Síntesis elaborada por Equipo MARGEN

DELITOS INFORMÁTICOS Y CIBERSEGURIDAD

NORMAS PRINCIPALES

- **CÓDIGO PENAL DE LA NACIÓN ARGENTINA**

http://www.informaticalegal.com.ar/1984/05/01/codigo-penal-de-la-nacion-argentina/

- **LEY 26.388 de Ley de Delitos Informáticos**

http://www.informaticalegal.com.ar/2008/06/24/ley-26-388-delitos-informaticos/

- **Convención de Budapest sobre Ciberdelincuencia** (no ratificada por la Rep. Argentina)

http://www.informaticalegal.com.ar/2001/11/23/convencion-de-budapest-sobre-ciberdelincuencia/

MENORES Y PORNOGRAFÍA INFANTIL

- **CÓDIGO PENAL DE LA NACIÓN ARGENTINA**, art. 128 (producción, distribución y tenencia de pornografía infantil), art. 131 (contacto a menores por medios electrónicos con una finalidad sexual -grooming-), art. 125 (corrupción de menores por medios digitales) y arts. 145 bis y 145 ter (trata de personas menores de edad).

- **LEY 26.061 de Protección Integral de los Derechos de las Niñas, Niños y Adolescentes**

http://www.informaticalegal.com.ar/2005/09/28/ley-26-061-proteccion-integral-de-los-derechos-de-las-ninas-ninos-y-adolescentes/

que tiene por objeto la protección integral de los derechos de las niñas, niños y adolescentes que se encuentren en Argentina, para garantizar el ejercicio y disfrute pleno, efectivo y permanente de aquellos reconocidos en el ordenamiento jurídico nacional y en los tratados internacionales en los que la Nación sea parte. Estos derechos están asegurados por su máxima exigibilidad y sustentados en el principio del interés superior del niño.

- **DECRETO 415/2006**

http://www.informaticalegal.com.ar/2006/04/17/decreto-4152006-reglamento-de-la-ley-26-061-de-proteccion-integral-de-los-derechos-de-las-ninas-ninos-y-adolescentes/

que reglamenta la Ley 26.061 de Protección Integral de los Derechos de las Niñas, Niños y Adolescentes.

- **LEY 26.904 de Grooming**

http://www.informaticalegal.com.ar/2013/12/04/ley-26-904-contacto-a-menores-con-el-proposito-de-cometer-delitos-contra-la-integridad-sexual-grooming/

que incorpora el art. 131 del Código Penal que pena con prisión de 6 meses a 4 años el que, por medio de comunicaciones electrónicas, telecomunicaciones o cualquier otra tecnología de transmisión de datos, contactare a una persona menor de edad, con el propósito de cometer cualquier delito contra la integridad sexual de la misma.

- **DECISION MARCO 2004-68-JAI del Consejo de Europa**

http://www.informaticalegal.com.ar/2004/01/20/decision-marco-200468jai-del-consejo-de-europa-explotacion-sexual-de-los-ninos-y-pornografia-infantil/

relativa a la lucha contra la explotación sexual de los niños y la pornografía infantil (20 de enero de 2004).

- **LEY 863 de la Legislatura de la Ciudad Autónoma de Buenos Aires** http://www.informaticalegal.com.ar/2002/08/15/ley-863-de-la-legislatura-de-la-ciudad-autonoma-de-buenos-aires-establecimientos-comerciales-y-filtros-sobre-paginas-pornograficas/

establece que los establecimientos comerciales que brinden acceso a Internet deben instalar y activar filtros de contenido sobre páginas pornográficas.

- **CÓDIGO CONTRAVENCIONAL DE LA CIUDAD DE BUENOS AIRES** http://www.informaticalegal.com.ar/2004/09/23/codigo-contravencional-de-la-ciudad-autonoma-de-buenos-aires/

en su art. 61 castiga al que tolere o admita la presencia de menores en lugares no autorizados (local de espectáculos públicos, de baile o de entretenimientos tipo ciber) y en su art. 62 castiga al que suministre o permita a un menor el acceso a material pornográfico.

