Unidas para Investigaciones sobre la Delincuencia y la Justicia)
- Catherine Cummings y Jessica Sarra (*International Centre for Missing & Exploited Children*)
- Johan Martens (*Child Helpline International*)
- Michael Moran (Interpol)

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, diríjase a Cristina Bueti en la dirección cop@itu.int



Índice

Prefacio	
Resumen ejecutivo	1
Directrices para los encargados de formular políticas	4
Marco jurídico	
Mecanismos de presentación de informes y recursos para hacer cumplir la ley	
Convergencia nacional	
Recursos educativos y de divulgación	
1. Antecedentes	7
2. Utilización de Internet por niños y jóvenes	11
Interactividad y contenidos generados por el usuario	
Sitios de interfuncionamiento social	
Conversación y mensajería instantáneas	
Programas de intercambio de ficheros entre pares	

3. Material pedófilo	17
Una definición	
Armonización de las leyes	
Capacitación informática forense para el cumplimiento de la ley	
Cooperación internacional e intercambio de datos	
Requisitos de notificación	
Reducción de la disponibilidad de imágenes pedófilas	
4. Principales riesgos para los menores en línea	31
Contenido	
Contacto	
Conducta	
Comercio	
Uso excesivo	
Efectos sociales	
5. Soslayar los riesgos	35
Una Lista de Actividades Nacionales	
Marco jurídico completo	
Necesidad de una convergencia en la protección de la infancia en línea a escala nacional	
Necesidad de desarrollar los recursos locales en los que se reflejan las normas culturales locales y las leyes nacionales	
Necesidad de realizar actividades de concienciación y educación pública	
Necesidad de establecer mecanismos de notificación de comportamientos predatorios en línea, incluida la intimidación	
Ayudar a los niños a mantenerse seguros gracias a la utilización de herramientas técnicas	



6. Partes interesadas	41
Niños y jóvenes	
Padres, tutores y pedagogos	
Sector industrial	
La comunidad de instituciones de investigación y ONG	
Observancia de la ley	
Servicios sociales	
7. Conclusión	45
Apéndice 1	47
Contactos delictivos contra niños y jóvenes	
Apéndice 2	49
“Pornografía infantil: legislación modelo y análisis mundial”	
Apéndice 3	70
Software sobre seguridad de menores	
Apéndice 4	71
Elaboración de una estrategia nacional	



“La protección de los niños en línea es un problema mundial que exige una respuesta mundial”



Prefacio



Acojo con agrado esta oportunidad de compartir con ustedes estas directrices, las cuales han sido elaboradas con la ayuda inapreciable de múltiples interesados.

La Protección de la Infancia en Línea —en la era de Internet en banda ancha disponible de manera generalizada— es una cuestión de importancia capital que exige urgentemente una respuesta coordinada a escala mundial. Aunque indudablemente las iniciativas locales e incluso nacionales cumplen su función, Internet no tiene fronteras y por consiguiente la cooperación internacional será la clave para poder ganar las batallas que libremos.

La contribución de los encargados de formular políticas es esencial para triunfar en la lucha contra el ciberdelito y las ciberamenazas, por lo cual les estoy personalmente agradecido.

Dr. Hamadoun I. Touré

Secretario General de la Unión Internacional de
Telecomunicaciones (UIT)



En la Convención de las Naciones Unidas sobre los Derechos del Niño se define a un niño como cualquier persona menor de 18 años. En estas Directrices se abordan los problemas que tienen ante sí todas las personas menores de 18 años de edad en todas las regiones del mundo. Sin embargo, es muy poco probable que un joven usuario de Internet de 7 años de edad tenga las mismas necesidades o intereses que un joven de 12 años que comienza la escuela secundaria u otro de 17 que está a punto de entrar en la edad adulta. En diferentes partes de estas Directrices los autores han ajustado su asesoramiento o sus recomendaciones a esos diferentes contextos. Aunque el hecho de recurrir a categorías generales puede servir como una guía útil, nunca debe olvidarse que, en última instancia, cada niño es diferente. Además, hay numerosos factores legales y culturales locales diferentes que pueden influir de una manera importante en el modo según el cual se podrían utilizar o interpretar estas Directrices en un país o una región dados.

Actualmente se dispone de un acervo apreciable de instrumentos internacionales y de derecho internacional que sustentan y, en muchos casos, imponen la adopción de medidas encaminadas a proteger a los niños tanto en general como específicamente en relación con Internet. Esas leyes e instrumentos constituyen la base de estas Directrices, y están resumidas exhaustivamente en la Declaración y Llamamiento a la Acción de Río de Janeiro para evitar y poner término a la explotación sexual de niños y adolescentes, adoptada en el tercer Congreso Mundial contra la Explotación Sexual de Niños y Adolescentes celebrado en noviembre de 2008.



Resumen ejecutivo

Hace un decenio, aproximadamente 182 millones de personas tenían acceso a Internet a escala mundial, y casi todas esas personas habitaban en el mundo desarrollado. Sorprendentemente, a principios de 2009 se registraron más de 1.500 millones de usuarios de Internet en todo el mundo, de los cuales más de 400 millones disponían de acceso en banda ancha. Hoy en día los usuarios de Internet, pese a no ser ubicuos, se hallan realmente en todo el mundo, pues hay más de 600 millones de usuarios en Asia, 130 millones en América Latina y el Caribe y 50 millones en África¹. Internet sigue siendo un recurso dinámico e increíble, con unas capacidades casi ilimitadas para hacer frente a problemas sociales, que van desde la facilitación del acceso a la atención de salud hasta las oportunidades de aprendizaje a distancia

o el cibergobierno, pasando por la posibilidad de obtener empleos innovadores y mejor remunerados. No obstante, los crecientes problemas mundiales que plantea la ciberseguridad en línea exigen una respuesta mundial, sobre todo cuando se trata de proteger a nuestros ciudadanos digitales más jóvenes y vulnerables: nuestros niños.

Según las encuestas efectuadas recientemente, más del 60% de los niños y jóvenes establecen diariamente contactos en salas de conversación. Tres de cada cuatro niños en línea están dispuestos a compartir información personal sobre ellos mismos y sus familias a cambio de bienes y servicios, y nada menos que uno de cada cinco niños podría ser elegido como víctima de un depredador cada año.

Estas Directrices han sido elaboradas en el contexto de la Iniciativa para la Protección de la Infancia en Línea (PIeL)², con miras a sentar las bases para un ciber mundo seguro y protegido para las futuras generaciones. Se pretende que sirvan como un programa que pueda adaptarse y utilizarse de una manera coherente con las costumbres y leyes nacionales o locales. Además, se apreciará que en estas Directrices se abordan las cuestiones que podrían afectar a todos los niños y jóvenes menores de 18 años de edad, pero reconociendo que cada uno de esos grupos de edad tendrá diferentes necesidades.

Las Directrices han sido preparadas por la UIT en total colaboración entre un equipo de autores contribuyentes procedentes de instituciones de vanguardia activas en el sector de las TIC y de la seguridad

¹ Base de datos sobre indicadores mundiales de las telecomunicaciones/TIC, 2008, 12.ª edición.

² www.itu.int/cop



de la infancia en línea, a saber: *Children's Charities' Coalition on Internet Safety* (CHIS), *Child Helpline International* (CHI), *International Centre for Missing & Exploited Children* (ICMEC), Interpol e Instituto Interregional de las Naciones Unidas para Investigaciones sobre la Delincuencia y la Justicia (UNI-CRI). Se recibieron asimismo invaluable contribuciones de diferentes gobiernos y empresas de alta tecnología que comparten el objetivo común de lograr que Internet sea un lugar mejor y más seguro para niños y jóvenes.

Se espera que estas Directrices no sólo conducirán a la creación de una sociedad de la información más

integradora, sino que también permitirán a los Estados Miembros de la UIT cumplir con sus obligaciones de protección y salvaguarda de los derechos de los niños, tal como están consagrados en la Convención de las Naciones Unidas sobre los Derechos del Niño³ adoptada en el marco de la Resolución 44/25 de la Asamblea General de las Naciones Unidas el 20 de noviembre de 1989 y el Documento⁴ en el que se consignan los Resultados de la Cumbre Mundial sobre la Sociedad de la Información (CMSI)⁵.

En la CMSI, los dirigentes de la comunidad internacional le encomendaron a la UIT la Línea de Acción C5: “Creación de confianza

y seguridad en la utilización de las TIC”. En los resultados de la CMSI también se reconocían específicamente las necesidades de los niños y los jóvenes y de su protección en el ciberespacio. En el Compromiso de Túnez se reconoció “la función de las TIC en la protección de los niños y la facilitación del desarrollo de los niños”, así como la necesidad de “reforzar las actividades encaminadas a proteger a los niños contra los abusos y defender sus derechos en el contexto de las TIC”.

Mediante la publicación de estas Directrices, la Iniciativa PIeL hace un llamamiento a todos los interesados para que promuevan la adopción de políticas y estrategias encaminadas a proteger a los niños en el ciberespacio y fomentar su acceso seguro a todas las extraordinarias oportunidades que pueden ofrecer los recursos en línea.

³ www.unicef.org/crc/

⁴ La CMSI tuvo lugar en dos fases: en Ginebra (10-12 de diciembre de 2003) y en Túnez (16-18 de noviembre de 2005). La CMSI concluyó con el firme compromiso de “construir una sociedad de la información centrada en las personas, integradora y orientada hacia el desarrollo, en la que todos puedan crear, utilizar y compartir información y conocimientos y acceder a los mismos”. Véase www.itu.int/wsis

⁵ www.itu.int/wsis

Directrices para los encargados de formular políticas

Con miras a elaborar una estrategia nacional que apunte a la seguridad de los menores en línea, es preciso que los encargados de formular políticas consideren toda una gama de estrategias. A continuación se indican algunos ámbitos esenciales, y el Apéndice 4 contiene sugerencias adicionales.

	#	Ámbitos esenciales que se han de considerar
Marco jurídico	1.	Analizar el marco jurídico en vigor con el fin de determinar que se dispone de todas las facultades jurídicas necesarias para hacer cumplir la ley y de otros organismos pertinentes para proteger a las personas menores de 18 años en línea en todas las plataformas de Internet.
	2.	Determinar, <i>mutatis mutandis</i> , que todo acto contra un niño que sea ilegal en el mundo real es ilegal en línea y que son adecuadas las normas sobre protección y privacidad de datos en línea para personas legalmente menores de edad.
Mecanismos de presentación de informes y recursos para hacer cumplir la ley	3.	Garantizar que se establece y se promueve ampliamente la utilización de un mecanismo fácilmente comprensible para notificar contenidos ilícitos encontrados en Internet, como por ejemplo una línea directa nacional con capacidades de respuesta inmediata, y que los materiales ilícitos se eliminan o quedan inaccesibles.



	#	Ámbitos esenciales que se han de considerar
Convergencia nacional	4.	<p>Agrupar a todas las correspondientes partes interesadas en la seguridad de la infancia en línea, y en particular:</p> <ul style="list-style-type: none"> • Organismos gubernamentales • Organismos responsables de hacer cumplir la ley • Organizaciones de servicios sociales • Proveedores de servicios Internet (PSI) y demás proveedores de servicios electrónicos (PSE) • Proveedores de redes de teléfonos móviles • Otras empresas pertinentes de alta tecnología • Organizaciones de profesores • Organizaciones de padres • Niños y jóvenes • Organizaciones dedicadas a la protección de la infancia y demás ONG pertinentes • Comunidad de entidades académicas y de investigación • Propietarios de cibercafé y otros proveedores de acceso público, como por ejemplo bibliotecas, telecentros, PC Bangs⁶ y centros de juegos en línea, etc.
	5.	<p>Considerar las ventajas que podría aportar el establecimiento de una política de autorregulación o corregulación, en lo tocante a la formulación y publicación de códigos de buena conducta, tanto en lo que respecta a ayudar a propiciar y mantener la participación de todos los interesados pertinentes, como a acelerar la velocidad para formular y llevar a la práctica respuestas adecuadas a los cambios tecnológicos.</p>
Recursos educativos y de divulgación	6.	<p>Aprovechar los conocimientos y la experiencia de todos los interesados y elaborar materiales y mensajes para la seguridad de Internet que reflejen las leyes y normas culturales locales y garanticen que éstas se distribuyen con eficacia y se presentan adecuadamente a todos los tipos de audiencia previstos. Considerar la posibilidad de obtener la ayuda de los medios de comunicación masivos para promover los mensajes de sensibilización. Elaborar materiales que hagan hincapié en los aspectos positivos y capacitantes de Internet para los niños y los jóvenes y evitar los mensajes basados en el miedo. Promover formas positivas y responsables de comportamiento en línea.</p>
	7.	<p>Considerar la función que pueden desempeñar instrumentos técnicos tales como los programas de filtrado y los software sobre seguridad de menores para promover y complementar las iniciativas de educación y concienciación.</p>
	8.	<p>Alentar a los usuarios a asumir la responsabilidad de sus computadores, fomentando un servicio periódico que incluya la actualización del sistema operativo, además de la instalación y el perfeccionamiento de programas cortafuegos y antivirus.</p>

⁶ “PC Bang” es un término utilizado normalmente en Corea del Sur y en algunos otros países para describir una gran sala en la que se ofrecen prestaciones LAN para juegos en gran escala, ya sea en línea o entre los jugadores de la sala.





1



Antecedentes

El origen de la tecnología que hoy conocemos como “Internet” se remonta por lo menos al decenio de 1950. No obstante, la chispa que hizo estallar el crecimiento exponencial de Internet y la transformó en un elemento extremadamente útil para nuestras vidas, tanto desde el punto de vista económico como social, así como en una característica aparentemente permanente de la vida moderna, fue la creación de la *World Wide Web* a principios del decenio de 1990.

En los albores de la revolución de Internet, los usuarios quedaban muy sorprendidos ante la posibilidad de ponerse en contacto con personas y acceder a la información a través de océanos y zonas horarias con sólo unas pocas pulsaciones del ratón. Sin embargo, para poder hacerlo en general debían encontrarse en un sitio fijo frente a un computador a menudo grande o macizo, normalmente un PC. Hoy en día las personas pue-

den conectarse a la red mundial utilizando un teléfono móvil, un ordenador portátil u otro dispositivo portátil, con frecuencia con capacidades vídeo y acceso a alta velocidad. Muchas consolas de juegos también funcionan con Internet y ello ha impulsado un enorme crecimiento de los juegos en línea entre niños y jóvenes.

Tomó unos 20 años alcanzar los primeros mil millones de usuarios de teléfonos móviles, pero los segundos mil millones se registraron en apenas unos pocos años. En cambio, tomó 125 años llegar a los primeros mil millones de abonados al teléfono de línea fija.

Cabría afirmar que la evolución de la segunda a la tercera generación de redes de teléfonos móviles es tan importante como el salto inicial del sistema analógico al digital. Éste comenzó hace más de un decenio y avanza a una velocidad acelerada. Las nuevas tecnologías incipientes de la cuarta genera-

“Agrupar a todas las correspondientes partes interesadas en la seguridad de la infancia en línea”





ción mantienen el énfasis en el acceso móvil pero a velocidades aún mayores. La convergencia de los medios de comunicación y las redes de banda ancha están abriendo nuevas avenidas para la distribución de programas recreativos digitales.

Actualmente los dispositivos de usuario son multifuncionales y están cada vez más personalizados. En un futuro próximo, los avances de la informática conectada permitirán que cientos de millones de objetos tengan la posibilidad de comunicarse entre sí por Internet, abriéndole el camino a innumerables aplicaciones domésticas y comerciales.

En los mercados de línea fija y celulares, la transición hacia redes de mayor capacidad va acompañada por una transición hacia redes basadas en el protocolo Internet. Como consecuencia de ello, cada vez se recurre más a las transmisiones por el protocolo

Internet (VoIP) (por ejemplo a través de servicios como Skype o Vonage), pero también aumenta la posibilidad de visualizar imágenes en movimiento por las redes IP. Nuevas tecnologías tales como la radiodifusión vídeo digital y la radiodifusión multimedios digital permitirán a los espectadores visualizar contenidos emitidos por dispositivos móviles en todo momento y en todo lugar.

Al parecer el mundo de las actividades recreativas entra en una era totalmente nueva. Al mismo tiempo, la tecnología digital tiene un efecto apreciable en la naturaleza de las interacciones sociales. Los teléfonos móviles ya han alterado el modo según el cual las personas se comunican, conciertan citas y efectúan múltiples tareas.

La expansión de la infraestructura electrónica y digital le ha ofrecido a muchos millones de personas la posibilidad de aprender, publicar y comunicarse a una escala

sin precedentes. Con frecuencia los niños y los jóvenes han sido los “pioneros” de la adopción y adaptación a las nuevas posibilidades que ofrecen estas tecnologías nuevas e incipientes. Ello ha capacitado enormemente a muchos jóvenes y está abriendo inmensas nuevas posibilidades en la esfera de la educación y el aprendizaje personalizado.

La rápida disminución del costo real de la información necesaria y de las tecnologías de comunicación, junto con los vastos cambios y mejoras de la infraestructura disponible, han permitido a muchos niños y jóvenes aprovechar las ventajas de la tecnología para hacer y lograr cosas desconocidas para generaciones anteriores.

Aunque el desarrollo de Internet difiere en función del país y la región, prácticamente en todos lados se puede acceder a la misma. En los países en desarrollo se utiliza tecnología inalámbrica para

muchas conexiones telefónicas y de Internet, en vez del acceso en línea fija; la transferencia y el almacenamiento de datos se están descentralizando y son aparentemente ilimitados. La “sociedad interconectada” que se viene vislumbrando desde hace unos decenios comienza a transformarse en realidad.

Gracias al mayor acceso, Internet está adquiriendo un carácter verdaderamente mundial y ofrece sus beneficios a un número cada vez mayor de personas, con inclusión de niños y jóvenes. La cultura y la economía de un país determinan las modalidades de desarrollo de Internet y ello tiene un efecto en los riesgos a los que estarán expuestos los menores, así como la manera según la cual los interesados locales hacen frente a esos riesgos. No puede haber un modelo único o sencillo para abordar una cuestión tan compleja.





2.

Utilización de Internet por niños y jóvenes

Aunque Internet viene existiendo desde hace varios decenios, su naturaleza ha cambiado espectacularmente desde su creación. Al principio era fundamentalmente un instrumento para intercambiar información y datos entre organismos gubernamentales e instituciones académicas. Durante el decenio de 1980 la red Internet fue abierta al público en general. Con el surgimiento de la *World Wide Web* en el decenio de 1990, Internet comenzó a propagarse a un ritmo sorprendente. En los últimos años ha tenido lugar una nueva revolución: el surgimiento de la Web 2.0. La web es cada vez más interactiva y una proporción mucho mayor de la sociedad está presente en Internet. Actualmente el número de personas conectadas es mayor, y a menudo los niños y

los jóvenes marchan a la cabeza como usuarios precoces.

Si bien el desarrollo de la web abrió Internet al público en general, durante cierto tiempo ésta siguió siendo una red poseída y poblada básicamente por gobiernos, instituciones académicas y empresas comerciales. Los particulares entraban en línea para acceder a informaciones que les proporcionaban esos grandes agentes, y esas primeras épocas de la web estuvieron marcadas por las siguientes características:

- Bajos niveles de conectividad
- Principalmente escasa anchura de banda
- Baja capacidad para el almacenamiento de datos
- Acceso y comunicación unidireccional



Con el correr del tiempo Internet siguió evolucionando y se registraron cuatro fenómenos de particular importancia:

- Aumento de la anchura de banda a un precio asequible
- Aumento de una capacidad de almacenamiento comparativamente barata
- Menores costos de acceso
- Desarrollo de la Internet móvil.

Estos nuevos adelantos ayudaron a establecer un nuevo tipo de Internet; en lugar de conectar sencillamente particulares a empresas, organizaciones y gobiernos, Internet también empezó a permitir que los particulares se conectasen entre sí y pasaran a ser editores en línea por propio derecho. Esta nueva Internet, a la que con frecuencia se alude como Web 2.0, tiene las siguientes características:

- Altos niveles de conectividad
- Gran anchura de banda
- Altos niveles de capacidad de almacenamiento
- Contacto personalizado e interactivo (contenido generado por el usuario)

Se han desarrollado nuevos instrumentos que proporcionan

a los usuarios diversos medios para establecer relaciones sociales y conectarse entre sí, a saber: mensajería instantánea, tableros de mensajes y conversación, servicios de acogida de fotos y vídeos, programas de intercambio de ficheros de par a par (P2P). Consideradas en conjunto, estas tecnologías y otras han dado lugar a un crecimiento fenomenal de sitios de interfuncionamiento social, los cuales en un periodo de tiempo muy breve han adquirido enorme popularidad entre niños y jóvenes.

Interactividad y contenidos generados por el usuario

Cada vez más los niños y los jóvenes, así como los adultos, atraviesan una parte importante de su vida con asistencia de estas nuevas tecnologías, y como resultado de ello, la naturaleza de los riesgos que asumen ha empezado a estar inextricablemente entrelazada con aspectos más generales de su comportamiento. Actualmente ya no es posible trazar una línea clara entre las llamadas “cuestiones de Internet” y los problemas del “mundo real”.

Sitios de interfuncionamiento social

La dimensión cualitativamente nueva e inteligente que caracteriza a los sitios de interfuncionamiento social es la manera según la cual éstos han agrupado varias tecnologías de Internet preexistentes en un solo lugar, al que le han incorporado nuevas prestaciones y han creado interfaces de muy grata utilización para el usuario. Gracias a estas nuevas interfaces, ahora es extremadamente sencillo utilizar las diversas prestaciones. Consideradas en conjunto, éstas han impulsado un rápido aumento en la popularidad de los sitios de interfuncionamiento social, lo que ha tomado a muchas personas por sorpresa, sobre todo a los padres.

Los sitios de interfuncionamiento social permiten a los usuarios crear perfiles en línea en los cuales pueden divulgar toda una serie de informaciones personales, como la edad, el sexo, la ciudad donde habitan y sus intereses. En particular las nuevas interfaces desarrolladas por los sitios de interfuncionamiento social hacen que resulte más fácil personalizar las páginas web del usuario,

añadiendo por ejemplo su música, sus fotografías y vídeos preferidos. Los niños y los jóvenes se han volcado a este proceso de una manera muy creativa. Los perfiles de usuario en los sitios de interfuncionamiento social se han transformado en extensiones del usuario y en un medio importante para que éste haga declaraciones acerca de sí mismo a sus amigos y al mundo en general.

Lo que es más importante, estos sitios de interfuncionamiento social permiten a los usuarios incorporar amigos con quienes pueden intercambiar mensajes. La audiencia que puede visualizar un perfil determinado depende por lo general del modo según el cual la persona ha utilizado los parámetros de privacidad del sitio. Con demasiada frecuencia, y esto ocurría sobre todo en los primeros días del interfuncionamiento social, los niños y los jóvenes no son conscientes de que, a menos que tomen medidas específicas para limitar el acceso, por ejemplo

fijando su perfil con los parámetros “privados” o “únicamente para amigos”, cualquiera puede abrir y visualizar el perfil en su totalidad. Esto los hace vulnerables a los depredadores que podrían haber enmascarado su edad con miras a establecer una relación con el/la niño/a o el/la joven. Según informes, ha habido casos de niños y jóvenes que han publicado imágenes eróticas de ellos mismos, o que las han intercambiado por teléfono móvil, un fenómeno conocido como “sexting”⁷, a menudo sin advertir que la difusión de su imagen podría ser tanto perjudicial para ellos como un acto ilegal, y que además podría verla un gran número de personas que visiten su sitio o perfil. En términos más generales, en los sitios de interfuncionamiento social se ha puesto de relieve el problema de cómo administrar los contenidos generados por el usuario, que es el rasgo característico de la Web2.0. Algunos sitios han establecido políticas de moderación proacti-

va, a tenor de las cuales rastrean vídeos e imágenes inapropiados o ilegales, mientras que en otros sólo se considera una imagen o un vídeo en particular si éste le es notificado mediante informe por una persona que lo considera inconveniente y desea que éste sea suprimido.

A menudo la popularidad de los diferentes sitios de interfuncionamiento social está determinada por pautas idiomáticas y regionales. Algunos ejemplos son: MySpace (particularmente popular en América del Norte), Facebook (muy popular en América del Norte, Europa y Oceanía), Hi5 (el más propagado en América Latina), Orkut (América Latina), SkyBlog (países francófonos), Live Journal (Rusia y CEI), Friendster (Asia y Pacífico), Cyworld (República de Corea y República Popular de China), LinkedIn (Europa, Estados Unidos e India), Last.fm (Países Nórdicos y Bálticos y Europa Central).

⁷ *Sexting*: fenómeno relativamente nuevo en el marco del cual niños y jóvenes se ponen en peligro al divulgar en línea imágenes de ellos mismos sexualmente provocativas o enviarlas a amigos utilizando tecnologías móviles.

Fuente: Proyecto de Directrices para Padres, Tutores o Educadores sobre Protección de la Infancia en Línea, UIT, 2009.



Según Danah Boyd⁸, las expresiones en línea, los perfiles personales u otros tipos de publicaciones tienen cuatro características fundamentales que pueden crear riesgos adicionales para niños y jóvenes:

1. Persistencia: Las comunicaciones interconectadas se registran y con ello se amplía el periodo de vida de cualquier comunicación.

2. Capacidad de rastreo: Puesto que las comunicaciones en línea se registran y se determina la identidad mediante textos, los instrumentos de búsqueda y hallazgo pueden ayudar a las personas a encontrar a otras personas.

3. Duplicabilidad: Las comunicaciones interconectadas pueden copiarse de un lugar a otro verbatim de tal modo que no es posible hacer una distinción entre el “original” y la “copia”.

4. Audiencias invisibles: En la práctica es imposible determinar

quién podría navegar a través de perfiles o de otras comunicaciones en línea. Este hecho se ve complicado aún más por las otras tres características antes mencionadas, dado que los perfiles pueden verse o se puede acceder a los mismos en un momento y un lugar diferentes del momento y el lugar en el que fueron originalmente creados.

Conversación y mensajería instantáneas

Las herramientas de mensajería instantánea (IM) permiten a las personas conectarse entre sí en línea directamente y mantener conversaciones mediante mensajes escritos (y cada vez más a través de videoconferencias). Las personas pueden añadir el nombre de los particulares que conocen a sus listas de contactos y ver si éstos están disponibles (en línea) para hablar con ellos. Estas conversaciones, o “chats”, pueden mantenerse con una persona

(bilateralmente) o con un grupo de personas (multilateralmente). La mayoría de los programas permite guardar el contenido de las conversaciones si así se desea o necesita. Entre los programas de IM y chats más conocidos cabe mencionar MSN Chat, Yahoo! Messenger, Google Talk, y AOL Instant Messenger.

Programas de intercambio de ficheros entre pares

Los programas de intercambio de ficheros entre pares (también llamados programas P2P) permiten a los particulares cargar y descargar directamente ficheros desde y hacia sus propios discos de almacenamiento. Cualquier persona que utilice el mismo programa puede buscar ficheros y telecargarlos desde otros que tengan esos mismos ficheros

disponibles. Estos programas facilitan el intercambio de conocimientos e información, pero también han conducido a violaciones de los derechos de autor y a la proliferación de programas maliciosos (*malware*) tales como virus y Troyanos⁹. Estas redes también se utilizan para distribuir CAM. Entre los programas P2P más conocidos figuran Bittorrent, E-mule, E-donkey y Kazaa.

⁸ Danah Boyd, Fellow en *Harvard Law School's Berkman Center for Internet and Society*.

⁹ El caballo de Troya, también conocido como “Troyano” en el contexto de la informática y los software, se refiere a una clase de amenaza informática (programas informáticos dañinos) que parece desempeñar una función conveniente pero que de hecho realiza funciones dañinas encubiertas que permiten un acceso no autorizado al aparato huésped, dándoles así la posibilidad de salvar sus ficheros en el ordenador del usuario o incluso mirar la pantalla del usuario y controlar el computador. Véase [http://en.wikipedia.org/wiki/Trojan_horse_\(computing\)](http://en.wikipedia.org/wiki/Trojan_horse_(computing))





3.

Material pedófilo

Una definición

En muchas jurisdicciones aún se les sigue llamando “pornografía infantil” o “imágenes indecentes de niños” a las fotografías o vídeos de menores que son víctimas de explotación y malos tratos. Hoy en día muchos profesionales prefieren utilizar el término “material pedófilo” o CAM (*child abuse material*), pues se estima que esa expresión transmite con mayor precisión la naturaleza real del contenido. En este documento se utilizará ese término.

Internet ha transformado completamente la magnitud y la naturaleza de la producción y distribución de CAM.

La revolución sexual de mediados del decenio de 1960, caracterizada por una apertura a la variación y la expresión sexual, abonó el terreno para una demanda floreciente de pornografía que proliferó en almacenes y librerías de numerosas ciudades europeas y americanas¹⁰. Esas tiendas, y de hecho todo un montaje de negocios de estilo encomienda postal, almacenaban y suministraban cantidades masivas de pornografía de todo tipo y todos los grados posibles de severidad. La demanda de pornografía fue atendida vigorosamente por cierto número de grandes agentes en todo el mundo pues, como todos los vacíos, éste fue rellenado rápidamente por empresarios que establecieron con celeridad una gran red de suministro.

¹⁰ O'Donnell and Milner, (2007), *Child Pornography, Crime computers and society*, Willan.

Una parte de los materiales pornográficos que se compraban, vendían y comercializaban contenían imágenes de niños que eran víctimas de abusos sexuales. Las leyes para combatir el CAM promulgadas en 1977 en los Estados Unidos pronto se propagaron a Europa, donde se proscribió el CAM y su comercialización pasó a la clandestinidad. Hacia 1986, se habían cerrado prácticamente todas las vías tradicionales para obtener ese tipo de materiales, y existió la posibilidad de suprimir completamente el comercio de CAM¹¹.

A esa altura las dificultades para encontrar CAM hacían que las personas que deseaban obtener esos materiales debían tomar grandes riesgos e incurrir en ingentes gastos para acceder a los mismos. Pero todo eso cambió

con la llegada de Internet. Hablando de la cibersexualidad que se puede transferir fácilmente, el Dr. Alvin Cooper se refirió al “motor de la triple A” para describir la manera según la cual Internet revolucionó la posesión y distribución de CAM:

- accesibilidad (Internet pone a disposición CAM las 24 horas del día y los 7 días de la semana alrededor del mundo);
- asequibilidad (la mayor parte del CAM es gratuito y se puede canjear o sencillamente telecargar); y
- anonimato (la gente cree verdaderamente que sus comunicaciones por Internet son privadas y quedan ocultas).

Esto los alentó a buscar y comercializar CAM, pues estimaron que

ello no tenía repercusiones. El hecho de que esos materiales fueran gratuitos y estuviesen disponibles también les alentó a creer que eran inocuos.

En 1997, el Sr. William Utting, un distinguido experto en servicios sociales para menores, describió al CAM como una “industria artesanal”¹². Probablemente ése fue el último momento en la historia en el que se pudo hacer esa afirmación; hoy en día se trata de una industria mundial y al parecer ningún país es inmune a la misma.

Es muy difícil determinar el tamaño o la forma exactos de lo que básicamente es una empresa clandestina y a menudo ilícita. En diferentes momentos se hicieron todo tipo de estimaciones acerca del número de sitios web involucrados¹³, el número de menores

que son víctimas de abusos para crear las imágenes¹⁴ y el valor monetario total del mercado de imágenes. Nadie que esté familiarizado con este ámbito pone en duda que el número de personas que participa en la visualización y distribución de CAM es elevado, y ha habido pruebas de la participación del crimen organizado¹⁵ en la distribución comercial de estos materiales. Igualmente, no cabe ninguna duda de que el número de imágenes ilícitas actualmente en circulación en Internet asciende a muchos millones, mientras que el número de menores que muestran esas imágenes es del orden de las decenas de miles¹⁶, y esas cifras corresponden únicamente a los que se han descubierto hasta la fecha.

¹¹ Jenkins, P, *Beyond Tolerance*, 2001, New York University Press.

¹² Reino Unido, HMSO, 1997

¹³ En su Informe anual de 2007, IWF afirmó que menos de 3.000 sitios web en idioma inglés contenían el grueso de las imágenes pedófilas disponibles en línea. Tres años antes, el Centro de Investigaciones sobre Delitos Informáticos de los Estados Unidos dijo que ese número era superior a 100.000.

¹⁴ Correspondencia con Interpol. Véase el Informe de Teléfono Arcobaleno en http://www.telefonoarcobaleno.org/pdf/tredicmoreport_ta.pdf

¹⁵ Véanse los pormenores del caso “Reg Pay” en http://www.usdoj.gov/criminal/ceos/Press%20Releases/ICE%20Regpay%20PR_080906.pdf

¹⁶ Correspondencia con Interpol antes mencionada. Teléfono Arcobaleno en su Informe hablaba de 36.000 menores, de los cuales el “42% eran menores de 7 años de edad y el 77% menores de 12 años de edad”. http://www.telefonoarcobaleno.org/pdf/tredicmoreport_ta.pdf



Originalmente uno de los principales medios de distribución de CAM por Internet eran los *Usenet Newsgroups*. Aunque ésta sigue siendo una fuente importante, hoy en día también se utilizan varias otras tecnologías de Internet, de las cuales tal vez la más importante sea la *World Wide Web*, ya que es la más accesible y fácil de utilizar. Sin embargo, puesto que en algunos países se ha dificultado en gran medida la utilización de la web para distribuir CAM, también se utilizan otras tecnologías en Internet cada vez con mayor frecuencia. Entre ellas tal vez la más importante sea el software de intercambio de ficheros o P2P. Según Interpol, el software Peer2Peer es muy fácil de controlar desde el punto de vista técnico, pero el inmenso volumen de personas involucradas hace que en la práctica resulte muy difícil.

Toda vez que aparece en Internet o se telecarga la imagen de un menor víctima de abusos, en un sentido importante este menor

vuelve a ser víctima del abuso. Las víctimas deben vivir con la longevidad y la circulación de esas imágenes por el resto de sus vidas. La mejor prueba de ello es la reacción de las víctimas y sus familias cuando se enteran de que se han puesto en circulación o telecargado en Internet esas imágenes¹⁷.

Ésa es la razón por la cual hay acuerdo general de que tan pronto como se descubre una de esas imágenes o sitios web es importante actuar con la mayor celeridad posible para suprimir la imagen o eliminar el sitio o hacer que éste resulte inaccesible. Con miras a facilitar este proceso, se ha desarrollado un sistema de líneas directas (*hotlines*) nacionales. Actualmente están en funcionamiento líneas directas en más de 30 países y su número va en aumento¹⁸. Sería muy conveniente que el número de líneas directas aumentara apreciablemente como parte de una campaña mundial para poner término al tráfico de CAM en línea.

Otra razón para actuar con rapidez con el fin de suprimir o hacer que las imágenes ilícitas encontradas en Internet resulten inaccesibles es el hecho de que, cuanto más tiempo permanezcan en circulación mayor será la posibilidad de que un nuevo usuario tropiece con la imagen y la telecargue. Existen ciertas evidencias de que las personas que participan en la telecarga y compilación de CAM son más propensas a participar en actividades delictivas o abusivas de niños en el mundo real. (En *Fantasy to Reality: The Link Between Viewing Child Pornography and Molesting Children*. Kim, C (2004)).

Para las autoridades encargadas de hacer cumplir la ley, la importancia de identificar a una víctima de CAM publicado en Internet es cada vez mayor. Se están estableciendo procedimientos y sistemas nacionales a tenor de los cuales el CAM incautado durante las investigaciones o que de otro modo cae en manos de los investigadores se examina para tratar de identificar a la víctima del abuso y por consiguiente al perpetrador. Los materiales que no han sido vistos anteriormente y no puede deter-

minarse que han sido fabricados localmente se hacen circular en una red internacional de investigadores y especialistas nacionales en CAM. Esa red ha evolucionado en torno a la base de datos internacional sobre explotación sexual infantil (*International Child Sexual Exploitation Database, ICSE*) de Interpol y está coordinada en la sección Tráfico de Seres Humanos de Interpol, junto con el Grupo de Especialistas sobre Delitos contra Menores de esa misma organización.