OTROS PROGRAMAS GUBERNAMENTALES

- **RESOLUCIÓN 69/2016 del Ministerio de Justicia y Derechos Humanos** http://www.informaticalegal.com.ar/2016/03/11/resolucion-692016-ministerio-de-justicia-y-derechos-humanos-programa-nacional-contra-la-criminalidad-informatica/

que crea el Programa Nacional contra la Criminalidad Informática y reemplaza a la **Comisión Técnica Asesora de Cibercrimen**.

http://www.informaticalegal.com.ar/2011/10/05/resolucion-conjunta-8662011-y-15002011-jefatura-de-gabinete-de-ministros-y-ministerio-de-justicia-y-derechos-humanos-comision-tecnica-asesora-de-cibercrimen

- **RESOLUCIÓN CONJUNTA 866/2011 y 1500/2011 de la Jefatura de Gabinete de Ministros y el Ministerio de Justicia y Derechos Humanos** http://www.informaticalegal.com.ar/2011/10/05/resolucion-conjunta-8662011-y-15002011-jefatura-de-gabinete-de-ministros-y-ministerio-de-justicia-y-derechos-humanos-comision-tecnica-asesora-de-cibercrimen/

que crea la Comisión Técnica Asesora de Cibercrimen.

LEGISLACIÓN INTERNACIONAL SOBRE DELITOS INFORMÁTICOS

(Fuente: Innocenti Research Center de la UNICEF)

Por otra parte, cabe señalar que, a nivel mundial, muchos países cuentan con legislación en materia de delitos informáticos, algunos incluso desde hace ya más de una década.

Dado que el abuso a menores en la Red no tiene fronteras, señalan como imprescindible la coordinación internacional en las áreas de justicia y de protección al menor.

Actualmente los instrumentos internacionales existentes son, tal y como los enumera el informe:

- La Convención sobre los Derechos del Niño (1989)
- El Protocolo Opcional de la Convención sobre los Derechos del Niño acerca de la venta de niños, la prostitución infantil y la pornografía infantil (OPSC, 2000)
- El Protocolo para la Prevención, Supresión y Castigo del Tráfico de Personas, Especialmente Mujeres y Niños, complementario a la Convención de las Naciones Unidas contra el Crimen Organizado Trasnacional ("Protocolo de Palermo", 2000).
- La Convención del Consejo de Europa sobre Ciberdelitos (2001)
- La Convención del Consejo de Europa sobre la Protección de los Niños ante la Explotación y el Abuso Sexuales (2007).

En conjunto estos instrumentos jurídicos internacional proporcionan un marco de medidas y de definición de delitos para la protección (también online) de los derechos de los menores.

La Declaración de Río (2008) supuso un avance al demandar de los Estados acciones para evitar y frenar las imágenes de abuso a menores y el grooming en Internet.

No obstante, la implementación de estas medidas es aún insuficiente, explican. Según un estudio de 2010 del Centre for Missing & Exploited Children:

- Sólo 45 de los 196 países analizados tenía legislación suficiente para combatir los delitos de imágenes de abuso infantil.
- 89 países no tenían legislación en absoluto acerca de la pornografía infantil.
- De los que sí la tenían, 52 no definían lo que era la pornografía infantil.
- De los que tenían legislación sobre pornografía infantil, 18 no tenían en cuenta los delitos relacionados con los ordenadores.
- De los que tenían legislación sobre pornografía infantil, 33 no crimilizaban la posesión de la pornografía infantil, sin tener en cuenta la intención de distribuirla.

Las investigaciones sugieren que los menores de casi todo el mundo utilizan de manera muy similar las redes sociales, lo cual crea oportunidades para que los potenciales groomers contacten con ellos, especialmente en aquellos países donde se conectan maś desde fuera de casa o donde los padres tienen menores conocimientos.

El informe también menciona el avance que dentro de la UE ha supuesto la directiva aprobada por el Parlamento Europeo en noviembre de 2011 criminalizará formas de abuso y explotación sexuales a menores actualmente no cubiertas por la legislación de la Unión Europea, tales como el grooming, las exhibiciones pornográficas infantiles online y el visionado de pornografía infantil sin descarga de ficheros.

Establece umbrales más bajos para aplicar las máximas condenas.

Asegura que los culpables que sean ciudadanos de la UE serán perseguidos por delitos cometidos fuera de la Unión.

Proporciona a las víctimas infantiles asistencia, apoyo y protección, incluyendo reclamación de compensaciones.

Comparte datos de las condenas a delincuentes sexuales entre las diversas autoridades de los países miembros.