La finalidad de esta base de datos es agrupar en un lugar todos los materiales CAM existentes en Internet que caen en manos de las autoridades responsables de la observancia de la ley. Esos materiales son examinados por una red de funcionarios especializados de todo el mundo y, de ser posible, se transfieren al país de origen para tratar de determinar la identidad del menor víctima. Cuando eso no es posible, los materiales se incorporan en la base de datos con detalles sobre el lugar donde se encontró, quién lo descubrió y cuándo.

¹⁷ *Child Molesters: a behavioral Analysis*, Kenneth V. Lanning, 2001.

¹⁸ Véase www.inhope.org





Se utilizan poderosos dispositivos de recuperación que indican si esas imágenes fueron vistas o no con anterioridad y, como suele ocurrir, las imágenes encontradas en un país pueden dar indicios que ayuden a identificar un caso de abuso en otro país. A veces puede verse incluso el rostro del delincuente en las imágenes, lo que conduce a su detención.

La iniciativa de INTERPOL y COP fomenta las prácticas idóneas en este ámbito al promover la formación de un recurso centralizado a escala nacional, capaz de administrar todos los materiales que se incautan dentro de sus fronteras, creando así un mecanismo nacional y contribuyendo de ese modo a los esfuerzos internacionales desplegados en esta esfera. De este modo se reducirían los esfuerzos de los investigadores, se evitaría la duplicación de actividades a escala mundial y, en última instancia, ello conduciría a la identificación de las víctimas y a la detención de los delincuentes.

Armonización de las leyes

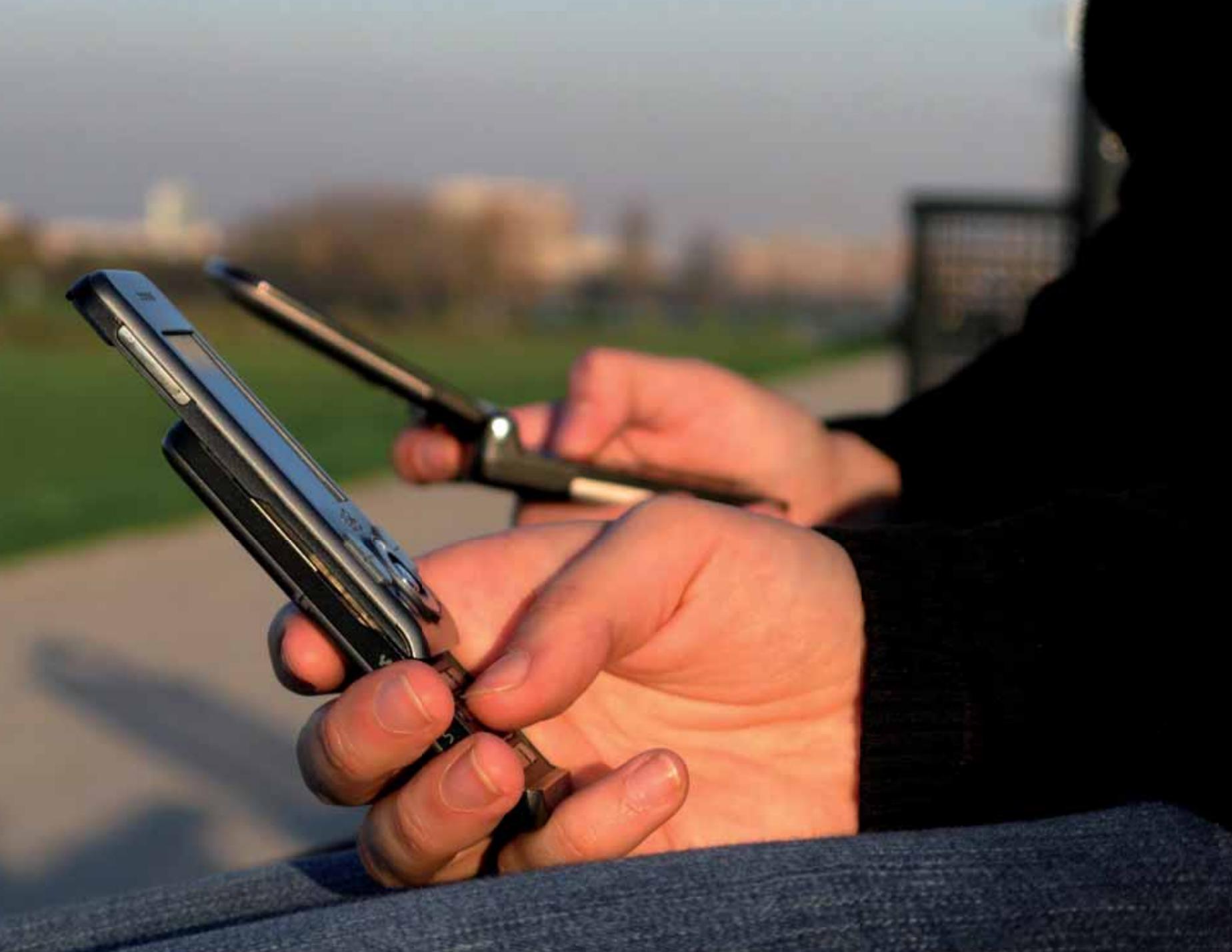
La adopción en todos los países de una legislación adecuada contra la utilización errónea de las tecnologías de la información y la comunicación (TIC) con fines delictivos o de otra índole es fundamental para lograr la ciberseguridad mundial. Puesto que las amenazas pueden tener su origen en cualquier lugar del planeta, el alcance de los problemas es inherentemente internacional y exige la cooperación internacional, así como asistencia en materia de investigación y unas disposiciones básicas y de procedimiento comunes. Por consiguiente, es importante que los países armonicen sus marcos jurídicos para combatir el ciberdelito, proteger a los menores en línea y facilitar la cooperación internacional.

El establecimiento de una legislación nacional adecuada, con su marco jurídico para combatir el ciberdelito y, en el marco de este enfoque, la armonización a nivel internacional, son aspectos esen-

ciales para el éxito de cualquier estrategia nacional sobre protección de la infancia en línea. Esto exige ante todo las necesarias disposiciones jurídicas de derecho penal básico para sancionar actos tales como el fraude informático, el acceso ilegal, la interferencia de datos, las violaciones de los derechos de autor y los CAM. El hecho de que el código penal contenga disposiciones aplicables a actos similares cometidos en el mundo real no implica que éstas puedan aplicarse también a los actos cometidos por Internet. Así pues, es vital realizar un análisis exhaustivo de la legislación nacional en vigor para identificar cualquier posible laguna. El siguiente paso consistiría en identificar y definir el léxico legislativo y los materiales de referencia que podrían ayudar a los países a promulgar normas de procedimiento y leyes sobre ciberdelito armonizadas. Los países podrían utilizar esos instrumentos prácticos para elaborar un marco jurídico sobre ciberseguridad y leyes conexas. La UIT ha estado trabajando con Estados Miembros y partes interesadas pertinentes en este contexto y

está aportando una gran contribución a la normalización mundial de las leyes sobre ciberdelito.

El *International Centre for Missing & Exploited Children*, ICMEC (Centro Internacional sobre Niños Desaparecidos y Explotados) publicó en abril de 2006 su Informe “Child Pornography: Model Legislation & Global Review” (Pornografía infantil: Análisis mundial y legislación modelo). La principal finalidad del Informe, del que ya se ha publicado la quinta edición, era dar un panorama general de la legislación sobre CAM en vigor y determinar la importancia que se le asigna a esta cuestión en los programas de política nacionales. El estudio giraba en torno a algunos ámbitos esenciales: legislación específica sobre CAM; leyes que contienen una definición de CAM; leyes que penalizan la posesión, independientemente de la intención de distribuir esos materiales, leyes que contemplan los delitos facilitados por ordenador relacionados con el CAM; y notificación de contenidos ilícitos por parte de los PSI.





El Apéndice 4 contiene una copia de las conclusiones detalladas de ICMEC. Del Informe se desprende claramente que hay considerables e importantes variaciones en los enfoques legislativos adoptados por los diferentes países. La comunidad internacional debe encontrar el modo de conferir mayor coherencia a la lucha contra este problema mundial.

Otro objetivo del Informe de ICMEC sobre la legislación modelo es recomendar los ámbitos en los cuales se necesita una legislación para contemplar los diversos aspectos de los CAM y los delitos conexos a escala mundial. Como ocurre con otros tipos de ciberdelitos, la posesión, fabricación y distribución de CAM a menudo se efectúa sin tener en cuenta las fronteras internacionales y por consiguiente exige la promulgación de leyes en cada país que sean compatibles o jurídicamente equivalentes: esto es lo que se entiende por armonización.

Los delincuentes que explotan sexualmente a niños, independientemente del hecho de que

lo hagan usando ordenadores e Internet o mediante viajes a otros países, preferirán atacar niños en países que carezcan de legislación o fiscalización estricta y en países que estén al margen del marco de cooperación internacional. Para poner término a la explotación infantil a nivel internacional es indispensable observar las normas jurídicas internacionales y adoptar las correspondientes leyes y prácticas nacionales.

Muchos países abordan en términos generales la explotación infantil en la medida en que ésta guarda relación con la mano de obra y otros delitos, o bien pueden prohibir la pornografía en general. Sin embargo, estas leyes no bastan, ya que no se refieren específicamente a los aspectos criminales de las diversas formas de explotación sexual de niños y las imágenes de maltrato infantil. Para que éstas sean verdaderamente eficaces, los países deberían alentar la adopción de una legislación específica para penalizar el CAM e incluir delitos concretos por la utilización de tecnologías e Internet

para actividades relacionadas con CAM; de otro modo, los delincuentes podrán sacar provecho de las lagunas de la legislación.

Asimismo, la ley debe contener disposiciones que prevean la asignación de recursos para hacer cumplir esas leyes específicas e impartir formación a los magistrados, así como funcionarios fiscales y encargados de hacer cumplir la ley, quienes indefectiblemente se verán obligados a mantenerse al corriente de la utilización de tecnologías por los delincuentes.

Entre las principales esferas de inquietud y orientaciones con miras a la adopción de leyes cabe mencionar las siguientes:

- Definir un “niño” de una manera clara y precisa, de conformidad con la Convención de las Naciones Unidas sobre los Derechos del Niño.
- Definir los “materiales pedófilos” (CAM) para incluir terminología específica de la esfera informática y de Internet.

- Crear delitos específicamente relacionados con: posesión, fabricación y distribución de CAM, con inclusión de pseudoimágenes, telecarga o visualización deliberadas de esas imágenes en Internet.
- Crear delitos para padres o tutores que permiten o facilitan la participación de sus niños en CAM.
- Crear delitos para las personas que revelen a otros dónde encontrar CAM.
- Considerar el intento de perpetrar un delito relacionado con CAM como un delito penal.
- Contemplar la responsabilidad penal de los niños involucrados en CAM. La responsabilidad penal debe recaer en el delincuente adulto, no en el niño víctima.
- Aumentar las penas para los delincuentes reincidentes o miembros del crimen organizado, y considerar otros factores agravantes al emitir la sentencia.

Una definición básica de CAM debería incluir la representación visual o descripción de un niño que realiza un acto o exhibición sexual real o simulado, o pseudoimágenes de los mismos; en ésta también se debería tener en cuenta cómo se utilizan tecnologías tales como ordenadores, Internet, teléfonos móviles, PDA, consolas de juegos, cámaras vídeo y DVD para facilitar los CAM, indicando claramente que los CAM y todo lo que está relacionado con los mismos es ilegal, independientemente de la plataforma utilizada.

Capacitación informática forense para el cumplimiento de la ley

Además de las disposiciones jurídicas de derecho penal básico, los organismos encargados de hacer cumplir la ley necesitan disponer de las herramientas e instrumentos necesarios para investigar el cibercrimen. Esas mismas investigaciones plantean algunos desafíos. Los perpetradores pueden actuar

prácticamente desde cualquier lugar del mundo y tomar medidas para enmascarar su identidad. Las herramientas e instrumentos necesarios para investigar el cibercrimen pueden ser muy diferentes de las que se utilizan para investigar delitos ordinarios.

Para los depredadores que tienen la intención de explotar sexualmente a menores, la red Internet, los ordenadores, los teléfonos celulares, los PDA y demás dispositivos digitales de todo tipo son instrumentos indispensables. La tecnología con la que funcionan estos dispositivos es cada vez más compleja y cambia a un ritmo acelerado. Para poder obtener y preservar importantes evidencias dejadas por los delincuentes es indispensable que las autoridades encargadas de hacer cumplir la ley reciban la capacitación y tengan la competencia técnica necesaria para recuperar pruebas que se ajusten a los requisitos de los tribunales nacionales e internacionales. Por consiguiente, se debe

impartir formación a los funcionarios encargados de asuntos jurídicos, fiscales y de la observancia de la ley, para ayudarlos a comprender cómo se efectúa el análisis forense de los discos duros de los ordenadores y otros dispositivos. Esta capacitación debe actualizarse continuamente para mantenerlos al corriente de los constantes cambios tecnológicos y permitirles adquirir experiencia práctica. Hay muchos conjuntos de software que vienen con mecanismos para efectuar exámenes de los materiales incautados con posibilidad de lectura únicamente, y a menudo en el precio de compra de estos conjuntos está incluida la capacitación. Por desgracia estas soluciones a menudo son caras y están fuera del alcance de los países en desarrollo. Si se proporcionase una financiación adecuada se podría disponer de capacitación desde dentro de la industria de la seguridad privada y la observancia de la ley.

Numerosas empresas del sector privado cuentan con la tecnología y la competencia técnica necesarias para contribuir a esta labor, de modo que podría tratar de obtenerse la asistencia crítica mediante la concertación de alianzas entre los sectores público y privado para impartir formación y proporcionar apoyo técnico.

Cooperación internacional e intercambio de datos

Es muy importante promover el intercambio de datos y la cooperación internacional a alto nivel.

Un papel fundamental de la UIT, a tenor de la CMSI, es crear confianza y seguridad en la utilización de las TIC. Los jefes de Estado y de gobierno y otros dirigentes mundiales que participaron en la CMSI, así como los Estados Miembros de la UIT, le encomendaron a la Unión que tomase medidas concretas para reducir las amenazas e inseguridades relacionadas con la sociedad de la información.



La CMSI consideró que la Línea de Acción C5 abarca una amplia gama de temas y partes interesadas. Según se destaca en el párrafo 110 de la Agenda de Túnez, *“La coordinación de las actividades de implementación por las múltiples partes interesadas contribuiría a evitar la duplicación de actividades. Se coordinarían, entre otras cosas, el intercambio de información y mejores prácticas, la creación de conocimientos y la asistencia en la creación de asociaciones entre múltiples partes interesadas y entre los sectores público y privado”*.

A través de su red integrada por 187 países, INTERPOL¹⁹ se especializa en facilitar el intercambio de información sobre políticas. Esta red permite el intercambio instantáneo de información entre países y por ampliación del sistema i24/7, directamente a las unidades de especialistas.

Cuando el intercambio de información y evidencias es en la esfera jurídica, la cooperación mutua en las investigaciones penales internacionales se efectúa con arreglo al marco jurídico y las disposiciones de convenios multilaterales o tratados bilaterales de asistencia jurídica mutua. Éstas no siempre se adecuan al mundo de Internet, que avanza a un ritmo acelerado.

A pesar de los acuerdos con carácter de tratado, si no existe una ley correspondiente en el país que solicita la cooperación, la asistencia podría no proporcionarse en absoluto o ser muy limitada. La parte que proporciona la información podría imponer condiciones para la utilización de la información y exigir confidencialidad.

Es fundamental aplicar un enfoque cooperativo destinado a crear un consenso a escala global sobre estos elementos comunes que deberían formar parte de cualquier marco jurídico encaminado a proteger a los niños en el ciberespacio. Habida cuenta del carácter internacional del ciberdelito y de la explotación infantil en particular, es imperativa una cooperación internacional efectiva para hacer cumplir la ley si queremos hacer frente a este problema a escala mundial.

19 INTERPOL también coordina su grupo de trabajo sobre delitos contra menores, que se reúne una vez por año en sesión grupal. Este grupo de trabajo está dividido en cinco subgrupos y sus miembros se reúnen prácticamente a lo largo de todo el año con el fin de elaborar proyectos. Los cinco subgrupos son: Delitos

contra menores facilitados por Internet, Delincentes del sexo, Tráfico de menores y Delitos graves y violentos contra menores. El quinto subgrupo se dedica a la identificación de víctimas y facilita la cooperación internacional en torno a la base de datos internacional sobre explotación sexual infantil.





Requisitos de notificación

Los miembros del público que entran en contacto con CAM deben informar al respecto a los responsables locales de hacer cumplir la ley y/o a una línea directa nacional²⁰. Además hay tres clases de individuos y de organizaciones a las que se debería alertar en particular para que notificaran presuntos CAM, ya sea directamente al organismo encargado de hacer cumplir la ley o a otra organización designada, como por ejemplo una línea directa:

1. Particulares que en el ejercicio de su profesión entran en contacto con niños y tienen el deber de protegerlos, como por ejemplo, maestros, tutores, consejeros, proveedores de servicios de atención de salud y funcionarios encargados de hacer cumplir la ley.

2. Particulares que en el ejercicio de sus funciones no entran necesariamente en contacto con niños pero pueden estar expuestos a CAM en el curso de su labor, por ejemplo técnicos informáticos, reveladores de fotos, etc.
3. Organizaciones o empresas cuyos servicios se utilizan para proliferar CAM y que deberían ejercer su responsabilidad de ciudadanía empresarial, por ejemplo, los PSI y otros PSE, las empresas de tarjetas de crédito y los bancos.

Aunque la inclusión de personas en las categorías 1 y 2 se explica por sí sola, la notificación por parte de los PSI, los bancos y las empresas de tarjetas de crédito es fundamental por cuanto sus servicios son esenciales para la transmisión de esos materiales y los delincuentes “utilizan indebidamente” esos servicios para

cometer actos delictivos contra niños. Esas industrias están en condiciones de detectar evidencias de CAM y se les debería alertar energicamente a que cooperen con las autoridades para proporcionar información sobre CAM toda vez que tropiecen con estos materiales.

Cabe señalar que actualmente hay unas empresas que están proporcionando una asistencia muy útil a este respecto. En el caso de los PSI y PSE, es más probable que éstos encuentren evidencias de CAM en ficheros, URL, nombres de dominio e imágenes, por lo que deberían notificar de inmediato a las autoridades correspondientes. Además, la compartición de URL, nombres de dominio y direcciones PI brinda la oportunidad de interrumpir el acceso a los sitios web conocidos por abuso infantil. Asimismo, habría que alertar los PSI y los PSE a explorar proactivamente sus redes en busca de CAM y notificar al respecto a las correspondientes autoridades encargadas de hacer cumplir la ley.

Habida cuenta de la función que desempeña actualmente Internet y su empleo con fines delictivos, la cooperación con las empresas relacionadas con Internet es indispensable. Además, las leyes deberían conferir protección a los PSI, PSE y demás entidades privadas que notifiquen la existencia de CAM y deberían ofrecer orientación sobre el tratamiento y la transmisión seguros de imágenes.

Se debería establecer un régimen de “Aviso y desmontaje” para autorizar a los PSI, PSE, registradores de nombres de dominio y anfitriones web a cerrar un sitio ofensivo o anular una cuenta de correo electrónico previa solicitud. En la mayoría de los casos, la utilización delictiva estará en violación de las “Condiciones de utilización” del contrato que concierta el usuario con el PSI o el PSE, lo que le confiere a la empresa el derecho irrefutable de tomar las medidas apropiadas. Siempre que sea posible, estas medidas deben tomarse en estrecha coordinación con las autoridades

²⁰ Las líneas directas nacionales remitirán los informes a los responsables de hacer cumplir la ley, y estos podrán luego analizar los informes para determinar conexiones locales o enviar la información a la base de datos internacional sobre explotación sexual infantil para su análisis.

encargadas de hacer cumplir la ley, en un esfuerzo por garantizar que se inicie una investigación que podría salvar a un niño de un abuso y permitir la detención del delincuente.

Desafortunadamente, la venta de CAM en Internet se ha transformado en una empresa global lucrativa que utiliza servicios bancarios, transferencias por cable y tarjetas de crédito para facilitar las transacciones, la distribución o la transmisión de CAM. Los funcionarios del sector financiero que entran en contacto con información relacionada con el CAM la deben remitir a las correspondientes autoridades. A menudo los sitios web que ofrecen servicios en régimen “pague para ver” o abonos a CAM aceptan tarjetas de crédito o servicios de transferencia de dinero para el pago.

Por regla general, se debería alentar al sector financiero a cooperar en consonancia con el modelo de la *Financial Coalition Against Child Pornography* (FCACP) (Coalición Financiera Contra la Pornografía Infantil)²¹, un proyecto conjunto

de IC-MEC y su organización hermana, el *National Center for Missing & Exploited Children* (NCMEC) (Centro Nacional sobre Niños Desaparecidos y Explotados). Esta efectiva coalición ofrece un medio para una cooperación estrecha entre la industria de servicios financieros, la industria de servicios Internet, las autoridades encargadas de hacer cumplir la ley y las ONG. La coalición ya ha obtenido un éxito destacado al negar a los proveedores comerciales de CAM la utilización del sistema financiero internacional. Trabajando de consuno, los miembros de la FCACP consiguieron no sólo aplazar las transacciones y las cuentas sospechosas, sino también rastrear actividades contables y flujos de dinero con miras a identificar a las personas y organizaciones que son en última instancia responsables de la venta de CAM. En 2009, se iniciaron actividades similares en el marco de una versión europea de esta coalición.

Reducción de la disponibilidad de imágenes pedófilas

La proliferación de CAM en Internet ha provocado un llamamiento público a la acción. Las autoridades encargadas de hacer cumplir la ley, los PSI, PSE y ONG de todo el planeta están colaborando para combatir estos contenidos en línea. Es evidente que las entidades encargadas de la observancia de la ley no dan a basto para soslayar este problema y que es necesario desplegar mayores esfuerzos para interrumpir y reducir el tráfico de CAM. Como resultado de ello, muchos países han comenzado a explorar remedios adicionales que multiplican los enfoques tradicionales para la observancia de la ley.

En varios países se ha adoptado el enfoque de alentar a los PSI y otros PSE a reducir la disponibilidad de páginas web que se sabe ofrecen CAM y bloquear el acceso a los *Usenet Newsgroups* que tienen periódicamente estos contenidos o bien publicitan su disponibilidad.

Conforme a este enfoque, se proporciona a los PSI y los PSE una “lista” de los *Usenet Newsgroups* y las páginas web activas que contienen o publicitan CAM. Esta lista se elabora y distribuye ya sea en cumplimiento de la ley o, en algunos casos, directamente mediante líneas directas nacionales. Es muy importante articular claramente la base sobre la cual se elaboran dichas listas. No se debe dejar lugar a ninguna sospecha de que el gobierno, las entidades responsables de hacer cumplir la ley u otros organismos puedan ejercer influencia en su composición con miras a incluir *Newsgroups* o sitios web que no contengan CAM sino artículos que éstos no desean ver publicados por otras razones.

A la hora de distribuir esta lista a los PSI y PSE, es esencial mantener un diálogo continuo con las entidades encargadas de hacer cumplir la ley. Estas últimas necesitan un tiempo suficiente para penetrar, analizar y documentar los contenidos y, en caso necesario, iniciar una investigación. Si no se tienen en cuenta las actividades

²¹ FCACP : http://www.icmec.org/missingkids/servlet/PageServlet?LanguagePaís=en_X1&PageId=3064.



de las entidades encargadas de la observancia de la ley se podría obstruir o retardar una investigación en curso. Además, sin la participación de estas entidades y sin una investigación, nunca se podrán detener y llevar a la justicia a los particulares que continuamente distribuyen CAM en línea.

Es importante que la lista de *Usenet Newsgroups* y de sitios conocidos se someta frecuentemente a prueba, se actualice y verifique para garantizar su exactitud. La lista no debería ser acumulativa; antes bien, un procedimiento de nuevo ensayo multiestratificado ayudará a garantizar la confianza pública en el funcionamiento de la lista. También es importante velar por que las directrices sobre los criterios para la inclusión en la lista sean transparentes. Algunos países utilizan un medio independiente para controlar la calidad de funcionamiento de la lista. Por último, se debería establecer un mecanismo para permitir las apelaciones contra la inclusión en la lista. En dicha lista sólo deben figurar los sitios que autorizan la publicación o visualización de contenidos ilícitos de confor-

midad con las leyes nacionales del país de que se trate. Cuando se bloquea un sitio, se debería mostrar al usuario una página con el signo STOP. Esta página STOP cumpliría la doble función de informar acerca de las razones por las cuales el sitio fue bloqueado (ilegalidad de contenido) y actuar además como un vehículo de prevención que recuerde al usuario/consumidor el carácter ilícito de los materiales, así como la presencia en línea de organismos encargados de la observancia de la ley.

El bloqueo del acceso a los sitios web y los *Usenet Newsgroups* con contenidos CAM puede ser una importante contribución a la interrupción y reducción del volumen de los contenidos que circulan o se distribuyen por Internet. Sin embargo, se reconoce que esto es solamente una parte de la solución y no se pretende que este enfoque sea la única solución. El objetivo es complementar los esfuerzos de los organismos responsables de hacer cumplir la ley y reducir la disponibilidad de CAM en línea. Los particulares que tengan un interés sexual en los niños y su-

ficientes conocimientos técnicos y determinación aún podrían ser capaces de localizar esos contenidos. No obstante, la interfaz de la web en particular es de tan fácil utilización por el usuario, motivo por el cual se ha transformado en una de las aplicaciones de Internet de uso más generalizado y más populares, que es esencial concebir métodos concretos para hacerle frente mientras se siguen evaluando nuevos métodos para reducir la distribución en otras plataformas de Internet.

Siempre hay que considerar la posibilidad de lanzar una campaña de concienciación mixta entre el gobierno y la industria destinada a los consumidores de CAM. Se les debe recordar a los usuarios/consumidores que los contenidos CAM representan un perjuicio real para niños reales y que la creación, posesión o distribución de CAM es ilícita en muchos países.

“A menudo los niños y jóvenes son particularmente vulnerables en línea ,”





4.

Principales riesgos para los menores en línea

Aunque los adultos y los niños están expuestos de igual modo a los riesgos y peligros en línea, con frecuencia los niños y los jóvenes son particularmente vulnerables. Los niños se encuentran aún en proceso de desarrollo y aprendizaje y ello incide en su capacidad para identificar, evaluar y manejar posibles riesgos. En la Convención de las Naciones Unidas sobre los Derechos del Niño²² está consignada la idea de que los niños son vulnerables y deben ser protegidos contra todas las formas de explotación.

La utilización de Internet por parte de niños y jóvenes plantea algunas cuestiones que suscitan una inquietud creciente en los padres y los propios niños, así como en los representantes gubernamentales, los políticos y la comunidad

encargada de formular políticas. Esas inquietudes pueden resumirse como sigue:

Contenido

- Capacidad de Internet para exponer a los niños y jóvenes a contenidos ilícitos, por ejemplo CAM.
- Capacidad de Internet para exponer a niños y jóvenes a contenidos legales pero inadecuados para su edad, por ejemplo imagería muy violenta.

²² <http://www.unhchr.ch/html/menu3/b/k2erc.htm>





Contacto

- Capacidad de Internet para exponer a niños y jóvenes a depredadores sexuales, ya sean éstos adultos u otros menores²³.
- Manera según la cual Internet puede exponer a los niños a comunidades dañinas en línea tales como sitios que fomentan la anorexia, la autoflagelación o el suicidio, así como fuentes de influencia política que preconizan la violencia, el odio y el extremismo político.

Conducta

- Manera según la cual Internet facilita y puede fomentar interacciones sexuales riesgosas entre los propios niños, en particular alentándolos a tomar y divulgar fotos de ellos mismos u otros (*sexting*) que, además de ser perjudiciales, también podrían ser ilícitas. El desarrollo sexual normal y la experimentación en línea a veces puede dar lugar a la producción y distribución

involuntarias de CAM que exponen a los niños y sus amigos a posibles sanciones legales o los obligan a tenerse las que ver con la parte árida del sistema de justicia penal.

- Manera según la cual algunos aspectos de Internet alienan a los niños a poner en dominio público información sobre ellos mismos, o difundir fotos o videos o textos que podrían comprometer su seguridad personal o poner en peligro alguna de sus opciones profesionales en el futuro.
- Capacidad de Internet para exponer a los niños y jóvenes a la intimidación y permitir o fomentar un entorno en el cual se les alienta a intimidar a otros.

Comercio

- Manera según la cual Internet ha permitido a los niños adquirir o acceder a bienes y servicios inapropiados para su edad, por lo general bienes y servicios que éstos

no podrían comprar personalmente en una tienda.

- Capacidad de Internet para exponer a los niños y jóvenes al correo basura, la usurpación de identidad, el fraude y amenazas similares que tienen carácter económico y están enraizadas en una protección insuficiente de los datos o leyes de privacidad inadecuadas.

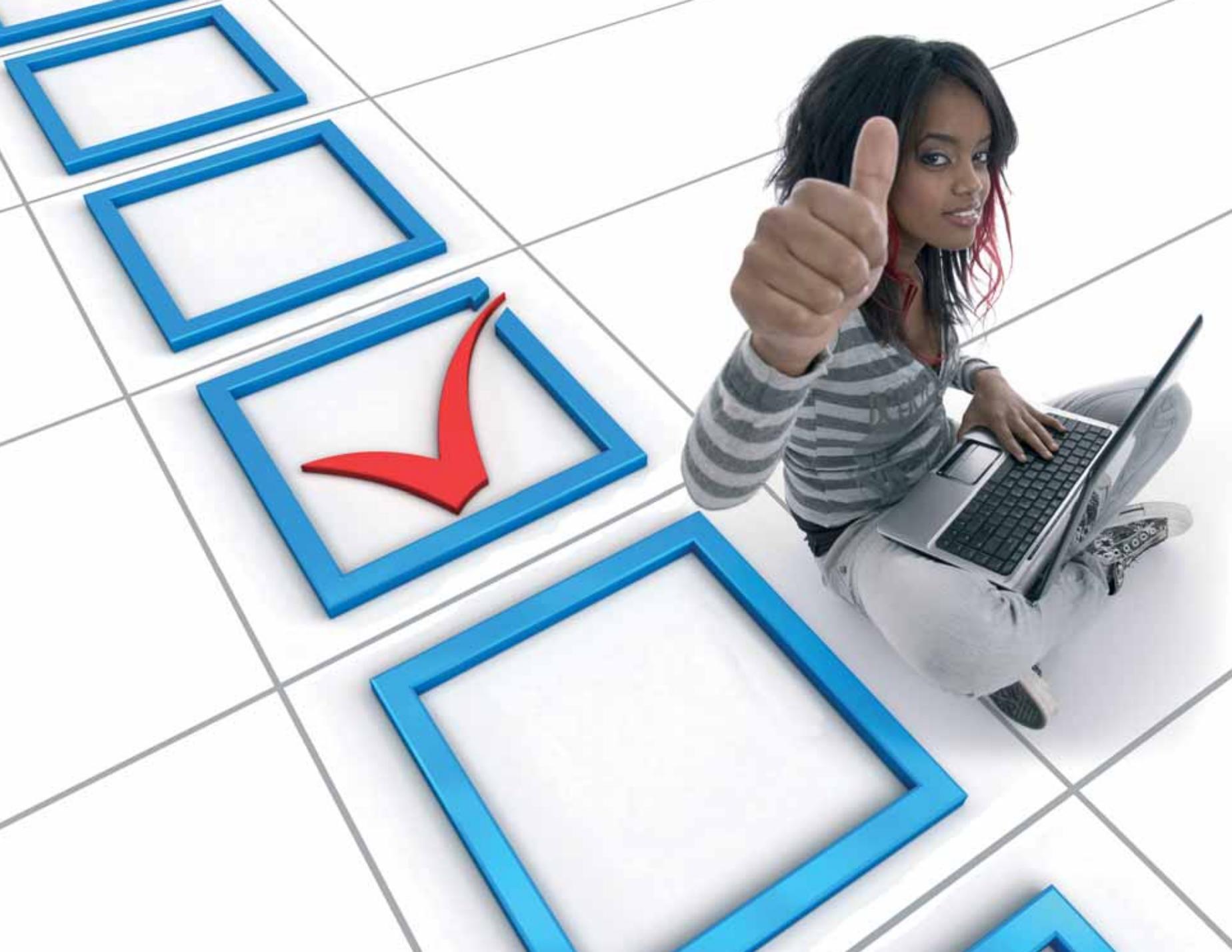
Uso excesivo

- Manera según la cual Internet parece haber alentado, en algunos niños y jóvenes, un comportamiento obsesivo o una utilización excesiva que podría tener efectos deletéreos en su salud o aptitudes sociales, cuando no en ambas cosas. Con frecuencia los juegos por Internet muestran comportamientos de este tipo en línea, lo que en algunos países se considera como una forma de adicción.

Efectos sociales

- Manera según la cual Internet ha creado una nueva brecha digital entre niños y jóvenes, a saber: entre los que tienen acceso cómodo e inmediato en el hogar, la escuela y cualquier otro sitio, y los que no lo tienen; entre los que son usuarios seguros y eficaces y los que no lo son. Estas disparidades amenazan con afianzar o ampliar las pautas actuales de ventaja y desventaja, o tal vez crear nuevas lagunas.
- Posibilidad de que Internet agrave o incluso magnifique las vulnerabilidades de ciertos niños y jóvenes y engrose las adversidades a las que éstos podrían tener que afrontar en el mundo real.

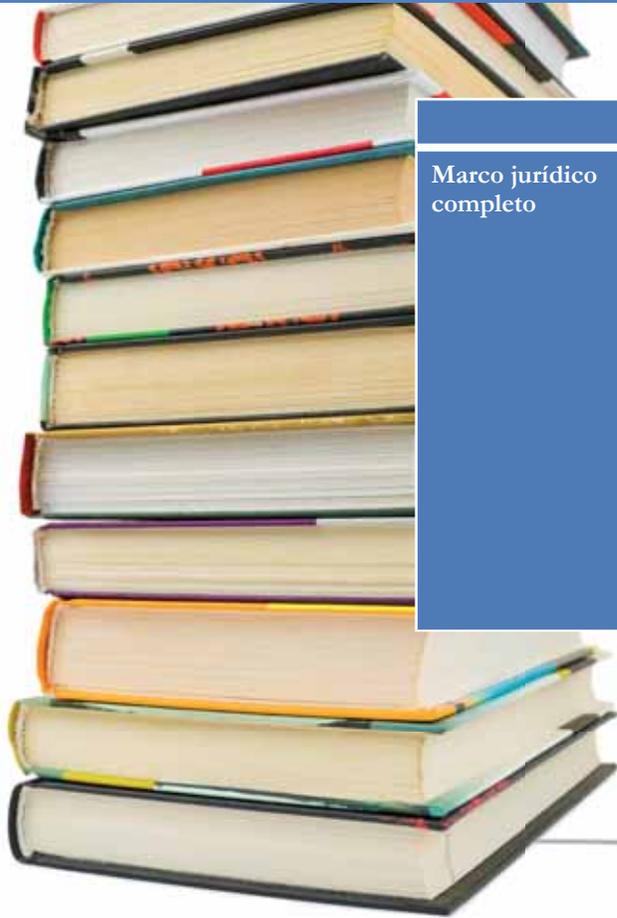
²³ Para un examen más detallado de este aspecto, véase el Apéndice 1.