Introduce la eliminación obligatoria y el bloqueo opcional de webs que contengan material de abuso a menores.

Señala que las empresas de la UE son pioneras en cuanto a autorregulación y pone como ejemplo el European Framework for safer mobile use by younger children and teenagers aprobada en febrero de 2007. En junio de 2010 ya había Códigos de Conducta al respecto en 25 países de la Unión y un informe revelaba en esa misma fecha que el 83% de los operadores de telefonía móvil, que daban servicio al 96% de los usuarios de móvil de la UE, implementaban ya el Marco Europeo por medio de códigos de conducta. En febrero de 2009 se lanzó un documento similar, pero esta vez para las redes sociales online: Safer Social Networking Principles for the EU, que recoge medidas en cuanto a configuración de privacidad, educación y concienciación y facilidades de denuncia de abusos. En mayo de 2011 se analizó el grado de cumplimiento pero sólo 3 de 14 servicios de red social recibieron una buena cualificación.

En otros ámbitos destaca el Memorándum de Montevideo (julio de 2009), aunque no es vinculante para ningún Estado americano.

En cuanto a la persecución de los ciberdelitos contra los menores, los investigadores de UNICEF señalan algunos problemas que la complican: la dificultad para determinar cuál es la jurisdicción pertinente en delitos originados en la Red, los casos que implican a varias víctimas residentes en jurisdicciones distintas y la distancia que separa en ocasiones a los perpetradores y a las víctimas. También reconocen que determinar si se ha cometido o no un delito de abuso contra menores en la Red no es un proceso directo, dado que no suele haber contacto físico. Las cuestiones que esto plantea a la policía son varias:

- ¿Es suficiente el intento de engañar a un menor con fines sexuales para que se haya cometido delito?
- ¿Qué evidencias de ese intento se requieren?
- ¿Cuándo una imagen de un(a) menor es pornográfica?
- Las imágenes de niños no reales ¿son perseguibles?

Por parte de las propias víctimas existen también dificultades: la vergüenza y el sentirse en cierta medida cómplices de lo sucedido, hacen que muchas veces no denuncien el hecho hasta que la propia policía lo descubre en una investigación. Incluso entonces, ante la propia imagen de su abuso, hay víctimas que niegan que haya sucedido. Si ya es minoritario el número de abusos sexuales que se dan a conocer fuera de la Red, entre los que suceden online el número es aún menor.

En algunos casos de grooming el menor o la menor percibe al abusador como su novia o novio y es emocionalmente dependiente de él (o ella). Otra dificultad surge en los casos en los que el menor está aislado o carece de soporte social o familiar, con lo cual es aún más improbable que denuncie. Y por supuesto, muchos ni siquiera sabrán nunca que han sido víctimas de abuso puesto que una foto suya captada en Internet puede ser retocada digitalmente para hacerlos aparecer desnudos o en escenas sexuales y ser distribuido por la Red sin que lo llegue a saber el menor.

Otro aspecto que no suele ser tenido en cuenta de manera suficiente es que el menor puede no sólo sufrir con el abuso sino que la revelación del abuso. En ocasiones se retractan de la denuncia por temor las consecuencias para ellos o sus seres queridos.

También aquí existen dificultades adicionales en los países empobrecidos: la policía no dispone en muchos casos de la capacitación para perseguir estos crímenes, que requieren conocimientos especializados de Internet y de protección de menores. En ocasiones, el personal está formado suficientemente, pero no dispone de la tecnología necesaria. Incluso en los países ricos, es frecuente que estos casos sean catalogados como ciberdelito y pasen así a equipos más especializados en el fraude online que en la protección al menor. Organismos como CEOP recomiendan que se integre a personal especializado en menores en este tipo de investigaciones policiales.

Los estudios sobre la materia indican que, por otra parte, los propios profesionales que trabajan en la protección al menor —docentes, enfermeros escolares, sanitarios, oficiales de policía, trabajadores sociales, consejeros, psicoterapeutas…— no son suficientemente conscientes de los riesgos del abuso online. Por ejemplo, ante un cambio de comportamiento en una chica de 13 años, a pocos se les ocurre preguntar por sus actividades online. Dada la creciente importancia de las TIC en la vida de los adolescentes, esto quiere decir que un gran número de profesionales están fallando en la identificación e investigación de un contexto de abuso cada vez más frecuente.