5.

Soslayar los riesgos Una Lista de Actividades Nacionales



	#	Lista de actividades nacionales
Marco jurídico completo	1.	<p>En general será necesario que exista un acervo de leyes que deje en claro que todos y cada uno de los crímenes que pueden cometerse contra un niño en el mundo real también pueden, <i>mutatis mutandis</i>, cometerse por Internet o cualquier otra red electrónica.</p> <p>Asimismo, podría ser necesario promulgar nuevas leyes o adaptar las existentes para proscribir ciertos tipos de comportamiento que sólo pueden tener lugar por Internet, como por ejemplo, incitar a distancia a los niños para que realicen u observen actos sexuales, o “condicionar” (“grooming”) a los niños para reunirse con ellos en el mundo real con un propósito sexual.</p> <p>Además en general también será necesario que exista en un lugar un marco jurídico que proscriba la utilización indebida de computadores con fines delictivos, así como la piratería u otras modalidades de utilización maliciosas o no consensuales de códigos informáticos y dictamine que Internet es un lugar en el que se pueden cometer delitos.</p>





	#	Lista de actividades nacionales
<p>Necesidad de una convergencia en la protección de la infancia en línea a escala nacional</p>	2.	<p>Varios gobiernos han considerado útil agrupar a todos los principales interesados y agentes para centrarse en el desarrollo e implementación de una iniciativa nacional con la finalidad de transformar a Internet en un lugar más seguro para niños y jóvenes, promover la conciencia acerca de las cuestiones que ésta entraña y de cómo hacer frente a las mismas de una manera muy práctica.</p> <p>En el marco de esa estrategia, será importante advertir que actualmente se puede acceder a Internet por varios tipos diferentes de dispositivos, entre los cuales los computadores son sólo uno de los diversos medios de entrar en línea. Cada vez adquieren mayor importancia los teléfonos móviles, las consolas de juegos y los PDA. Es preciso lograr que participen los proveedores de acceso tanto alámbrico como inalámbrico. Además, en numerosos países la red de bibliotecas públicas, telecentros y cibercafé pueden ser importantes fuentes de acceso a Internet, en particular para niños y jóvenes.</p> <p>Algunos países han estimado ventajoso establecer un modelo de autorreglamentación o correglamentación en relación con el establecimiento de una política en este ámbito, y a través de esos modelos éstos han publicado, por ejemplo, códigos de buena conducta para orientar a la industria de Internet acerca de cuáles son las medidas que podrían dar mejor resultado para mantener la seguridad de los niños y jóvenes en línea. Esto también ha funcionado a nivel regional, por ejemplo en la Unión Europea, donde se han publicado códigos a nivel de toda la UE para sitios de interfuncionamiento social y redes de teléfonos móviles en relación con el suministro de contenidos y servicios para niños y jóvenes a través de sus redes. La autorreglamentación y la correglamentación también pueden ser un medio muy eficaz de lograr y mantener la participación de todos los interesados pertinentes, así como una forma muy eficaz para acelerar la velocidad con la que se formulan y se ponen en práctica medidas de respuesta adecuadas para los cambios tecnológicos.</p> <p>Las escuelas y el sistema educativo en general desempeñarán una función muy importante en el despliegue de esa estrategia nacional, pero también es necesario que ésta tenga un alcance más amplio.</p>

	#	Lista de actividades nacionales
Necesidad de una convergencia en la protección de la infancia en línea a escala nacional		Asimismo, se debería considerar la posibilidad de obtener la asistencia de los medios de comunicación masivos en la promoción de mensajes y campañas de concienciación
Necesidad de desarrollar los recursos locales en los que se reflejan las normas culturales locales y las leyes nacionales	3.	Muchas de las principales empresas de Internet crean sitios web que contienen gran cantidad de información sobre cuestiones en línea para niños y jóvenes. Sin embargo, muy a menudo estos materiales sólo están disponibles en inglés o en un número muy reducido de idiomas. Por lo tanto, es importante que se produzcan materiales a escala local en los cuales se reflejen las leyes locales así como las normas culturales locales. Este aspecto será esencial para cualquier campaña sobre seguridad de Internet o cualesquiera materiales de capacitación que se elaboren.
Necesidad de realizar actividades de concienciación y educación pública	4.	<p>Los padres, tutores y profesionales como los maestros deben desempeñar un papel cardinal a la hora de ayudar a mantener la seguridad de los niños y jóvenes en línea. Se deberían elaborar programas didácticos y de divulgación que ayuden a tomar conciencia de las cuestiones que están en juego y formular estrategias para hacer frente a las mismas.</p> <p>Al producir materiales didácticos es importante tener en cuenta que muchas personas que no conocen la tecnología no se sentirán muy cómodas al utilizarla. Ésta es la razón por la cual es importante velar por que se pongan a disposición materiales seguros en forma escrita o utilizando otros medios con los cuales los novatos se sientan más familiarizados, como por ejemplo el vídeo.</p> <p>En toda campaña de concienciación y educación será importante hacer hincapié en la tónica correcta. Se deben evitar los mensajes basados en el temor y conferir la debida preeminencia a los numerosos aspectos positivos y recreativos de las nuevas tecnologías. Internet encierra enormes posibilidades como un medio de capacitación de niños y jóvenes para que éstos descubran nuevos mundos. Un objetivo capital de los programas de educación y concienciación debe ser enseñar formas positivas y responsables de comportamiento en línea.</p>



	#	Lista de actividades nacionales
Necesidad de establecer mecanismos de notificación de comportamientos predatorios en línea, incluida la intimidación	5.	Se deberían publicitar y promover de manera generalizada, tanto en Internet como en otros medios de comunicación, mecanismos concebidos para notificar abusos de un servicio en línea o un comportamiento censurable o ilícito en línea, como por ejemplo una línea directa nacional. Se deberían mostrar abundantemente enlaces hacia mecanismos de notificación de abusos en las partes pertinentes de cualquier sitio web que autorice la aparición de contenidos generados por el usuario. Asimismo, debería ser posible que las personas que de algún modo se sientan amenazadas, o personas que hayan sido testigos de actividades inquietantes en Internet, puedan notificar al respecto lo más rápidamente posible a los correspondientes organismos encargados de hacer cumplir la ley, los cuales habrán recibido formación y estarán en condiciones de responder. El Grupo de Trabajo Global Virtual (<i>Virtual Global Taskforce</i>) es un órgano responsable de la observancia de la ley que ofrece un mecanismo que funciona las 24 horas los 7 días de la semana para recibir informes sobre contenidos o comportamientos ilícitos de personas que habitan en los Estados Unidos de América, Canadá, Australia e Italia, y se espera que a la brevedad se sumarán otros países. Véase www.virtualglobaltaskforce.com
Ayudar a los niños a mantenerse seguros gracias a la utilización de herramientas técnicas	6	<p>Hay algunos programas informáticos disponibles que pueden ayudar a excluir materiales no deseados o bloquear contactos no deseados. Algunos de estos programas de seguridad y filtrado pueden ser básicamente gratuitos, puesto que forman parte del sistema operativo del computador o se proporcionan como parte de un conjunto que puede solicitarse al PSI o PSE. Los fabricantes de algunas consolas de juegos también proporcionan instrumentos similares si el dispositivo funciona con Internet. Estos programas no ofrecen una garantía a toda prueba, pero pueden proporcionar un bienvenido nivel de apoyo, sobre todo en familias con niños pequeños.</p> <p>Estas herramientas técnicas se deberían utilizar como parte de un arsenal más amplio. Es indispensable la participación de los padres y/o tutores. A medida que los niños comienzan a crecer un poco aspiran a una mayor privacidad y sienten un deseo más fuerte de comenzar a explorar por sus propios medios. Además, cuando existe una relación de facturación entre el vendedor y el cliente, los procedimientos de verificación de la edad pueden desempeñar un papel muy útil para ayudar a los vendedores de bienes y servicios para consumo con limitación de edades o a los editores de materiales destinados únicamente para audiencias mayores de cierta edad a llegar a esos destinatarios específicos. Cuando no existen relaciones de facturación el uso de tecnologías que exigen la verificación de la edad puede plantear problemas o incluso en muchos países puede resultar imposible a causa de la falta de fuentes de datos fiables.</p>





6.

Partes interesadas

Al elaborar una estrategia nacional para promover la seguridad en línea de niños y jóvenes, los gobiernos y las instituciones responsables de formular políticas deben identificar a las principales partes interesadas y entablar contactos con las mismas.

Niños y jóvenes

Los niños y jóvenes de todo el mundo han demostrado que pueden adaptarse con gran facilidad a las nuevas tecnologías y utilizarlas. Internet adquiere cada vez mayor importancia en las escuelas y como un lugar en el cual los niños y jóvenes pueden trabajar, jugar y comunicarse.

La mayoría de los niños y jóvenes no tienen miedo a Internet y se sienten cómodos utilizando diferentes dispositivos que actualmente pueden ofrecer acceso a la red; con frecuencia saben más de

informática y de Internet que sus padres o profesores.

Pero conocimiento no significa sabiduría: su falta de experiencia del mundo en general los hace vulnerables a una serie de riesgos. Éstos tienen derecho a esperar que se les brinde ayuda y protección. También es importante recordar que las vivencias de Internet o de las nuevas tecnologías que tienen todos los niños y jóvenes difieren. Algunos niños con necesidades especiales provocadas por discapacidad física o de otro tipo podrían ser particularmente vulnerables a un entorno en línea y por consiguiente necesitan apoyo adicional.

Las encuestas realizadas han demostrado reiteradamente que existe una gran diferencia entre lo que los adultos piensan que hacen los niños y jóvenes en línea

yo que realmente ocurre. Por esta razón, además de otras, es importante velar por que en los acuerdos concertados a escala nacional para establecer políticas en este ámbito se incluyan mecanismos adecuados para que se pueda oír la voz de todos los niños y jóvenes y se tengan en cuenta sus experiencias concretas en el uso de la tecnología.

Padres, tutores y pedagogos

Una de las razones por las cuales muchos padres están comprando ordenadores con acceso a Internet para el hogar es contribuir a la educación de sus niños y ayudarles a cumplir sus deberes escolares. Así pues, las escuelas tienen la responsabilidad particular de enseñar a los niños cómo permanecer seguros en línea, ya estén utilizando Internet en la escuela, en el hogar o en cualquier otro sitio. Para que los profesores estén en condiciones de hacerlo, éstos necesitan a su vez que se les imparta formación sobre recursos de enseñanza actualizados de primera clase.

Los padres y tutores siempre serán la primera y más sólida defensa y apoyo para sus propios niños, pero sin embargo cuando se trata de Internet éstos pueden sentirse un poco perdidos. Las escuelas pueden actuar una vez más en este contexto como un canal importante para llegar a los padres y tutores, ponerlos en conocimiento de los riesgos y de las numerosas posibilidades positivas que ofrecen las nuevas tecnologías. No obstante, las escuelas no deben ser la única ruta que se toma para llegar a los padres y tutores, sino que es importante utilizar diferentes canales con miras a aumentar al máximo la posibilidad de llegar al mayor número posible de padres y tutores. Las bibliotecas públicas, los centros de salud, e incluso los grandes almacenes y otros importantes centros de venta al por menor pueden ofrecer vías accesibles para la difusión de informaciones sobre seguridad.

Sector industrial

Evidentemente las empresas que están desarrollando o proporcionando productos y servicios basados en nuevas tecnologías se encontrarán en un lugar ideal para ayudar a otras partes interesadas a comprender cómo éstos funcionan y cómo utilizarlos de una manera segura y apropiada. Ésta es la razón por la cual es importante participar con el sector empresarial para alentar a las empresas a compartir sus conocimientos y experiencia.

El sector industrial también tiene la importante responsabilidad de ayudar a promover la conciencia acerca del programa de seguridad en línea, particularmente entre niños y jóvenes y sus padres o tutores, pero también entre la comunidad en general. Al participar de este modo, el sector industrial podrá aprender más acerca de las inquietudes de las diferentes partes interesadas y esos conocimientos le ayudarán a identificar los peligros de los nuevos productos o servicios que están desarrollando, gracias a lo cual podrán corregir los existentes.

En algunos países Internet está regida por un marco de autorregulación o corregulación. Esto puede hacer que se escuche la voz de la industria de Internet al elaborar políticas públicas y garantizar a su vez que esas políticas tengan un fundamento técnicamente sólido. Ello significa asimismo que, a medida que las tecnologías evolucionan, se pueden introducir ajustes en la práctica con gran rapidez sin tener que esperar los procesos a veces prolongados que entrañan el diseño y la promulgación de nuevas leyes. Al tiempo que se acoge con agrado la participación de la industria para ayudar a promover una mejor comprensión de las cuestiones relativas a la seguridad en línea, también será importante que los gobiernos nacionales y demás partes de la comunidad responsable de formular políticas tengan sus propias fuentes independientes de asesoramiento.



La comunidad de instituciones de investigación y ONG

En las universidades y otras partes de la comunidad de investigación es muy probable que haya personas instruidas y eruditos con un interés profesional en los aspectos sociales y técnicos y las repercusiones de Internet, y con un conocimiento muy detallado de todos esos aspectos. Éstos pueden ser una fuente muy valiosa de asistencia para los gobiernos nacionales y los encargados de formular políticas a la hora de elaborar estrategias basadas en hechos concretos y evidencias fidedignas. Asimismo, éstos podrían actuar como un contrapeso intelectual para las empresas de alta tecnología cuyos intereses a veces pueden ser a corto plazo y de un carácter predominantemente comercial.

De manera similar, dentro de la comunidad de las ONG con frecuencia podrá encontrarse un acervo de competencia técnica e información que puede ser un

recurso inapreciable para llegar a los niños, jóvenes, padres, tutores y educadores y proporcionarles servicios con el fin de promover el programa de seguridad en línea.

Observancia de la ley

Triste es advertir que, por maravillosa que sea la tecnología, ésta también ha atraído la atención de elementos delictivos y antisociales. Internet ha contribuido a aumentar en gran medida la circulación de CAM. Los depredadores sexuales han utilizado Internet para entablar un contacto inicial con niños y jóvenes, seduciéndolos hacia formas de contacto muy dañinas, tanto en línea como fuera de ésta. La intimidación y otras formas de acoso pueden ser muy perjudiciales para la vida de niños y jóvenes, e Internet ha proporcionado una nueva forma de hacerlo.

Éstas son las razones por las cuales es indispensable que la comunidad encargada de hacer cumplir la ley participe plenamente en toda estrategia general

encaminada a lograr que Internet sea más segura para niños y jóvenes. Los oficiales responsables de la observancia de la ley deben recibir una formación adecuada para efectuar investigaciones sobre delitos contra niños y jóvenes relacionados con Internet. Éstos deben poseer el nivel adecuado de conocimientos técnicos y tener acceso a instalaciones forenses que les permitan extraer e interpretar los datos obtenidos de los computadores o de Internet.

Además, es muy importante que los responsables de hacer cumplir la ley establezcan mecanismos claros para permitir a los niños y jóvenes, o a cualquier miembro del público, notificar cualesquiera incidentes o inquietudes que pudieren tener respecto de la seguridad de niños o jóvenes en línea. Muchos países han creado por ejemplo líneas directas para facilitar la notificación de CAM y mecanismos especializados similares para facilitar la comunicación de otros tipos de problemas, por ejemplo la intimidación y otras modalidades de comportamiento amenazador.

El cumplimiento de la ley es la principal fuente de CAM incautados dentro de las fronteras nacionales. Es necesario establecer un mecanismo para examinar estos materiales con miras a determinar si se pueden o no identificar las víctimas locales. Cuando ello no sea posible esos materiales deben remitirse a INTERPOL para su inclusión en la base de datos ICSE.

Servicios sociales

Es probable que los niños o jóvenes que hayan sido perjudicados o injuriados en línea, por ejemplo al publicar una fotografía inadecuada o ilícita de los mismos, necesiten apoyo o consejo especializado y a largo plazo. Es preciso impartir una formación adecuada a los profesionales dedicados a la prestación de servicios sociales para que éstos les ofrezcan el tipo de apoyo que necesitan.





7

Conclusión

Actualmente Internet es un nexo indispensable para todo un conjunto de tecnologías digitales que están transformando la economía, abriendo una serie de nuevas posibilidades para mejorar el nivel de vida de las personas y enriquecer las sociedades de diversas maneras.

A nivel macroeconómico, es sumamente importante el hecho de que las ventajas económicas que puede generar Internet están distribuidas de una manera uniforme en todo el mundo. Durante el proceso de la CMSI se abordó la perspectiva de una brecha digital creciente entre el mundo industrializado y los países en desarrollo, que afianza o amplía las desventajas o los desequilibrios existentes. Esa brecha sigue siendo un tema cardinal de los debates de política entablados en el Foro de la CMSI²⁴, el Foro sobre

Gobernanza Internet (FGI)²⁵ y en muchos otros foros internacionales conexos.

A nivel individual, Internet ha pasado a ser una tecnología tremendamente enriquecedora y capacitante. Los niños y los jóvenes en particular han sido uno de los principales beneficiarios de Internet y de las tecnologías digitales asociadas. Dichas tecnologías están transformando el modo según el cual nos comunicamos todos entre nosotros y ha creado muchas nuevas modalidades para jugar, disfrutar la música o participar en un amplio abanico de actividades culturales, disolviendo numerosas barreras de tiempo y espacio. Con mucha frecuencia los niños y los jóvenes han marchado a la vanguardia en cuanto a la adopción de las posibilidades que ofrece Internet o su adaptación a las mismas.

²⁴ <http://www.itu.int/wsis/implementation/2009/forum/geneva/index.html>

²⁵ www.intgovforum.org

No obstante, es innegable que Internet ha traído consigo una serie de problemas para la seguridad de los niños y jóvenes que es preciso abordar, no sólo porque éstos son importantes por propio derecho sino también porque es importante comunicar a cualquier persona interesada que Internet es un medio en el que debemos poder confiar. Es igualmente esencial que, colectivamente, no permitamos que una aparente inquietud por proteger a los jóvenes y niños en línea se transforme en una plataforma para justificar ataques a la libertad de palabra, la libre expresión o la libertad de asociación que no guardan ninguna relación con esos problemas.

Es extremadamente importante que la próxima generación sienta confianza en la utilización de Internet para que éstos puedan, a su vez, seguir beneficiándose de su desarrollo. Así pues, al considerar la seguridad de niños y jóvenes en línea, es vital llegar a un equilibrio.

Es esencial discutir abiertamente los peligros que existen para los jóvenes y niños en línea, de modo que podamos enseñarles a evitar los riesgos completamente o a hacerles frente en caso de que a pesar de todo éstos se materialicen, pero no debemos hacerlo de una manera que exagere los peligros o que cree miedos infundados. Es muy poco probable que los niños y jóvenes tomen en serio un enfoque que se detenga únicamente o en su mayor parte en los aspectos negativos de la tecnología, puesto que cientos de millones de ellos ya la están utilizando diariamente y por lo tanto saben bastante lo que es y lo que puede ser. En este sentido, los padres y los miembros de generaciones mayores pueden encontrarse a menudo en una situación de desventaja. Se trata de una instancia en la cual muy a menudo los jóvenes saben más acerca de la tecnología y sus posibilidades que sus padres y profesores; pero conocimiento no es lo mismo que sabiduría.

Los gobiernos nacionales tienen la obligación de disponer lo necesario para proteger a los menores de edad tanto en el mundo “real” como en el “virtual”. En buena medida ya no tiene sentido tratar de mantener una distinción rígida entre los eventos “del mundo real” y los eventos en línea, pues hoy en día las nuevas tecnologías se encuentran absolutamente integradas en la vida de incontables niños y jóvenes de diversas formas importantes. Ambos mundos están cada vez más entrelazados y son cada vez más interdependientes.

Los gobiernos nacionales y la comunidad responsable de formular políticas tienen la enorme responsabilidad de establecer un marco dentro del cual se pueda diseñar una respuesta nacional y multinacional adecuada y luego mantenerla en vigor con el correr del tiempo. Al actuar de este modo, la propia industria de Internet y todos los demás interesados

pertinentes estarán desempeñando un papel muy importante, aunque más no sea porque a causa de la velocidad con la cual puede evolucionar la tecnología, muchos de los métodos tradicionales de elaboración de políticas o leyes tal vez ya no se ajusten a esta finalidad. Como se ha demostrado en el presente Informe, las nuevas tecnologías también están imponiendo nuevos requisitos a los legisladores.



Apéndice 1

Contactos delictivos contra niños y jóvenes

Los niños y jóvenes pueden estar expuestos a toda una gama de contactos no deseados o inapropiados en Internet que podrían tener consecuencias desastrosas para ellos. Algunos de esos contactos pueden ser de carácter sexual.

Los estudios realizados en Europa por *EU Kids Online* en 2008 revelan algunos resultados perturbadores (cifras promediadas): 15-20% han sido intimidados, acosados o acechados en línea; 25% han recibido comentarios sexuales indeseables; 9% se han reunido con personas en la vida real que previamente sólo habían conocido en línea. Aunque las tasas varían de un país y región a otros, estas cifras demuestran que los riesgos son reales²⁶. De un estudio realizado por American Internet²⁷ se desprende que

el 32% de los adolescentes en línea han sido abordados por un perfecto extraño, de los cuales el 23% dijo que había tenido miedo y se había sentido incómodo durante ese contacto y el 4% declaró haber recibido propuestas sexuales agresivas.

Los depredadores sexuales utilizan Internet para ponerse en contacto con niños y jóvenes con fines sexuales, a menudo utilizando una técnica conocida como “condicionamiento” (“grooming”), con la cual van ganando su confianza al hablarles de sus propios intereses. Con frecuencia introducen temas, fotos y expresiones explícitamente sexuales para desensibilizarlos, despertar su conciencia sexual y ablandar la voluntad de sus jóvenes víctimas. Se utilizan como señuelo regalos, dinero e incluso billetes de trans-

porte para persuadir al menor de que vaya a un sitio en el cual el depredador pueda explotarlo/a sexualmente. Estos encuentros pueden incluso ser fotografiados o filmados en vídeo. Los niños y jóvenes a menudo carecen de madurez emocional y autoestima, lo que los hace susceptibles a la manipulación e intimidación. Éstos también dudan de contarles acerca de estos encuentros a adultos por temor de sentirse avergonzados o de que se les niegue el acceso a Internet. En algunos casos éstos son amenazados por los depredadores, quienes les dicen que deben mantener la relación en secreto.

Los depredadores sexuales aprenden de su experiencia recíproca en las salas de conversación y foros de Internet. Cuando se comunican con niños y jóvenes, estos

²⁶ EU Kids Online Report, *Comparing Children's Online Opportunities and Risks Across Europe*, páginas 29-30, junio de 2008.

²⁷ *Pew Internet and American Life Project 2007*.

depredadores a menudo pretenden tener una edad más próxima de la real a la del niño o joven y declaran que están buscando amistad. Una vez que ganan la confianza del menor, aprovechan sus vulnerabilidades —por ejemplo la soledad o la turbación por una pérdida personal— para crearle una dependencia emocional. Hay numerosos informes de los medios de comunicación sobre casos en los cuales niños o jóvenes convinieron en reunirse personalmente con alguien con quien habían estado conversando en línea y que creían se hallaba dentro de su mismo grupo de edad, para darse cuenta de que el individuo en cuestión era un hombre mayor interesado en mantener relaciones sexuales. Desgraciadamente algunos de esos casos terminaron en el engaño del niño y en su manipulación sexual, y en unos pocos casos los resultados fueron mucho peores.

Una tendencia particularmente preocupante de los depredadores es la de difundir por la web actos sexuales con niños o jóvenes en tiempo real a una audiencia formada por otros depredadores,

a menudo para solicitar su aprobación. En tales casos, el niño o joven no sólo sufre perjuicios y tramas psicológicos duraderos (y a veces incluso físicos) de esos actos odiosos, sino que padece como víctima repetidas veces a causa de la publicación de las imágenes en Internet, donde éstas se transforman en objetos de colección para otros depredadores. Estas nuevas imágenes son bienvenidas y se utilizan, intercambian y en ocasiones venden en Internet a otros depredadores que necesitan nuevos materiales para satisfacer sus fantasías sexuales. Lamentablemente, con frecuencia las víctimas no son capaces de dar vuelta a la página y volver a recomenzar su vida, incluso mucho tiempo después de que han ocurrido estos horribles eventos, puesto que viven en el miedo constante de que su imagen sea reconocida por otros. Aún más despreciable es la utilización de esas imágenes por el depredador para “chantajear” al niño o joven con el fin de obligarlo a mantener silencio y acceder a la continuación de los abusos.





Apéndice 2

“Pornografía infantil: legislación modelo y análisis mundial”

Con el apoyo de Interpol y Microsoft, el *International Centre for Missing & Exploited Children* (ICMEC) analizó la legislación sobre pornografía infantil de los 187 países miembros de Interpol y formuló recomendaciones sobre algunos conceptos cardinales que, al ser aplicados en la legislación nacional, constituirían una estrategia legislativa completa para luchar contra la pornografía infantil.

Por desgracia, en el informe se llega a la conclusión²⁸ de que pocos países en el mundo tienen una

legislación suficientemente sólida como para combatir la pornografía infantil a algún nivel.

El informe completo, que actualmente ya se ha publicado en su quinta edición, puede consultarse en www.icmec.org en los idiomas árabe, inglés, francés, coreano, portugués, ruso, español, tailandés y turco²⁹.

A continuación figura una lista de los países miembros de Interpol y el estado de su legislación sobre pornografía infantil.

²⁸ En el informe se llega a la conclusión de que:

- ✓ sólo 29 países tienen una legislación suficiente como para combatir los delitos de pornografía infantil (cinco países miembros de Interpol cumplen con todos los criterios antes expuestos y 24 países miembros de Interpol cumplen con todos los criterios salvo el último, es decir la notificación por parte de los PSD);
- ✓ 93 países miembros de Interpol no disponen de una legislación en la que se aborde específicamente la pornografía infantil.

De los países miembros de Interpol restantes que tienen una legislación específica sobre pornografía infantil:

- en la legislación nacional de 54 países no está definida la pornografía infantil;
- en la legislación de 24 países no se prevén explícitamente los delitos facilitados por ordenador; y
- en la legislación de 36 países no se penaliza la posesión de pornografía infantil, y ello independientemente de la intención de distribuirla.

²⁹ www.icmec.org

Análisis mundial

(Nueva publicación con el permiso del *International Centre for Missing & Exploited Children*)

✘ = No ✔ = Sí

País	Legislación específica sobre pornografía infantil ³⁰	En la legislación está definida la “pornografía infantil”	Delitos facilitados por ordenador ³¹	Simple posesión ³²	Obligación de notificación por parte de los PSI ³³
Afganistán	✘	✘	✘	✘	✘
Albania	✘	✘	✘	✘	✘
Argelia	✘	✘	✘	✘	✘
Andorra	✔	✘	✘	✔	✘
Angola	✘	✘	✘	✘	✘

³⁰ A los efectos del presente Informe, tratamos de encontrar leyes específicas que proscriban y/o penalicen los delitos de pornografía infantil. La mera legislación laboral que sencillamente prohíbe las “peores formas de labor infantil”, entre las cuales figura la pornografía infantil, no se considera “legislación específica sobre pornografía infantil”.

Además, en los países en los cuales existe una prohibición general de la pornografía, independientemente de que los actores sean adultos o niños, no se considera “legislación específica sobre pornografía infantil” a menos que se prevea una sentencia agravada por los delitos cometidos contra una víctima menor de edad.

³¹ Para que un delito sea considerado facilitado por ordenador, intentamos encontrar una mención específica de un ordenador, un sistema informático, Internet o alguna expresión similar (incluso si se menciona una “imagen informática” o algo similar en la definición de “pornografía infantil”). En los casos en los cuales se utiliza otro lenguaje en la legislación nacional, se proporciona una nota explicativa.

³² A los efectos del presente Informe, se entiende por “simple posesión” la posesión independientemente de la intención de distribuir los materiales.

³³ Si bien algunos países pueden haber promulgado leyes generales sobre la obligación de notificación (es decir, cualquier persona con conocimiento de un delito debe notificar dicho delito a las correspondientes autoridades), únicamente los países que le exigen concretamente a los PSI que notifiquen presuntos casos de pornografía infantil a las autoridades responsables de hacer cumplir la ley (u a otro organismo encomendado) están considerados como países cuya ley obliga a los PSI a notificar al respecto. Cabe señalar que algunas leyes nacionales también contienen disposiciones (particularmente dentro de la Unión Europea) que limitan la responsabilidad de los PSI en la medida en que un PSI suprima los contenidos ilícitos una vez que se entera de su presencia; no obstante, dicha legislación no está contemplada en esta sección.



País	Legislación específica sobre pornografía infantil	En la legislación está definida la “pornografía infantil”	Delitos facilitados por ordenador	Simple posesión	Obligación de notificación por parte de los PSI
Antigua y Barbuda	✗	✗	✗	✗	✗
Argentina	✓	✓	✓	✗	✗
Armenia	✓	✗	✓	✗	✗
Aruba	✓	✗	✓	✓	✗
Australia	✓	✓	✓	✓	✓
Austria	✓	✓	✓ ³⁴	✓	✗
Azerbaiyán	✗	✗	✗	✗	✗
Bahamas	✗	✗	✗	✗	✗
Bahrein	✗	✗	✗	✗	✗
Bangladesh	✗	✗	✗	✗	✗
Barbados	✓	✗	✗	✓	✗

³⁴ En la sección 207a(1)(3) del Código Penal Austríaco se penaliza el acto de “poner a disposición de cualquier otra manera... una descripción pornográfica de un menor”. *Negritas añadidas.*

País	Legislación específica sobre pornografía infantil	En la legislación está definida la “pornografía infantil”	Delitos facilitados por ordenador	Simple posesión	Obligación de notificación por parte de los PSI
Belarús	✓	✗	✗	✗	✗
Bélgica	✓	✓	✓ ³⁵	✓	✓
Belice	✗	✗	✗	✗	✗
Benín	✗	✗	✗	✗	✗
Bhután	✓	✗	✓ ³⁶	✗	✗
Bolivia	✗	✗	✗	✗	✗
Bosnia y Herzegovina	✓	✗	✓ ³⁷	✓	✗
Botswana	✗	✗	✗	✗	✗
Brasil	✓	✓	✓	✓	✗

³⁵ En el Artículo 383bis del Código Penal belga, en su forma enmendada del 1 de abril de 2001, se penaliza, entre otras cosas, la divulgación de pornografía infantil, incluyendo en ésta la difusión por ordenador. Carta de Jan Luyckx, Jefe Adjunto de Misión, Embajada de Bélgica, Washington, D.C., dirigida a Ernie Allen, Presidente y Director General del *International Centre for Missing & Exploited Children* (24 de febrero de 2006) (en los archivos del mencionado Centro).

³⁶ De conformidad con el Artículo 225b) del Código Penal de Bhután, “un acusado será culpable del delito de pedofilia si éste... vende, fabrica, distribuye o **efectúa algún otro tipo de transacción** con materiales que contengan cualquier descripción de un menor realizando un acto sexual”. *Negritas añadidas*.

³⁷ En los Artículos 189 y 211 del Código Penal de Bosnia y Herzegovina se hace referencia a “otros materiales pornográficos”, además de las fotografías y las videocasetes.



País	Legislación específica sobre pornografía infantil	En la legislación está definida la “pornografía infantil”	Delitos facilitados por ordenador	Simple posesión	Obligación de notificación por parte de los PSI
Brunei	✓	✗	✓	✗	✗ ³⁸
Bulgaria	✓	✗	✓ ³⁹	✓	✗
Burkina Faso	✗	✗	✗	✗	✗
Burundi	✗	✗	✗	✗	✗
Camboya	✗	✗	✗	✗	✗
Camerún	✗	✗	✗	✗	✗

³⁸ Conforme a la Legislación de Brunei, aunque ésta carece de un requisito obligatorio de notificación por parte del PSI, todos los PSI y proveedores de contenidos Internet (PCI) titulares de una licencia a tenor de la notificación de radiodifusión (licencia de clase) de 2001 deben observar el código de conducta consignado en la Ley de Radiodifusión (Cap. 181). Los PSI y los PCI deben presentar pruebas satisfactorias al Ministro responsable de asuntos relativos a la radiodifusión en el sentido de que han tomado medidas responsables para cumplir con este requisito. De conformidad con la Ley de Radiodifusión, el Ministro está facultado para imponer sanciones. Entre los contenidos no autorizados figuran, entre otros, aquellos en los cuales se describe o propaga la pedofilia.

El titular de la licencia debe suprimir o prohibir la difusión de la totalidad o cualquier parte de un programa incluido en su servicio si el Ministro le informa que la difusión de la totalidad o una parte de ese programa está en contravención con el código de conducta aplicable al titular de la licencia, o si el programa está en pugna con el interés público, el orden público o la armonía nacional, o constituye una ofensa al buen gusto o la decencia.

El titular de la licencia también debe prestar asistencia al Ministro responsable de la radiodifusión en la investigación de cualquier violación de lo dispuesto en su licencia o cualquier presunta violación de cualquier ley cometida por el titular de la licencia o cualquier otra persona, y también debe proporcionar la información, registros, documentos, datos u otros materiales que pudiere necesitar el Ministro a los efectos de la investigación. Correo electrónico de Salmaya Salleh, Subsecretario, Embajada de Brunei, Washington, D.C., a Jessica Sarra, Directora de *Global Operations, International Centre for Missing & Exploited Children* (21 de marzo de 2006) (en los archivos del mencionado Centro).

³⁹ En el Artículo 159(3) del Código Penal búlgaro, cuando éste se lee junto con el Artículo 159(1), se penaliza, entre otras cosas, el acto de “**hacer circular de otro modo** trabajos con contenido pornográfico [con menores]”. *Negritas añadidas.*

País	Legislación específica sobre pornografía infantil	En la legislación está definida la “pornografía infantil”	Delitos facilitados por ordenador	Simple posesión	Obligación de notificación por parte de los PSI
Canadá	✓	✓	✓	✓	✗ ⁴⁰
Cabo Verde	✓	✗	✗	✗	✗
República Centroafricana	✗	✗	✗	✗	✗
Chad	✗	✗	✗	✗	✗
Chile	✓	✓	✓	✗	✗

⁴⁰ Aunque en Canadá no se ha impuesto ninguna obligación específica de notificación a los PSI, éstos deben colaborar con los responsables de hacer cumplir la ley y trabajar en estrecha cooperación para facilitar la notificación de existencia de material ofensivo. En el derecho penal de Canadá se utiliza una definición muy amplia de “pornografía infantil”, que le da un alcance adicional a todo su conjunto de delitos. En 2002, se agregaron los delitos concretos de transmitir, poner a disposición y facilitar el acceso, para considerar el contexto de Internet, y éste se aplicaría a las actividades de los PSI. En esa misma legislación, Canadá también introdujo una disposición sobre “notificación y supresión” de la pornografía infantil encontrada en Internet. Las penas por delitos de pornografía infantil fueron promulgadas en 2005, mediante la imposición de penas mínimas obligatorias; un aumento de la pena máxima por convicción sumaria de 6 a 18 meses de prisión; haciendo de la perpetración de un delito de pornografía infantil con la intención de sacar provecho un factor agravante a los efectos de la sentencia; haciendo de la denuncia y la disuasión los principales objetivos de la sentencia en cualquier caso que entrañe el abuso de un menor; y haciendo del abuso de cualquier niño un factor agravante a los efectos de la sentencia. Además de la protección cabal conferida a tenor del derecho penal, Canadá también cuenta con una página web pública nacional para la notificación de casos de explotación sexual infantil en línea (<http://www.Cybertip.ca>) en la que se efectúa una selección de esas notificaciones para los organismos encargados de la observancia de la ley. Adicionalmente, Cybertip.ca también mantiene la base de datos *Project Cleanfeed* Canadá, la cual le bloquea a aproximadamente el 90% de los abonados canadienses el acceso a sitios conocidos de pornografía infantil que podrían estar más allá del alcance de la fiscalización canadiense. Por otro lado, Canadá ha formulado una Estrategia Nacional para la protección de menores contra la explotación sexual en Internet, de la cual es un componente clave el Centro Nacional de Coordinación contra la Explotación Infantil. Este Centro, que está situado en los locales de la *Royal Canadian Mounted Police*, coordina las investigaciones nacionales y extranjeras sobre explotación sexual infantil en línea, imparte formación a los funcionarios encargados de la observancia de la ley canadiense y actúa como un centro de intercambio de información sobre las notificaciones recibidas de Cybertip.ca. Resumen de una carta de Carole Morency, Consejera General Adjunta, Sección de Política de Derecho Penal, Departamento de Justicia de Canadá, dirigida a Jessica Sarra, Directora de *Global Operations, International Centre for Missing & Exploited Children* (24 de junio de 2008) (el texto completo de esta carta figura en los archivos del Centro).

País	Legislación específica sobre pornografía infantil	En la legislación está definida la “pornografía infantil”	Delitos facilitados por ordenador	Simple posesión	Obligación de notificación por parte de los PSI
China ⁴¹	✓ ⁴²	✗	✓ ⁴³	✗	✗
Colombia	✓	✓	✓	✗	✓
Comoras	✗	✗	✗	✗	✗
Congo	✗	✗	✗	✗	✗
Costa Rica	✓	✓	✗	✓	✗
Côte d’Ivoire	✗	✗	✗	✗	✗
Croacia	✓	✗	✓	✓	✗

⁴¹ La legislación sobre pornografía infantil de Hong Kong es diferente de la de China, por cuanto en la primera:

- se define la pornografía infantil;
- se penalizan los delitos facilitados por ordenador;
- se penaliza la simple posesión de pornografía infantil.

⁴² Aunque China no ha promulgado ninguna ley específica sobre pornografía infantil, en el Código Penal se estipula una prohibición general de materiales obscenos y pornográficos. Con el fin de proteger mejor a los menores, en 2004 la Corte Popular Suprema y el Protectorado Popular Supremo promulgaron una “Interpretación de diversas cuestiones relacionadas con la implementación de leyes sobre casos delictivos que entrañan la producción, duplicación, publicación, venta, divulgación de información electrónica pornográfica utilizando Internet, terminales de comunicaciones móviles y estaciones radioeléctricas”. El Artículo 6 de esta Interpretación estipula explícitamente que “toda persona que divulgue, duplique, publique o venda información electrónica pornográfica en la que se describan comportamientos sexuales de adolescentes menores de 18 años o proporcione enlaces directos en el servidor de Internet o en los sitios web de su propiedad o gestionados o utilizados por esa persona con información electrónica, a sabiendas de que en dicha información se describen comportamientos sexuales de adolescentes menores de 18 años, será penalizado severamente de conformidad con el Artículo 363 de la legislación penal que regula el castigo del delito de producción, duplicación, publicación, venta y divulgación de materiales pornográficos, o el Artículo 364 relativo al castigo de delitos de divulgación de materiales pornográficos con circunstancias agravantes”. Correo electrónico de Chen Feng, Encargado de Coordinación Policial, Embajada de la República Popular de China, Washington, D.C., dirigido a Jessica Sarra, Directora de *Global Operations, International Centre for Missing & Exploited Children* (17 de marzo de 2006) (en los archivos del mencionado Centro).

⁴³ La Interpretación de la Corte Popular Suprema y del Protectorado Popular Supremo de 2004 se aplica a los delitos facilitados por ordenador.

País	Legislación específica sobre pornografía infantil	En la legislación está definida la “pornografía infantil”	Delitos facilitados por ordenador	Simple posesión	Obligación de notificación por parte de los PSI
Cuba	✗	✗	✗	✗	✗
Chipre	✓	✓	✓	✓	✗
República Checa	✓	✗	✓	✓	✗ ⁴⁴
República Democrática del Congo	✗	✗	✗	✗	✗
Dinamarca	✓	✓	✓ ⁴⁵	✓	✗
Djibouti	✗	✗	✗	✗	✗
Dominica	✗	✗	✗	✗	✗
República Dominicana	✓	✓	✓	✓	✗
Ecuador	✓	✗	✗	✗	✗
Egipto	✓	✗	✓	✓	✗

⁴⁴ Aunque la Ley checa no contiene ningún requisito obligatorio de notificación por parte de los PSI, en el Plan Nacional checo para la lucha contra la explotación sexual de menores con fines comerciales, disponible en línea en: http://www.mvcr.cz/prevence/priority/kszd/en_tab.html, se designa al Ministerio de Transporte y Comunicaciones y al Ministerio del Interior como organismos nacionales encargados de especificar la obligación estatutaria de los proveedores de Internet incluidos en la Ley de Telecomunicaciones (Nº 151/2000) de transmitir los datos necesarios sobre sitios web ilícitos al organismo checo encargado de la observancia de la ley. El resultado previsto de esta medida es obtener “evidencias fácticas contra aquellas personas que propagan pornografía infantil en Internet”.

⁴⁵ En la sección 235 del Código Penal danés se penalizan, entre otras cosas, la divulgación y posesión de “otras... reproducciones visuales” de materiales pornográficos relacionados con menores de 18 años de edad.

País	Legislación específica sobre pornografía infantil	En la legislación está definida la “pornografía infantil”	Delitos facilitados por ordenador	Simple posesión	Obligación de notificación por parte de los PSI
El Salvador	✓	✗	✓	✓	✗
Guinea Ecuatorial	✗	✗	✗	✗	✗
Eritrea	✗	✗	✗	✗	✗
Estonia	✓	✗	✓ ⁴⁶	✓	✗
Etiopía	✗	✗	✗	✗	✗
Fiji	✗	✗	✗	✗	✗
Finlandia	✓	✓	✓ ⁴⁷	✓	✗
Francia	✓	✓	✓	✓	✓
Gabón	✗	✗	✗	✗	✗
Gambia	✓	✗	✗	✗	✗
Georgia	✓	✓	✗	✗	✗

⁴⁶ Los Artículos 177 y 178 del Código Penal estoniano penalizan la utilización de un menor en “otros trabajos” o “de cualquier otra manera” para fabricar, almacenar, transmitir, visualizar o poner a disposición materiales de pornografía infantil.

⁴⁷ En la sección 18 del Capítulo 17 de la Ley Penal finlandesa se penaliza a “cualquier persona que... o de otra manera distribuya imágenes obscenas o grabaciones visuales en las que figuren niños”.

País	Legislación específica sobre pornografía infantil	En la legislación está definida la “pornografía infantil”	Delitos facilitados por ordenador	Simple posesión	Obligación de notificación por parte de los PSI
Alemania	✓	✓	✓	✓	✗ ⁴⁸
Ghana	✗	✗	✗	✗	✗
Grecia	✓	✓	✓ ⁴⁹	✓	✗
Granada	✗	✗	✗	✗	✗
Guatemala	✓	✗	✗	✗	✗
Guinea	✗	✗	✗	✗	✗
Guinea Bissau	✗	✗	✗	✗	✗
Guyana	✗	✗	✗	✗	✗
Haití	✗	✗	✗	✗	✗
Honduras	✓	✓	✓	✓	✗

⁴⁸ Aunque un PSI no tiene la obligación explícita de notificar a las autoridades encargadas de hacer cumplir la ley o a otros organismos responsables, en la mayoría de los casos los PSI presentarán informes a dichos organismos. Un PSI que tenga conocimiento de materiales de pornografía infantil en sus sitios web y no suprima el contenido ilícito incurrirá en un delito punible. Entre los factores que se consideran figura la cuestión de determinar si el PSI podía razonablemente detectar los datos y suprimirlos o bloquearlos, puesto que hay numerosos PSI en Alemania que ofrecen grandes capacidades de almacenamiento con fines comerciales. Correo electrónico de Klaus Hermann, Consejero/Coordinador de Policía, Embajada de Alemania, Washington, D.C., dirigido a Jessica Sarra, Directora de *Global Operations, International Centre for Missing & Exploited Children* (9 de febrero de 2006) (en los archivos del mencionado Centro).

⁴⁹ A tenor del Artículo 348a del Código Penal greco se penalizan diversos delitos relacionados con la pornografía infantil, con inclusión de la posesión, compra, transferencia y venta de pornografía infantil “de cualquier manera”.



País	Legislación específica sobre pornografía infantil	En la legislación está definida la “pornografía infantil”	Delitos facilitados por ordenador	Simple posesión	Obligación de notificación por parte de los PSI
Hungría	✓	✓	✓ ⁵⁰	✓	✗
Islandia	✓	✗	✓ ⁵¹	✓	✗
India	✓	✗	✓	✓	✗
Indonesia	✗	✗	✗	✗	✗
Irán	✗	✗	✗	✗	✗
Iraq	✗	✗	✗	✗	✗
Irlanda	✓	✓	✓	✓	✗
Israel	✓	✓	✓	✓	✗
Italia	✓	✓	✓	✓	✗
Jamaica	✗	✗	✗	✗	✗
Japón	✓	✓	✓	✗	✗

⁵⁰ Con arreglo a la sección 195/A(3) del Código Penal húngaro, toda persona que haga, distribuya o comercialice imágenes pornográficas de un menor en video, película, fotografías o “por cualquier otro medio” o ponga esas imágenes a disposición del público, comete una felonía. Además, de conformidad con una decisión adoptada recientemente por el Tribunal de Apelaciones húngaro (Nº BH 133/2005), la referencia a “cualquier otro medio” y a “ponga a disposición del público” incluye la distribución por Internet. Carta de Viktor Szederkényi, Jefe Adjunto de Misión, Embajada de la República de Hungría, Washington, D.C., dirigida a Jessica Sarra, Directora de *Global Operations, International Centre for Missing & Exploited Children* (6 de febrero de 2006) (en los archivos del mencionado Centro).

⁵¹ En el Artículo 210 del Código Penal de Islandia se penaliza la “posesión de fotografías, películas o artículos comparables en los que se describan niños en actitud sexual u obscena”. *Negritas añadidas.*

País	Legislación específica sobre pornografía infantil	En la legislación está definida la “pornografía infantil”	Delitos facilitados por ordenador	Simple posesión	Obligación de notificación por parte de los PSI
Jordania	✗	✗	✗	✗	✗
Kazajstán	✓	✗	✗	✗	✗
Kenya	✗	✗	✗	✗	✗
Corea	✓	✓	✓	✗	✗
Kuwait	✗	✗	✗	✗	✗
Kirguistán	✓	✗	✗	✗	✗
Laos	✗	✗	✗	✗	✗
Letonia	✓	✗	✓ ⁵²	✗	✗
Líbano	✗	✗	✗	✗	✗
Lesotho	✗	✗	✗	✗	✗
Liberia	✗	✗	✗	✗	✗
Libia	✗	✗	✗	✗	✗

⁵² En el Artículo 166(2) de la Ley Penal de Letonia se penaliza “la importación, producción, demostración pública, publicidad u otro tipo de distribución de materiales pornográficos... que guarden relación o describan abusos sexuales de menores”. *Negritas añadidas.*

País	Legislación específica sobre pornografía infantil	En la legislación está definida la “pornografía infantil”	Delitos facilitados por ordenador	Simple posesión	Obligación de notificación por parte de los PSI
Liechtenstein	✓	✗	✓	✓	✗ ⁵³
Lituania	✓	✗	✗	✓	✗
Luxemburgo	✓	✗	✓ ⁵⁴	✓	✗
Macedonia	✓	✗	✓ ⁵⁵	✗	✗
Madagascar	✓	✗	✓ ⁵⁶	✗	✗
Malawi	✗	✗	✗	✗	✗
Malasia	✗	✗	✗	✗	✗
Maldivas	✗	✗	✗	✗	✗
Malí	✓	✗	✗	✗	✗
Malta	✓	✗	✓	✓	✗

⁵³ Aunque el Código Penal de Liechtenstein no contiene ninguna disposición específica sobre la notificación por parte de los PSI, en el proyecto de nueva Ley sobre niños y jóvenes se ha incluido un requisito de notificación que se aplicaría “a toda persona que tenga conocimiento de que se pone en peligro el bienestar de un menor”. Correo electrónico de Claudia Fritsche, Embajadora, Embajada de Liechtenstein, Washington, D.C., dirigido a Jessica Sarra, Directora de *Global Operations, International Centre for Missing & Exploited Children* (7 de febrero de 2006) (en los archivos del mencionado Centro).

⁵⁴ A tenor del Artículo 383 del Código Penal de Luxemburgo se penaliza no sólo la producción y posesión (con fines comerciales, de distribución o visualización pública) de “escritos, impresos, imágenes, fotografías, películas, u otros objetos de carácter pornográfico”, sino también la perpetración de una diversidad de otros delitos relacionados con la pornografía infantil de “cualquier otra manera”. *Negritas añadidas*.

⁵⁵ En el Artículo 193(3) del Código Penal de Macedonia se penaliza el abuso de un/una “joven” para la “producción de... otros objetos con un contenido pornográfico”.

⁵⁶ En el Artículo 346 del Código Penal de Madagascar se penaliza la utilización de “cualesquiera medios” para divulgar pornografía infantil.

País	Legislación específica sobre pornografía infantil	En la legislación está definida la “pornografía infantil”	Delitos facilitados por ordenador	Simple posesión	Obligación de notificación por parte de los PSI
Islas Marshall	✗	✗	✗	✗	✗
Mauritania	✗	✗	✗	✗	✗
Mauricio	✓	✗	✓	✗	✗
México	✓	✓	✓	✗	✗
Moldova	✓	✗	✗	✓	✗
Mónaco	✗	✗	✗	✗	✗
Mongolia	✗	✗	✗	✗	✗
Montenegro	✓	✗	✓ ⁵⁷	✗	✗
Marruecos	✓	✗	✗	✓	✗
Mozambique	✗	✗	✗	✗	✗
Myanmar	✓	✗	✗	✗	✗
Namibia	✗	✗	✗	✗	✗
Nauru	✗	✗	✗	✗	✗

⁵⁷ El Artículo 211(2) del Código Penal de Montenegro penaliza “la explotación de un niño para la producción de fotografías, audiovisuales u otros artículos de contenido pornográfico”. *Negritas añadidas.*

País	Legislación específica sobre pornografía infantil	En la legislación está definida la “pornografía infantil”	Delitos facilitados por ordenador	Simple posesión	Obligación de notificación por parte de los PSI
Nepal	✓	✗	✗ ⁵⁸	✗	✗
Países Bajos	✓	✓	✓	✓	✗ ⁵⁹
Antillas Neerlandesas	✗ ⁶⁰	✗	✗ ⁶¹	✗ ⁶²	✗
Nueva Zelanda	✓	✓	✓	✓	✗
Nicaragua	✗	✗	✗	✗	✗
Níger	✗	✗	✗	✗	✗
Nigeria	✗	✗	✗	✗	✗
Noruega	✓	✓	✓	✓	✗
Omán	✗	✗	✗	✗	✗
Pakistán	✗	✗	✗	✗	✗

⁵⁸ Pese a no referirse específicamente a la pornografía infantil, la sección 47 de la Ordenanza sobre Transacciones Electrónicas de 2004 prohíbe la publicación o visualización en ordenadores, Internet u otros medios electrónicos, de materiales que la Ley prohíbe publicar o visualizar porque atentan contra la moral y la decencia públicas.

⁵⁹ Aunque no existe ninguna obligación legal o contractual de que los PSI notifiquen sospechas de pornografía infantil a los organismos encargados de hacer cumplir la ley, los PSI basados en los Países Bajos tienen la práctica de notificar de inmediato a estos organismos cuando detectan pornografía infantil y los PSI suprimen dichos contenidos del sitio web en cuestión. Además, atendiendo a la solicitud de los responsables de la observancia de la ley, los PSI remiten sus logs relacionados con el sitio web que es objeto de sospechas. Correo electrónico de Richard Gerding, Consejero sobre Asuntos Policiales y Jurídicos, Embajada Real de los Países Bajos, Washington, D.C., dirigido a Jessica Sarra, Directora de *Global Operations, International Centre for Missing & Exploited Children* (8 de febrero de 2006) (en los archivos del mencionado Centro).

⁶⁰ Aunque aún no se ha promulgado ninguna legislación específica sobre pornografía infantil, se ha establecido un Comité con el cometido de revisar la versión actual del Código Penal de las Antillas Neerlandesas, y se introducirá una legislación específica sobre la pornografía infantil (Artículo 2.13.4 propuesto). Correo electrónico de Richard Gerding, Consejero sobre Asuntos Policiales y Jurídicos, Embajada Real de los Países Bajos, Washington, D.C., dirigido a Jessica Sarra, Directora de *Global Operations, International Centre for Missing & Exploited Children* (22 de febrero de 2006) (en los archivos del mencionado Centro).

⁶¹ El Artículo 2.13.4 propuesto penalizaría los delitos facilitados por ordenador.

⁶² El Artículo 2.13.4 propuesto penalizaría la simple posesión.

País	Legislación específica sobre pornografía infantil	En la legislación está definida la “pornografía infantil”	Delitos facilitados por ordenador	Simple posesión	Obligación de notificación por parte de los PSI
Panamá	✓	✓	✓	✓	✗ ⁶³
Papua Nueva Guinea	✓	✗	✗	✓	✗
Paraguay	✓	✗	✗	✓	✗
Perú	✓	✓	✓	✓	✗
Filipinas	✓	✗	✗	✗	✗
Polonia	✓	✗	✗	✓	✗
Portugal	✓	✗	✓ ⁶⁴	✓	✗
Qatar	✓	✗	✓ ⁶⁵	✗	✗
Rumania	✓	✓	✓	✓	✗

⁶³ Aunque el Código Penal panameño no contiene ninguna disposición específica que exija la notificación por parte de los PSI, el Artículo 231-I estipula que toda persona que esté en conocimiento de la utilización de menores en actividades pornográficas o sexuales, independientemente del hecho de que esa persona haya obtenido la información en el desempeño de sus funciones en el empleo, comercio, profesión o por cualquier otro medio, y no lo comunique a las autoridades, por dicha omisión esa persona podrá ser enviada a prisión. Si tras la notificación no puede comprobarse la comisión del delito (actividad sexual o pornográfica infantil), la persona autora de la notificación quedará exonerada de toda responsabilidad en lo que respecta a su notificación a las autoridades. Correo electrónico de Isabel Fernández, Embajada de Panamá, Washington, D.C., dirigido a Jessica Sarra, Directora de *Global Operations, International Centre for Missing & Exploited Children* (12 de abril de 2006) (en los archivos del mencionado Centro).

⁶⁴ Del Artículo 172 del Código Penal portugués cabe inferir que la expresión “por cualquier medio” permite a un fiscal considerar a las tecnologías de la información y la comunicación como un medio para perpetrar el delito de distribución de imágenes, sonidos o películas en los que se muestran claramente a menores de 14 años de edad realizando actos sexuales. Carta de Pedro Catarino, Embajador, Embajada de Portugal, Washington, D.C., dirigida a Ernie Allen, Presidente y Director General del *International Centre for Missing & Exploited Children* (22 de febrero de 2006) (en los archivos del mencionado Centro).

⁶⁵ En el Artículo 292 del Código Penal de Qatar se mencionan específicamente “libros, publicaciones, **otros materiales escritos**, imágenes, fotografías, películas, símbolos u **otros artículos**”. *Negritas añadidas.*



País	Legislación específica sobre pornografía infantil	En la legislación está definida la “pornografía infantil”	Delitos facilitados por ordenador	Simple posesión	Obligación de notificación por parte de los PSI
Rusia	✓	✗	✗	✗	✗
Rwanda	✗	✗	✗	✗	✗
Saint Kitts y Nevis	✗	✗	✗	✗	✗
Sta. Lucía	✗	✗	✗	✗	✗
San Vicente y las Granadinas	✗	✗	✗	✗	✗
San Marino	✓	✗	✓	✗	✗
Santo Tomé y Príncipe	✗	✗	✗	✗	✗
Arabia Saudita	✗	✗	✗	✗	✗
Senegal	✗	✗	✗	✗	✗
Serbia	✓	✗	✓ ⁶⁶	✗	✗
Seychelles	✗	✗	✗	✗	✗

⁶⁶ El Artículo 111a del Código Penal de Serbia penaliza la realización de “una fotografía, una película o **alguna otra imagen**” de un menor con el fin de elaborar materiales pornográficos. Además, el Artículo 185 penaliza la utilización de un menor para producir “fotografías, audiovisuales u **otros artículos** de contenido pornográfico”. *Negritas añadidas.*

País	Legislación específica sobre pornografía infantil	En la legislación está definida la “pornografía infantil”	Delitos facilitados por ordenador	Simple posesión	Obligación de notificación por parte de los PSI
Sierra Leona	✗	✗	✗	✗	✗
Singapur	✗	✗	✗	✗	✗
República Eslovaca	✓	✓	✓	✓	✗
Eslovenia	✓	✓	✓ ⁶⁷	✗	✗
Somalia	✗	✗	✗	✗	✗
República Sudafricana	✓	✓	✓	✓	✓
España	✓	✗	✓ ⁶⁸	✓	✗
Sri Lanka	✓	✗	✗	✓	✗
Sudán	✗	✗	✗	✗	✗
Suriname	✗	✗	✗	✗	✗
Swazilandia	✗	✗	✗	✗	✗

⁶⁷ El Artículo 187(2) del Código Penal de Eslovenia penaliza la utilización abusiva de un menor “para elaborar imágenes, audiovisuales u otros artículos de carácter pornográfico”; el Artículo 187(3) penaliza a cualquier persona que “produzca, distribuya, venda, importe, exporte... o suministre [materiales pornográficos con menores] de cualquier manera o posea esos materiales con la intención de producir, distribuir, vender, importar, exportar o suministrar esos materiales de **cualquier otro modo**”. *Negritas añadidas.*

⁶⁸ El Artículo 189(1)(a) del Código Penal español penaliza la utilización de un menor “para elaborar **cualquier tipo** de material pornográfico”; el Artículo 189(1)(b) penaliza la producción, venta, distribución, visualización o facilitación de la producción, venta, divulgación o exhibición de “cualquier tipo” de pornografía infantil por “cualquier medio”; y el Artículo 189(7) reitera las expresiones “cualquier tipo” y “cualquier medio” utilizadas anteriormente. *Negritas añadidas.*

País	Legislación específica sobre pornografía infantil	En la legislación está definida la “pornografía infantil”	Delitos facilitados por ordenador	Simple posesión	Obligación de notificación por parte de los PSI
Suecia	✓	✗	✓ ⁶⁹	✓	✗ ⁷⁰
Suiza	✓	✓	✓	✓	✗
Siria	✗	✗	✗	✗	✗
Tayikistán	✓	✗	✗	✗	✗
Tanzanía	✓	✗	✗	✗	✗
Tailandia	✗	✗	✗	✗	✗
Timor Oriental	✗	✗	✗	✗	✗
Togo	✗	✗	✗	✗	✗
Tonga	✓	✓	✓	✓	✗
Trinidad y Tabago	✗	✗	✗	✗	✗

⁶⁹ La legislación penal sueca está formulada de tal modo que, en principio, se ha de aplicar independientemente de los prerequisites técnicos. La penalización de la pornografía infantil no constituye una excepción y, por consiguiente, las disposiciones del Capítulo 16, Sección 10a del Código Penal sueco se aplican a los delitos facilitados por computador. Carta de Anette Nilsson, Primera Secretaria, Embajada Sueca, Washington, D.C., dirigida a Jessica Sarra, Directora de *Global Operations*, *International Centre for Missing & Exploited Children* (23 de febrero de 2006) (en los archivos del mencionado Centro).

⁷⁰ En 1998 se promulgó en Suecia el *Bulletin Board System (BBS) Liability Act* (1998:112), cuya finalidad es evitar la propagación de pornografía infantil imponiendo a los proveedores de BBS la obligación de supervisar los contenidos BBS. Estos proveedores también están obligados a suprimir o de alguna otra manera evitar la divulgación de mensajes con contenido delictivo, incluidos los relacionados con pornografía infantil. Carta de Anette Nilsson, Primera Secretaria, Embajada de Suecia, Washington, D.C., dirigida a Jessica Sarra, Directora de *Global Operations*, del *International Centre for Missing & Exploited Children* (23 de febrero de 2006) (en los archivos del mencionado Centro).

País	Legislación específica sobre pornografía infantil	En la legislación está definida la “pornografía infantil”	Delitos facilitados por ordenador	Simple posesión	Obligación de notificación por parte de los PSI
Túnez	✓	✗	✓ ⁷¹	✗	✗
Turquía	✓	✗	✗	✓	✗
Turkmenistán	✗	✗	✗	✗	✗
Uganda	✗	✗	✗	✗	✗
Ucrania	✓	✗	✓	✗	✗
Emiratos Árabes Unidos	✗	✗	✗	✗	✗
Reino Unido ⁷²	✓	✓	✓	✓	✗ ⁷³
Estados Unidos de América	✓	✓	✓	✓	✓
Uruguay	✓	✗	✓ ⁷⁴	✗	✗
Uzbequistán	✗	✗	✗	✗	✗

⁷¹ El Artículo 234 del Código Penal de Túnez penaliza, entre otras cosas, la utilización de “cualquier fotografía o grabación visual” con imágenes pornográficas de menores.

⁷² A los efectos del presente Informe, el Reino Unido incluye a Inglaterra y Gales.

⁷³ El Reino Unido aplica un procedimiento voluntario de “notificación y supresión” supervisado por la *Internet Watch Foundation* (IWF), un órgano independiente del sector industrial apoyado por la policía y el Gobierno. Los PSI del Reino Unido “suprimen” las imágenes de pornografía infantil cuando éstas son notificadas por la IWF. De no hacerlo, éstos pueden ser demandados. Carta de Tony Lord, Primer Secretario, *Justice & Home Affairs*, Embajada de Gran Bretaña, Washington, D.C., dirigida a Ernie Allen, Presidente y Director General del *International Centre for Missing & Exploited Children* (9 de febrero de 2006) (en los archivos del mencionado Centro).

⁷⁴ En la Ley 17.815 de la República Oriental del Uruguay se penalizan ciertos delitos relacionados con la pornografía infantil, independientemente de la forma en la que éstos hayan sido cometidos (Artículo 1: “que de cualquier manera realice o produzca pornografía infantil”; Artículo 2: “que de cualquier manera facilite la comercialización, difusión, exhibición, almacenamiento o adquisición de pornografía infantil”).



País	Legislación específica sobre pornografía infantil	En la legislación está definida la “pornografía infantil”	Delitos facilitados por ordenador	Simple posesión	Obligación de notificación por parte de los PSI
Ciudad del Vaticano	✗ ⁷⁵	✗	✗	✗	✗ ⁷⁶
Venezuela	✓	✓	✓	✗	✗
Viet Nam	✗	✗	✗	✗	✗
Yemen	✗	✗	✗	✗	✗
Zambia	✗	✗	✗	✗	✗
Zimbabwe	✗	✗	✗	✗	✗

⁷⁵ En ausencia de una legislación específica sobre pornografía infantil, esos casos se podrían delegar al sistema judicial italiano, previa solicitud de la Santa Sede.

⁷⁶ “La Santa Sede no tiene ningún proveedor de servicios Internet externo y la navegación desde el proveedor interno tiene filtros que impiden no sólo el acceso a cualquier sitio relacionado con pornografía infantil, sino también la distribución en línea de materiales pornográficos. Puesto que el sitio web de la Santa Sede es de carácter institucional, allí sólo se encuentran asuntos que son inherentes a su misión...”. Carta del Arzobispo Pietro Sambi, Nuncio Apostólico, Nunciatura Apostólica, Estados Unidos de América, dirigida a Ernie Allen, Presidente y Director General del *International Centre for Missing & Exploited Children* (5 de junio de 2006) (en los archivos del mencionado Centro).

Apéndice 3

Software sobre seguridad de menores

El mercado ofrece numerosos conjuntos de software e instrumentos técnicos que pueden ayudar a excluir contenidos y contactos no deseados e indeseables, limitar la cantidad de tiempo durante la cual un ordenador puede acceder a Internet o las aplicaciones que pueden funcionar en un ordenador o un dispositivo concreto. Algunos sistemas operativos también incluyen herramientas de este tipo como parte del suministro habitual. Por lo general estas funciones respaldarán o complementarán a los mensajes esenciales de seguridad que figuran en todas las campañas sobre seguridad de Internet de todo el mundo. Los software de seguridad de este tipo se utilizan de manera generalizada en las escuelas y bibliotecas públicas, y son similares a los que pueden instalar los empleadores en sus redes internas para limitar la utilización de Internet inapropiada o ajena a cuestiones laborales durante el horario de trabajo.

La eficacia de estos software puede variar enormemente, y en algunos países se han desplegado esfuerzos por introducir un “sello de aprobación” para conferir un nivel básico de garantías de calidad que ayude a los padres, profesores, niños y jóvenes a elegir el programa que mejor se ajuste a sus necesidades y funcione de una manera eficaz y fácil de comprender.

Cabe señalar que, tarde o temprano, todos los dispositivos fallan y los software pueden funcionar mal. Por consiguiente, los padres, profesores, niños y jóvenes nunca deben delegar completamente sus responsabilidades en los programas de seguridad. Estos programas deben considerarse siempre como un complemento de los programas de educación y concienciación diseñados para asegurar que el niño o el joven sepan cómo evitar los peligros en línea, o cómo hacerles frente a los mismos si éstos surgen.

Entre los conjuntos de software sobre seguridad infantil actualmente disponibles cabe mencionar los siguientes:

Productos gratuitos

1. *K9 Web Protection* (<http://www.k9webprotection.com/>)
2. *SafeFamilies* (<http://www.safefamilies.org/download.php>)
3. *File Sharing Sentinel* (<http://www.akidthaine.com/>)
4. *B-Gone* (<http://support.it-mate.co.uk/?mode=Products&p=bgone>)
5. Las últimas versiones de Windows y Mac OS también vienen con instrumentos que pueden utilizarse sin ningún pago adicional.

Productos comerciales

- *Net Nanny Parental Controls*
- *Safe Eyes*
- *CYBERsitter*
- *WiseChoice.net*
- *CyberPatrol*
- *MaxProtect*
- *FilterPak*
- *Netmop*
- *imView*
- *McAfee Parental Controls*
- *Norton Parental Controls*
- *Child Safe*
- *ContentProtect Security Appliance*
- <http://www.cybersentinel.co.uk/>

Para una lista más detallada de este tipo de productos gratuitos y comerciales véase www.getnetwise.org.



Apéndice 4

Elaboración de una estrategia nacional

Internet ha dado lugar a toda una serie de modalidades de abuso de niños y jóvenes que antes de su aparición como producto de consumo masivo eran sencillamente imposibles, como por ejemplo en el marco de salas de conversación y enlaces de distribución web. Internet también ha desempeñado un papel singular en la ampliación de la magnitud y disponibilidad de CAM en todo el mundo. Por estas razones, en el contexto de las preocupaciones por la seguridad de jóvenes y niños en línea, los encargados de formular políticas deberían apuntar a algunos de los siguientes objetivos, cuando no a su totalidad:

1. Proscribir el “grooming” (“condicionamiento”) u otras formas de incitación a distancia de menores para realizar actividades sexuales o entablar contactos sexuales inapropiados.
2. Proscribir la posesión, producción y distribución de CAM, independientemente de la intención de distribuir esos materiales.
3. Tomar medidas adicionales para interrumpir o reducir el tráfico de CAM, por ejemplo mediante el establecimiento de una línea directa nacional y la adopción de medidas para bloquear el acceso a los sitios web y los *Usenet Newsgroups* que se sabe contienen o publicitan la disponibilidad de CAM.
4. Garantizar que se establecen procedimientos nacionales para asegurar que todos los materiales CAM encontrados en un país se canalizan hacia un recurso nacional centralizado.
5. Elaborar estrategias para combatir la demanda de CAM, en particular entre personas que ya han sido convictas por ese tipo de delito. Es importante hacer tomar conciencia de que no se trata de un delito sin víctimas: se abusa de menores para producir los materiales visualizados, y al mirar o telecargar esos materiales de forma deliberada se contribuye directamente al abuso en cuestión y se alienta el abuso de otros niños para producir más imágenes.
6. Promover la conciencia del hecho de que los niños nunca pueden consentir ser abusados sexualmente, ya sea para la producción de CAM o de cualquier otro modo. Alentar a las personas que utilizan CAM a buscar ayuda, y al mismo tiempo aclararles que de persistir serán responsables de actividad ilícita delictiva.
7. Velar por que las estrategias para la prevención de delitos de los organismos responsables de la observancia de la ley, así como los programas sociales y basados en las escuelas, contengan secciones sobre ciberseguridad y sobre los riesgos que plantea el comportamiento predador en línea, con un asesoramiento apropiado para cada edad.
8. Considerar otras estrategias para hacer frente a la demanda de CAM. Por ejemplo, algunos países mantienen un registro de los delincuentes sexuales procesados. Los tribunales han emitido órdenes judiciales a tenor de las cuales se prohíbe a esos delincuentes utilizar Internet completamente o las partes de Internet utilizadas frecuentemente por niños o jóvenes. Hasta la fecha el problema con estas órdenes ha sido su inobservancia. Sin embargo, en algunos países se está considerando la posibilidad de integrar la lista de delincuentes sexuales conocidos en una lista general de bloqueo que impedirá a los que figuren en ella visitar o incorporarse a ciertos sitios web, por ejemplo los sitios a los que recurren grandes cantidades de niños y jóvenes.

Por supuesto si el delincuente se dirige a un sitio web utilizando otro nombre o un inicio de sesión falso estas medidas perderán en gran medida su eficacia, pero la penalización de este comportamiento puede representar otro factor disuasivo.

9. Proporcionar a las víctimas un apoyo adecuado a largo plazo. Cuando se han injuriado niños o jóvenes en línea y ha aparecido por ejemplo en Internet su imagen ilícita, éstos se sentirán naturalmente muy preocupados por el hecho de que esa imagen haya sido vista y sus posibles repercusiones. Esto puede dejar en los niños o jóvenes un sentimiento de vulnerabilidad ante las incitaciones o frente a nuevos abusos y explotaciones sexuales. En este contexto, es importante disponer de servicios de apoyo profesional para ayudar a los niños y jóvenes a encontrarse a ellos mismos en estas circunstancias. Podría ser necesario ofrecer este tipo de apoyo a largo plazo.

10. Garantizar que se establece y se promueve ampliamente un mecanismo destinado a ofrecer un medio rápido y fácilmente comprensible para notificar contenidos ilícitos o comportamientos en línea ilegales o preocupantes, por ejemplo un sistema similar al que ha establecido el *Virtual Global Taskforce*, <http://www.virtualglobaltaskforce.com>. Se debería fomentar la utilización del sistema i24/7 de INTERPOL.

11. Velar por que se imparte una formación adecuada a un número suficiente de funcionarios responsables de la observancia de la ley en materia de investigaciones en Internet y delitos informáticos, y que éstos tienen acceso a facilidades forenses adecuadas que les permiten extraer e interpretar datos digitales pertinentes.

12. Invertir en la formación de autoridades judiciales y del personal responsable de la fiscalización y la observancia de la ley, con el fin de familiarizarlos con los métodos utilizados por los delincuen-

tes en línea para perpetrar esos delitos. También será preciso destinar inversiones a la adquisición y mantenimiento de los medios necesarios para obtener e interpretar evidencia forense procedente de dispositivos digitales. Además, será importante establecer una colaboración bilateral y multilateral, así como mecanismos para el intercambio de información con los correspondientes órganos de investigación y autoridades encargadas de la observancia de la ley en otros países.



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

Impreso en Suiza
Ginebra, 2009

En colaboración con:

