Revista de Estudos Constitucionais, Hermenêutica e Teoria do Direito (RECHTD)
6(1): 31-43 janeiro-junho 2014
 - doi: 10.4013/rechtd.2014.61.03

Estudio comparativo entre España, México y Argentina sobre la protección del menor en las redes sociales

Protecting children in online social networks: A comparative study between Spain, Mexico and Argentina

Federico Bueno de Mata[1]
Universidad de Salamanca, España
febuma@usal.es

Erika Yamel Munive Cortés[2]
Universidad Rey Juan Carlos, España
ey.munive.cortes@hotmail.com

Humberto Martín Ruani[3]
Universidad de Ciencias Empresariales y Sociales, Argentina
hmr@estudioruani.com.ar

Resumen

A pesar de las ventajas que ofrecen las TIC (Tecnologías de la Información y la Comunicación), muchas organizaciones criminales están encontrando una manera nueva y eficaz para la comisión de diversas conductas delictivas, aprovechando la escasa legislación que existe al respecto, así como a la falta de conocimientos técnicos por parte de los juzgadores en este ámbito. Esta investigación se centra en estudiar la protección ofrecida por las redes sociales a los menores de edad en España, México y Argentina, con la intención de dar respuestas y sugerir mecanismos de protección en un terreno lleno de lagunas.

Palabras clave: Derecho Comparado, redes sociales, menores de edad.

[1] Doctor en Derecho y Profesor de Derecho Procesal. Acreditado como Profesor Contratado Doctor por ANECA y ACSUCYL. Profesor Contratado de Universidad Privada por la ACSUCYL y Ayudante Doctor en Derecho Procesal por ANECA y ACSUCYL. Universidad de Salamanca. Facultad de Derecho. Campus Unamuno, s/n. 37007, Salamanca, España.
[2] Doctoranda en Estudios Jurídicos. Universidad Rey Juan Carlos. Paseo de los Artilleros, s/n, 28032, Vicálvaro, Madrid, España.
[3] Becario del Doctorado en Derecho de la Universidad de Ciencias Empresariales y Sociales. Paraguay 1338, Buenos Aires, Ciudad Autónoma de Buenos Aires, Argentina.

Abstract

Despite the potential benefits of ICTs (Information and Communication Technologies), large organized criminal groups have found new ways to commit old crimes, taking advantage of weaknesses in cybercrime legislation, inefficient public policies and the lack of specialization at the legislative level in those fields. These factors may also affect vulnerable groups such as children. This comparative study between Spain, Mexico and Argentina intends to suggest mechanisms for protecting children's safety online and give actual legal advice on the use of social networking sites, which are areas that lack a definite legal regulation in most countries.

Keywords: Comparative Law, social networks, children.

Prólogo[4]

Tengo el gusto de sumar unas palabras introductorias al estudio iberoamericano elaborado por Bueno de Mata, Munive y Ruani sobre un tema tan interesante y necesario como son las medidas de protección del menor en las redes sociales.

Un primer tema que el estudio plantea es la necesidad de un acuerdo explícito técnico y normativo –sea como país o mejor si es como un colectivo de países– "para medir y hacer efectivo el cumplimiento de la misma a todos los operadores del mercado con independencia desde donde operen". Esto es fundamental si se quiere lograr avanzar hacia un real ejercicio de los derechos ciudadanos también en el ámbito virtual (es decir tener la posibilidad de ser también e-ciudadanos o ciberciudadanos). Allí avances como los logrados en España (como país) así como ejemplos de aspectos que las redes sociales podrían tener –a partir del caso de Tuenti– son aspectos a tener en cuenta.

Un segundo aspecto está centrado en medidas vinculadas a soluciones tecnológicas, jurídicas y de uso responsable del Internet donde se plantea la necesidad de explicitar el rol de los padres o apoderados, el Estado y las entidades supranacionales si es que realmente se quiere lograr avanzar en la protección del menor en las redes sociales en particular y en el ciberespacio en general.

Otro aspecto a considerar es la necesidad de constituir o consolidar la institucionalidad que como Estados se requiere para tomar acción sobre la defensa de sus ciudadanos en el ámbito del ciberespacio así como implementar medidas –i.e., políticas públicas sobre inclusión digital, sociedad de la información y el conocimiento, entre otros– y facilitar el uso de herramientas –i.e., Firma y Certificados Digitales– que no sólo ayudarán a una mejor identificación y protección de la identidad sino también podría ser un aliciente al proceso de desarrollo económico y social de nuestros países.

Es muy probable que antes de llegar a lograrlo se siga pasando por ciclos de ensayo, prueba y error entre otras posibilidades pero lo que no se puede perder de vista es que de por medio se encuentra la integridad de los menores de edad que hoy por hoy se enfrentan en una desprotección tácita y sería aún más extenso y definiría una "orfandad virtual" frente a su Estado y, en muchos casos, frente a sus padres en tanto estos últimos sea por estar inmersos en una brecha digital que se los impida, por falta de tiempo o cierto grado de desinterés, dejan que sean los menores los que naveguen y tomen decisiones sin mayor orientación o control.

Finalmente, considero que esfuerzos de análisis como los desarrollados en este estudio deben continuar y los aportes que nos dejan deben ser capitalizados no sólo por el ámbito académico sino también por ONGs e instancias de nuestros Estados.

La situación actual en España

La protección de los menores en las redes sociales españolas

Si nos adentramos en el mundo de las redes sociales en España, vemos como una compañía destaca por encima de los grandes gigantes *Facebook* o *Twitter*; no es

[4] El prólogo ha sido desarrollado por Juan Carlos Pasco Herrera, Magister en Gestión y Políticas Públicas (MGPP) por la Universidad de Chile (Departamento de Ingeniería Industrial) e Ingeniero Industrial y de Sistemas por la Universidad de Piura, Perú. Consultor/Investigador internacional en temas de gobierno electrónico y sociedad de la información. En cuanto a la docencia, se encuentra vinculado como especialista y coordinador de cursos en gobierno electrónico para el Departamento para la Gestión Pública Efectiva de la Secretaría de Asuntos Políticos (SAP) de la Organización de los Estados Americanos (OEA).

otra que la ya cada vez más conocida red social *Tuenti*, la cual cuenta con más de 13 millones de usuarios registrados (Tuenti, 2012a); siendo la red que más crece cada año, con un promedio de un 30% de nuevos fieles por año.

Tuenti es una red social dedicada al público joven español. Sigue un formato similar a otras redes sociales como *Facebook,* con la posibilidad de subir fotos, comentar en los perfiles de amigos, chatear con ellos y demás aplicaciones.

Esta red social fue creada en 2006 y en el mismo año 2010 fue absorbida por la multinacional Telefónica. El nombre que se le dio al sitio puede parecer a primera vista la pronunciación del número 20 en inglés (*twenty*), pero, en realidad, proviene de los vocablos "tú identidad"; para los creadores el nombre sonaba bien y contenía las sílabas "tú" y "tí", que era uno de los objetivos.

De esta forma *Facebook* y *Tuenti* se configuran como el mismo modelo de negocio pero con características técnicas diferentes en cuanto a seguridad y protección de datos de los usuarios menores de edad, siendo las de esta última mucho más eficaces, como a continuación expondremos.

De esta forma iremos analizando las peculiaridades, diferencias con *Facebook,* ventajas e inconvenientes de la red social líder en España para, de esta forma, acabar proponiendo una serie de soluciones y medidas para mejorar la protección ofrecida a los menores por estas aplicaciones en Internet. Del mismo modo hemos de indicar que la Comisión Europea cifra en 107,4 millones los usuarios europeos en 2012, lo cual otorga máximo interés y actualidad a dicha investigación. Al mismo tiempo España se configura como el primer país de toda Europa, y el quinto del mundo, con más usuarios en redes sociales[5].

Potenciales peligros ocasionados a los menores por una deficitaria regulación de las redes sociales

La falta de regulación específica de una realidad cada vez más imperante hace plantearnos una serie de conductas que se tornan como potenciales peligros acechando a los menores en el entorno de las redes sociales, tales como: *cyberbulling*, *grooming*, *cybermobbing* o la suplantación de personalidad o *stalking* (Gundín, 2012, p. 4 ss.).

De momento existen una serie de "buenas intenciones" a nivel comunitario ofrecidas por la Comisión Europea al firmar[6] con un gran número de redes el *Primer Acuerdo Europeo sobre la Red Social* para garantizar la seguridad infantil y proteger a los niños del "ciberacoso" en línea (Chacón Medina, 2003, p. 4-6). El nuevo acuerdo constituye un paso adelante para la erradicación de los abusos a menores a través de la red.

(a) La polémica sobre la edad mínima para ser usuario de una red social: el triunfo de la legislación española

Al mismo tiempo la Agencia Española de Protección de Datos (AEPD, 2012) ha conseguido que *Facebook* y *Tuenti* adecuen la edad mínima de sus usuarios a la legislación española. Hasta la fecha, en virtud de la legislación norteamericana, *Facebook* tenía fijado en 13 años el mínimo a partir del cual los menores pueden formar parte de su plataforma, mientras que en España la legislación establece que la edad mínima para que los menores puedan compartir información en este tipo de servicios es de 14 años.

Tras el anuncio de la compañía a la AEPD, España se convierte en el único país en el que *Facebook* ha incrementado la edad mínima a 14 años para poder registrarse y ser miembro de su red social.

(b) Facebook y Tuenti: mismo modelo de negocio, diferentes jurisdicciones

Existen diferencias importantes en cuanto a la sumisión a los tribunales (Bujosa Vadell, 2008, p. 2 ss.) para resolver un litigio por parte de las diferentes redes sociales a pesar de actuar en el mismo mercado; de esta forma *Tuenti* se encuentra sometida a la normativa española y a la europea, famosa por sus exigencias en materia de Protección de Datos y Protección de menores, mientras que *Facebook* literalmente hace caso omiso ya no a la legislación, sino también a las peticiones y recomendaciones de la Agencia Española de Protección de Datos y a la Comisión Europea, lo que lleva a la absoluta desprotección de sus usuarios y a una situación de dejadez que no acabamos de comprender.

De esta forma si analizamos la sección dedicada a la política en materia legal de *Facebook* vemos como el usuario se somete en la "Cláusula 15, Conflictos" a

[5] Es el resultado que se desprende del estudio realizado por el Pew Research Centre, con datos del año 2012. Casi el 50% de los adultos españoles tienen un perfil activo en una red social, llegando al 90% en el caso de jóvenes. Estos datos sitúan a España en el quinto lugar del ranking mundial de usuarios de redes sociales, con un índice del 49%, sólo por detrás del Reino Unido (52%), Estados Unidos y Rusia (ambos con un 50%) y la República Checa, también con una penetración del 49% (Pew Research, 2014).

[6] Entre otras, las empresas que han firmado el acuerdo de protección son Facebook, MySpace, Bebo, Microsoft y Yahoo.

los Tribunales de Santa Clara, California, Estados Unidos, para resolver reclamaciones y demandas, comprobando así esta clamorosa desprotección, más cuando Facebook abrió en el año 2011 una sede empresarial en España, con lo que se deberían revisar estas cláusulas de sumisión expresas por no parecer, *a priori*, legales.

Si sumado a todo lo anterior consideramos a los poseedores de un perfil en una red social como usuarios o consumidores, vemos como se estaría vulnerando el art. 54.2 LECiv española, en el que se dice que "no será válida la sumisión expresa contenida en contratos de adhesión, o que contengan condiciones generales impuestas por una de las partes, o que se hayan celebrado con consumidores o usuarios". Por todo ello esta cláusula se consideraría nula de pleno derecho.

Por otro lado, vemos como *Tuenti* se somete a los Tribunales de Madrid, España, lo que obliga a la red social española a cumplir la Ley de Protección de Datos, que da mayores garantías que la norteamericana en cuestión de datos de carácter personal. Una característica positiva respecto a los usuarios españoles pero que deberá ser modificada si la intención de esta red social es ampliar su estrategia de mercado al ámbito europeo o mundial, cuestión altamente probable debido a que ahora Telefónica toma el timón empresarial.

Todo lo anterior, desde nuestro punto de vista puede suponer un desincentivo claro a emprender proyectos de base tecnológica en España, a que empresas como *Tuenti*, en las que el tratamiento de datos personales es esencial y costoso para su correcto funcionamiento, decidan quitarse el cartel de sociedad española y constituirse en otros países con menos restricciones legales, en tanto no se unifique la normativa y los criterios para medir y hacer efectivo el cumplimiento de la misma a todos los operadores del mercado (con independencia desde donde operen, siempre que los destinatarios de los servicios sean ciudadanos españoles o europeos).

Las ventajas ofrecidas en España en cuestión de seguridad a los usuarios menores de edad: Tuenti vs. Facebook

Tuenti, al firmar la declaración sobre Principios para las Redes Sociales más Seguras de la Unión Europea[7], ofrece una serie de ventajas en cuanto a la privacidad de las que creemos que *Facebook* podría tomar buena nota; resumiéndolas podemos encontrar los siguientes puntos ventajosos.

(i) Sistemas de ayuda, condiciones de uso y política de privacidad más transparentes y accesibles[8]

Tuenti ofrece de forma permanente en el pie de todas sus páginas una pestaña denominada "Condiciones de Uso y Política de Privacidad", donde se puede observar que esas condiciones han sido consensuadas con la Agencia Española de Protección de Datos y con unas recomendaciones específicas para menores entre 14 y 18 años así como facilitando unos enlaces externos a consejos sobre navegación segura ofrecidos por instituciones para proteger a los menores. Al mismo tiempo en la página de inicio se cuenta con una pestaña denominada "Ayuda" desde finales del 2009, pasando a estar disponible para todas las personas sean usuarios o no de la red social.

(ii) Equipo eficaz de investigación de verificación de cuentas de menores

Otra gran hazaña realizada por la red social española es que desde el 17 de abril de 2009 cuenta con un protocolo de investigación y borrado de usuarios menores de 14 años consistente en que parte de su plantilla se dedica a verificar una media de 1.000 perfiles sospechosos a la semana y les solicita que remitan vía fax o escáner una copia de su identificación oficial para verificar la edad. Si en un plazo de 92 horas no la acreditan, dichos perfiles se dan de baja inmediatamente. A su vez, cuando los usuarios que han sido borrados mediante el proceso anterior intentan registrarse de nuevo con el mismo correo electrónico, el sistema de *Tuenti* lo impide.

(iii) Restricciones por defecto en pro de la seguridad de los menores

Al mismo tiempo se implanta una restricción por defecto, ya demandada por el que aquí escribe en otros foros y de la que *Facebook* hace caso omiso; no es otra que aplicar por defecto a todos los perfiles de menores de 18 años el grado máximo de privacidad por defecto, denominado "Sólo amigos", siendo cerrados dichos perfiles para usuarios desconocidos. También se produce

[7] El 12 de junio de 2009 Tuenti remitió a la Comisión Europea su "Self-Declaration", donde reflejaba su interpretación y grado de adecuación a los Principios de la Unión Europea para unas Redes Sociales más seguras.

[8] En su página de inicio se puede ver en la parte inferior derecha las pestañas sobre ayuda y privacidad (Tuenti, 2012b).

una restricción por defecto en cuanto a la indexación en búsqueda de servidores de tu perfil, con lo que si tecleamos en *Google* nuestros nombres y apellidos no aparecerá nuestra página de *Tuenti,* situación totalmente opuesta con lo que ocurre con *Facebook*.

(iv) Facilidades a la hora de denunciar incidencias o abusos

En cuanto al sistema de reporte, en *Tuenti* se pueden denunciar tanto perfiles de usuarios como fotos específicas subidas por cualquiera. Dichas denuncias son transmitidas de forma automática a un equipo que las analiza y responde en un plazo breve. Es necesario que se responda de forma muy rápida, pues muchas veces el daño producido por los ciberdelitos suele ser inmediato y el autor, aunque deje un rastro informático, es difícilmente perseguible y localizable según transcurre el tiempo. En los casos más graves en los que el usuario pudiera estar en grave riesgo o aparezcan indicios de la comisión de un posible hecho delictivo, el caso se remite de inmediato al Departamento Legal y de Privacidad que lo analiza y denuncia a la Policía en un plazo no superior a 24 horas.

Para que todos estos plazos sean más creíbles, reales y eficaces, las compañías deben firmar acuerdos con las fuerzas de seguridad del Estado. En este caso concreto, *Tuenti* firmó un acuerdo con la Guardia Civil y la Policía Nacional española; lo que permite que aquellos casos susceptibles de constituir un delito sean comunicados de inmediato a estos cuerpos.[9]

Propuestas para la mejora de la seguridad de los menores en las redes sociales

Tras sostener varias propuestas en diversos foros como en Barcelona o en Costa Rica, llegamos a la conclusión de que las redes sociales van tomando nota y van incorporando medidas demandadas como las restricciones por defecto a los perfiles de los menores de edad, la indexación de los perfiles de los usuarios en ciberbuscadores o la transparencia en cuanto a las políticas de privacidad y condiciones de uso de estas redes sociales.

Aún así vemos como aún queda mucho por andar, especialmente al gigante *Facebook*, el cual debería tomar buena nota de *Tuenti* para ofrecer unos servicios más proteccionistas y garantistas a sus usuarios y dejando de hacer caso omiso a las recomendaciones que se le dan desde la Unión Europea en cuestiones relativas a la protección de datos.

En primer lugar se debería ejercitar un buen uso de la patria potestad por parte de las personas que lo ostenten, es decir, la postura de los padres o tutores es aquí fundamental para hacer que el menor haga un uso correcto de dichas redes sociales. Para ello se debe "*cibereducar*" al menor, es decir, debemos transmitir a los menores que Internet no es un espacio sin normas, impune o sin responsabilidades.

El problema con el que se topan los padres o tutores es la temida brecha digital que posee un gran sector de la población, es decir, el desconocimiento por muchos progenitores de los usos y recursos tecnológicos por pertenecer a otra generación, y su desconocimiento se traduce en un potencial riesgo para el menor de edad. En estos casos vería conveniente la ayuda de profesores de informática como medio de educar a los menores en el uso de estas redes sociales, a la vez que se potencien acciones de divulgación para la sensibilización de este problema mediante los medios de prensa y televisión.

Del mismo modo, se debería desarrollar por las redes sociales una tecnología más proteccionista y segura. Propuesta que ya se ha sugerido en Sudamérica a través del Memorándum de Montevideo (II Justicia, 2009); y la cual vemos muy atractiva y no es otra que crear una tecnología eficiente en "filtrado e implementación de moderación humana" para impedir la publicación de pornografía infantil u otro tipo de contenido para adultos, a la vez que un etiquetado de fotos mediante un reconocimiento facial, para así no etiquetar a personas en mensajes de cualquier tipo que puedan dañar su imagen o expresen pensamientos delictivos.

Reitero una idea, a mi parecer capital, en materia de autenticación que puede ser viable, al menos en la UE, gracias a las nuevas regulaciones existentes en Europa dentro del proyecto *E-signature* propuesto por el Plan de Acción E-justicia 2009-2013, que aún está en fase de desarrollo, y por la creciente implantación del DNI electrónico en España. Se trata de utilizar como medio de acceso a una red social como *Tuenti*, una opción de firma electrónica para validar nuestro perfil a través del proceso de firma electrónica que ofrece nuestro documento de identidad electrónico. De este modo, al obtener una firma electrónica tendríamos plena constancia de quien se esconde detrás de cada perfil, con lo que se dejaría de actuar bajo el anonimato de la red, se controlaría de

[9] El Departamento Jurídico y de Privacidad de Tuenti ha sido propuesto como candidato para recibir, en el año 2010, la mayor condecoración de la Guardia Civil (la Cruz de Plata al mérito civil) por su colaboración activa con dicho cuerpo policial.

forma exhaustiva la entrada de menores de edad y desaparecerían los fenómenos de suplantación de identidad. Una propuesta que necesitaría de un acuerdo entre las redes sociales destacadas españolas y el gobierno, pero que se debería tener en cuenta.

Esperemos que estas ideas sean tomadas en consideración para una futura y necesaria regulación en la materia, para contribuir así a que las generaciones futuras crezcan de una forma fiable y se familiaricen con las nuevas tecnologías desde una perspectiva marcada por la protección a su intimidad y velando siempre por su educación y seguridad.

El panorama existente en México

El caso de las redes sociales en México no escapa del turbio panorama legal que impera a nivel internacional. Tal como lo menciona Bueno de Mata, la falta de regulación permite que las redes sociales guarden en su interior potenciales peligros que acechan a los menores y a la población en general.

El presidente de la Comisión Nacional de los Derechos Humanos, Raúl Plascencia Villanueva señaló el 8 de septiembre de 2010 que en México 40% de la población escolar de primaria y secundaria sufre acoso por parte de sus compañeros (*bullying*); el dato por sí solo es impresionante, sin embargo la señal de alarma se incrementa debido a que este tipo de conductas está siendo trasladado al ciberespacio y una de las principales fuentes de propagación son las redes sociales. Mediante este tipo de conductas reprobables se pretende herir, perturbar y arruinar la imagen de los menores (Sosa, 2010).

Soluciones tecnológicas, jurídicas y uso responsable de la Internet

Es primordial recordar que el ciberespacio no es un lugar seguro debido a que trae consigo muchos riesgos (muy similares a los existentes en las grandes ciudades del mundo); sin embargo, en este espacio intangible, es mucho más difícil velar por la seguridad de los que circulan a través de él. Por todo ello es necesario generar acuerdos multilaterales en los que se establezcan los parámetros mínimos necesarios para proteger a los usuarios de las redes sociales, en especial a los menores, ya que son un colectivo extremadamente vulnerable. Es importante destacar que la protección de los menores en la red no va a depender únicamente de soluciones tecnológicas o jurídicas, ya que también implica un uso responsable, consciente e informado en el que los padres y educadores se involucren en el mundo de la tecnología.

La tecnología está superando a la humanidad día a día. Los avances ocurren en menos tiempo y el uso de nuevos artefactos nos obliga a mantener un constante aprendizaje; este suceso no se puede detener ni prohibir, al contrario, se debe fomentar y orientar hacia la obtención de beneficios sociales. El impulso hacia una educación en Tecnologías de la Información y Comunicación (TIC) debe tener como inspiración el concepto de autocuidado.

El autocuidado es nuestra mayor arma de defensa y es una actividad que no puede ser delegada en ninguna otra persona; en tal sentido, resulta esencial que nosotros empecemos a tomar conciencia de lo que implica permitir el acceso a nuestra información. Ya no podemos omitir leer las Políticas de Privacidad que manejan los sitios que solemos frecuentar en Internet. Debemos de desechar la pereza y analizar cada una de las cláusulas antes de proporcionar nuestros datos personales. Esta sencilla acción nos permitirá ejercer nuestro derecho a la protección de datos personales a través de denuncias ante el organismo encargado de resguardarlos, para que emita recomendaciones al sitio, cuando esas Políticas pudiesen llegar a violar nuestra privacidad.

Reorganizar y eliminar los malos hábitos burocráticos

La mayoría de las actividades que realizamos en la vida diaria nos obligan a proporcionar nuestros datos personales (adquisición de bienes, servicios, trámites…); todos nuestros movimientos quedan registrados y al final resulta complicado saber ¿quienes poseen toda esa información?, ¿quiénes tienen acceso a ella? y sobre todo, saber ¿para qué van a ser utilizados?. Uno de los principales peligros que genera el tratamiento de los datos personales es la configuración de perfiles, debido a que mediante diversos métodos de clasificación pueden llegar a ser capaces de generar intromisiones en nuestra vida privada.

En México tenemos varias identificaciones oficiales; entre ellas están: la Credencial para Votar proporcionada por el Instituto Federal Electoral (IFE), la Clave Única de Registro de Población (CURP), la Credencial del Instituto Mexicano del Seguro Social (IMSS)[10], el Pasaporte, la Cédula Profesional y alguna otra más que

[10] La cual es obligatorio presentar al momento de realizar algún trámite ante el Instituto desde el 1 de Junio de 2010.

por el momento escapa de mi mente. Como podemos observar, el gobierno de México ya nos ha proporcionado múltiples identificaciones; todas ellas son necesarias para realizar trámites en distintos sectores y cada una de ellas cuanta con diversos niveles de seguridad para evitar que sean falsificadas.

Podríamos decir que en materia de identificación en México se está siguiendo un sistema similar al que utiliza Austria, pero de manera descontrolada. Austria asigna un número de identidad único, pero prohíbe el uso directo de ese número a sus ciudadanos, y cada vez que necesitan utilizar ese número, su tarjeta de identidad crea un código sectorial específico para utilizarse en ese sector. Ese código está matemáticamente disociado de los otros códigos sectoriales para impedir que se puedan cruzar datos de los ciudadanos entre sectores (Alamillo Domingo, 2010). En México tenemos un número de identidad único (CURP) que va directamente asociado a todos los códigos sectoriales, y además tenemos la obligación de usarlo directamente al momento de realizar cualquier trámite. Por tanto, obtener la configuración del perfil de cualquier ciudadano resulta ser una tarea muy sencilla. Además, es importante señalar que existen trámites en los que se nos obliga a presentar más de una de las identificaciones anteriormente mencionadas.

Respecto a la forma en que desarrollan sus actividades las instituciones, "la cooperación interinstitucional permite reducir costos de información y generar mayor desempeño económico" (Ramírez e Peñaloza, 2006); tal idea se desarrolla a partir de los temas de institucionalidad que Douglas North toma en cuenta al establecer que "la importancia de las instituciones radica en que afectan el comportamiento económico al determinar, conjuntamente con la tecnología empleada, los costos de transacción, transformación y producción". Por ello, es importante que en México y en toda Iberoamérica las instituciones se transformen y empiecen a trabajar de manera coordinada para que todos los países se desarrollen adecuadamente y al mismo tiempo mantengan cifras positivas en el crecimiento económico.

Es evidente el caos que existe en materia de identificaciones en México; nos hace falta regular y controlar en primer lugar la asignación de códigos de identificaciones para los ciudadanos y en segundo lugar necesitamos reglamentar el uso de dichos códigos de identificación. Al regular este aspecto, evitaríamos engorrosas situaciones causadas por la falta de precaución en el resguardo de información, tal como sucedió hace poco con la puesta en venta de los datos del Registro Nacional de Usuarios de Telefonía Móvil (RENAUT) (Heredia, 2010). Si esos datos hubieran sido el resultado de un código matemáticamente disociado, no serían de interés para el comercio y, por tanto, se encontrarían a salvo de los delincuentes informáticos.

Nuestra alternativa: "los códigos disociados"

Tomando en cuenta lo anterior, propongo que, para identificar a los usuarios de redes sociales que tengan domicilio en la República Mexicana, se utilice un código disociado del número de identificación poblacional. En Nueva Zelanda realizaron un estudio económico respecto a los costos que implica su implementación; de dicho documento se obtuvieron cifras impactantes, ya que, al utilizarse estos códigos por las dependencias gubernamentales, se puede lograr un beneficio tangible en un periodo de 10 años, de entre $385 millones y $527 millones de dólares, porque evitan invertir en infraestructura duplicada y reducen el costo de las transacciones y los gastos administrativos (Study Link, 2012). Aunado a ello en Nueva Zelanda pretenden desarrollar un marco legislativo coherente que regule el Servicio de Verificación de Identidad Electrónica y que evite el uso indebido del sistema. Esta legislación neozelandesa va a ser desarrollada con una visión a futuro, por si deciden extender el uso de este sistema al sector privado (Nueva Zelanda, 2011).

En Estados Unidos de Norte América, el sector privado verifica la identidad de los compradores online con el apoyo de una compañía privada llamada *IDology*. Reznikov (2007) señala que el método que utiliza esta compañía, consiste en responder diversas preguntas cuyas respuestas únicamente puede conocer el usuario; dichas respuestas son contrastadas con información que se encuentra en Registros Públicos.

El uso de un código disociado dentro de una red social implicaría, a grandes rasgos, realizar los siguientes pasos:

Primer paso: Solicitar el código para registrarse en una red social (código RS)

La petición de un código se realizará preferentemente de manera directa ante la Secretaría de Educación Pública (SEP) o ante el Instituto Federal Electoral (IFE). No obstante, también se podrá realizar a través de formularios disponibles en las páginas web de la SEP y del IFE; sin embargo, el trámite de esas solicitudes será más lento, pues implicará obtener y confirmar telemáti-

camente una cita para acudir a recoger personalmente el código RS ante dichas dependencias. Estos formularios únicamente necesitarían el código disociado que le ha sido asignado al ciudadano para efectuar trámites ante ese sector, y el nombre de la red social a la que desean pertenecer.

Segundo paso: Localizar la identidad del solicitante

Una vez recibida la petición de emisión de un código RS, se procederá a realizar la búsqueda de la identidad del dueño de ese código disociado.

(a) Cuando se trate de menores de edad, la dependencia encargada de realizar la búsqueda será la Secretaría de Educación Pública (SEP), debido a que es el organismo gubernamental que tiene a su cargo los datos de los menores de edad escolarizados y además posee el nombre de los padres o tutores.

(b) Cuando se trate de un adulto, el Instituto Federal Electoral (IFE) será quien realice la pesquisa, porque el Registro Nacional de Electores se encuentra bajo su custodia y contiene los datos de identificación de casi todas las personas mayores de edad del país.

Al realizar esta acción, se verificarían tanto la identidad como la edad de ambos tipos de usuarios.

Tercer paso:Validar el código RS dentro de la red social

Una vez que ha sido entregado el código RS al solicitante, ese dato junto con su nombre y su fecha de nacimiento serán remitidos directamente a los gestores de la red social que desee ingresar; de ese modo, la validación de datos se efectuaría casi automáticamente al momento de registrarse, pues deberán coincidir nombre, apellidos, fecha de nacimiento y código RS de la persona que desee registrarse. Aunado a ello, para generar otra barrera de seguridad, la red social deberá pedir que se respondan preguntas claves para poder lograr el acceso pleno a sus servicios.

Una vez seguidos esos pasos, podemos concluir lo siguiente:

• A través de este sistema, los padres de familia quedarán directamente responsabilizados por el mal uso que de las redes sociales puedan hacer los menores y también se evitarán muchas conductas delictivas por parte de los adultos; en caso de que les roben la identidad, deberán notificar dicho hecho a la entidad ante la cual solicitaron el código, ya que con ella han firmado un contrato que les obliga a custodiarlo debidamente; no obstante el código se desactivará automáticamente si se introducen erróneamente las preguntas claves que den acceso a la red social.

• Esta opción de registro evitará que perfiles de adultos y menores puedan mezclarse, y solo se permitirá ligar el perfil de un menor a aquellas "solicitudes de amistad" de perfiles de los familiares que sean aprobadas previamente por los padres o tutores los cuales tendrán el deber de formar parte de la red de amigos de sus hijos.

Sin embargo, esta medida no será la única a realizarse, ya que se deben tomar algunas prevenciones especiales, por ejemplo:

• Las redes sociales que deseen incluir dentro de sus miembros a mexicanos, previamente deberán cumplir la normativa referente a la protección de datos personales.

• Cada persona podrá solicitar únicamente un código RS para cada red social a la que desee pertenecer; dicho código podrá ser desactivado en caso de que se comunique la introducción de datos erróneos al ingresar a la red social o en caso de robo de identidad; por tanto, el usuario tendrá que solicitar un nuevo código para poder ingresar a su antiguo perfil en esa red social.

• Los códigos RS serán asignados tomando en consideración el nombre de la red a la que se desea pertenecer; por tanto, únicamente podrán utilizarse para ese fin.

• A pesar de que la red social cuente con los datos reales de los usuarios, se deberá brindar la posibilidad de elegir entre usar el nombre real o un pseudónimo, pues habrá algunas personas que no quieran dar a conocer su nombre completo porque les afrente o porque, en algunos casos, es necesario conservar su privacidad (artistas, testigos protegidos, víctimas de acoso).

Es necesario resaltar que él código RS no permitirá ser miembro de una red social de manera 100% anónima, ya que esa cifra, a pesar de no encontrarse ligada al número de identidad único, sí se encontrará unida al número que permita localizar los datos del titular de ese código, los cuales solo podrán entregarse bajo orden judicial.

La red social ideal

Según Monsoriu Flor (2009, p. 121), "la red social ideal es aquella que se basa en el respeto en tres ámbitos: respeto a la legislación vigente, respeto a los legítimos derechos de terceros y respeto a los derechos de los usuarios del servicio". En tal sentido, la legislación vigente en México ya ha incorporado en su acervo el concepto Protección de Datos Personales el cual se encuentra garantizado constitucionalmente dentro de los artículos 6° fracciones II y III, 16 y 73 fracción O (México, 2010a). Además, para poder hacer efectiva esa garantía en el ámbito de las redes sociales, recientemente se publicó la Ley Federal de Protección de Datos Personales en Posesión de los Particulares. Uno de los puntos que más ha llamado mi atención es el referente a los Delitos en Materia del Tratamiento Indebido de Datos Personales, ya que no se establece pena alternativa y la sanción va desde los tres meses hasta los diez años de prisión; además, dicha pena recae directamente en la persona autorizada para tratar los Datos Personales (México, 2010b). Aunado a ello, es importante agregar que se publicará también el Reglamento de esta Ley.

Los legítimos derechos de tercero quedan protegidos a través de todas aquellas normas relacionadas con los Servicios de la Sociedad de la Información; entre ellas tenemos los Códigos Civil y Penal Federales, la Ley de la Propiedad Industrial y la Ley Federal del Derecho de Autor, etc.

Y finalmente, en relación con el respeto a los usuarios del servicio, tenemos lo que estipula la Ley Federal de Protección al Consumidor en el artículo 76 bis (México, 2010c). Mediante ella se obliga a los proveedores –que realizan transacciones a través de medios electrónicos– a mantener la confidencialidad de la información y se les prohíbe difundirla o transmitirla a otros si no cuentan con la autorización del consumidor otorgada por escrito. Además, se exige que informen acerca de las medidas de seguridad que disponen los usuarios de sus servicios, antes de que celebren cualquier transacción. Al mismo tiempo, les obliga a establecer mecanismos que adviertan que la información no es apta para niños, ancianos o enfermos.

Como podemos apreciar, en México se tiene la intención de salvaguardar los derechos de sus ciudadanos. Únicamente hace falta establecer las medidas necesarias para informar a la población, acerca de cuáles son algunas conductas de seguridad que pueden evitar riesgos al utilizar las redes sociales e Internet; al respecto en algunos Estados ya se ha empezado a difundir información para proteger a los menores; por ejemplo, en Baja California la Procuraduría de Derechos Humanos imparte talleres de capacitación en el que padres, alumnos y profesores reciben el adiestramiento necesario para poder detectar y prevenir casos de explotación infantil. Además, para reforzar toda esta lucha, dentro de la Secretaría de Seguridad Pública se cuenta con la Unidad de Delitos Cibernéticos especialmente dedicada a delitos contra menores.[11]

Debo insistir en el hecho de que los menores no tienen temor a los peligros que existen en Internet y, por tal motivo, es importante establecer la edad mínima para que puedan registrarse no solo en las redes sociales, sino también en cualquier actividad que implique la posibilidad de comunicarse con personas ajenas a su entorno, tales como salas de chat, juegos en línea, recepción de SMS, foros, mensajería en línea.

Está claro que en Internet todos somos vistos como consumidores; por ello, cualquier información que establezca alguna preferencia de nuestro estilo de vida se torna valiosa. Ante tal situación es necesario exigir a las redes sociales que, además de establecer restricciones por defecto en los perfiles de menores, *eviten preguntar datos que revelen nuestros gustos y que se tornan excesivos al momento de rellenar cualquier solicitud de registro* para poder pertenecer a ellas; aunado a lo anterior, *sería importante que desactivaran el etiquetado de fotografías, ya que favorecen conductas abusivas* por parte de vendedores, políticos e incluso pueden facilitar la comisión de ilícitos; y por último es necesario que acerquen el contenido legal de sus políticas de privacidad a los usuarios a través de un *lenguaje sencillo, coloquial y adecuado a la edad de quien utilizará sus servicios*.

La investigadora del Instituto Nacional de Ciencias Penales (INACIPE) Eloisa Quintero señala que 15 días son suficientes para que un pederasta logre su objetivo (Monsoriu Flor, 2009); por tanto, los padres de familia deben estar muy atentos a lo que hacen sus hijos cuando se encuentran utilizando Internet, ya que el tiempo de comisión es extremadamente corto. Además, ese peligro no es el único, pues también existe información que puede dañar el libre desarrollo de los menores (anorexia, bulimia, grupos pro suicidio, consumo y tráfico de drogas, prostitución). Es preciso inculcar el sentimiento de seguridad en los menores, ya que solo de ese modo sentirán la confianza necesaria para acercarse a sus padres, familiares o profesores y comentar-

[11] La cual pone a disposición de los ciudadanos el siguiente correo electrónico: ciberprevencion@sspslp.gob.mx

les la existencia de cualquier tipo de problema que surja mientras utilizan Internet. Al respecto se dice que "La nueva alfabetización digital tiene que dotarse de un enfoque conceptual crítico sobre el entorno tecnológico con el fin de facilitar la integración de las personas como sujetos críticos y activos, y no como meros consumidores de tecnologías y contenidos digitales" (Casado Ortiz y Ontiveros Baeza, 2006). El camino para lograr ese tipo de alfabetización puede ser largo, sin embargo no es imposible.

A pesar de que este estudio comparativo va dirigido a salvaguardar a los menores que utilizan las redes sociales, debo hacer hincapié en que también existe un grupo minoritario que requiere nuestra atención, pues ya está empezando a ser víctima de la delincuencia cibernética; me refiero a los Adultos en Plenitud, que en busca de compañía y comprensión, son engañados por mujeres y hombres que los dejan en la ruina. Recordemos que al envejecer nuestras capacidades disminuyen y nos volvemos vulnerables igual que los niños.

La realidad argentina

Consecuentemente, con lo expuesto resulta claro y de nadie escapa el hecho de que el anonimato que ofrecen las redes sociales es el sueño hecho realidad de múltiples tipos de delincuentes. Teóricamente coincidimos en la descripción del estado de situación expuesto por el colega Bueno de Mata. Está claro que el fenómeno *Redes Sociales* abarca el ámbito nacional, el internacional, el intercontinental, y fundamentalmente resulta transversal a las distintas realidades sociales. Motivo por el cual, en todo el mundo nos encontramos con iguales realidades e idénticas necesidades.

El proceso escalonado y continuo hacia la protección de los usuarios

La protección de usuarios en general y de menores en particular requiere un proceso gradual y progresivo, partiendo desde lo más simple; proporcionar información del riesgo que implica el uso de las nuevas tecnologías y además especificar cuales son los procedimientos adecuados para evitarlos. La información debe brindarse de modo tal que sea accesible y abundante teniendo en cuenta los grupos de afinidad y los medios de difusión disponibles. Para el logro de tales fines pueden otorgarse beneficios impositivos o recompensas a quienes se ocupen de tales tareas.

Simultáneamente es necesario implementar globalmente, desde cada una de las redes sociales, un mecanismo que permita identificar y responsabilizar a quienes utilizan los medios masivos de comunicación en perjuicio de menores y usuarios en general. Estos mecanismos tienen que estar al alcance de las sociedades menos desarrolladas o con inferior capacidad económica o tecnológica; de nada sirve un control tecnológico de excelencia aplicable en algún lugar del planeta, si desde otro distante la falta de controles o tecnología permite a los inescrupulosos perjudicar a terceros gozando de la más absoluta impunidad. Por ello debe implementarse medidas útiles, consensuadas y plasmando en recomendaciones o acuerdos que comprendan todos los grados de desarrollo relativo.

Variedad de normas convenientes pero inaplicables

Por otro lado, y respecto de la realidad actual, es necesario destacar que una de las actividades más difíciles de encarar es la regulación de este tipo de fenómenos manteniendo la hermenéutica jurídica de los ordenamientos legales de cada Estado. Resulta, por ejemplo en Argentina, que se reguló por decreto la libertad de contenido respecto de Internet, protegiendo derechos fundamentales y de rango constitucional, como la libertad de expresión, mientras que una ley posteriormente estableció determinadas restricciones, como, por ejemplo, del contenido pedófilo entre otros, cercenando claramente la libertad de expresión referida y sin derogar el decreto anteriormente mencionado. A nadie se le ocurriría criticar una ley que censura este tipo de actividad, pero la realidad es que resulta sumamente dificultosa y mas aún en los países que no integramos la comunidad europea. Al no contar con directivas comunitarias, con el simple cambio de un gobierno, temas tan sensibles como estos van y vienen de una postura a la diametralmente opuesta y esto es un claro problema a la hora de determinar la tendencia del modelo legislativo, que no puede ser obviada a la hora de sugerir soluciones posibles.

Otro factor fundamental es la falta de aplicación de gran cantidad de normas que son en teoría sumamente claras, legales, legítimas y convenientes. En la República Argentina, existe una ley de protección de datos personales, por demás similar a la "*Ley Orgánica de Protección de Datos de Carácter Personal*" española (España, 1999), la cual es de nula aplicación, ya que no funcionan los órganos de control, y, lamentablemente, la educación es insuficiente a los efectos de suplir las sanciones. Insistimos, no estamos en contra de la normativa, de hecho actualmente se está trabajando en el desarrollo

de estrategias de control, pero una vez más la realidad es una sola, y actualmente los controles respecto de los derechos sobre los datos personales son insuficientes debido a la falta de institucionalidad tal como lo menciona la colega Munive.

El conocimiento indudable de la identidad del usuario

Volviendo a lo sugerido por Bueno de Mata, la resolución del conflicto mediante la firma electrónica parece una solución excelente. El conocimiento fehaciente de la identidad del usuario de la red social resulta de innegable trascendencia y es posiblemente el punto de quiebre de los delitos de este tipo a través de estos medios. El inconveniente es que nuevamente nos encontramos con algunos problemas los argentinos: una ley nacional, reglamentada según las prescripciones correspondientes y legalmente vigentes, pero sin que exista a la fecha ningún organismo certificador, ya que la *licitación pública* realizada al efecto quedó vacante. Razón por la cual, el inconveniente no resulta de la legislación, sino de la aplicabilidad de la normativa; por ello resulta imperante para nuestros países tomar de manera coordinada las decisiones necesarias para poder hacer frente a esta serie de problemas.

Pareciera ser, según lo expuesto, que es muy difícil confiar al gobierno de un Estado, llámese Argentina o cualquiera de los países iberoamericanos que estén en similares condiciones, el control de la identidad o del contenido en las redes sociales.

No pudiendo contar con el Estado para su control y ante la imperativa necesidad de solucionar este flagelo, la solución principal debería recaer en la identificación de los usuarios y la garantía de cumplimiento para con eventuales responsabilidades que pudieran surgir de las órbitas tanto contractual como extracontractual, similar en principio a lo propuesto anteriormente por Federico Bueno.

De manera que si establecemos que lo necesario es determinar los responsables, la condición *sine qua non* es la identificación de los usuarios para que posteriormente estos respondan por sus actos en las redes. Esto solucionaría en principio el tema de los adultos, pero, si consideramos las edades a partir de las cuales se es responsable por los actos, nos encontramos con que eso resulta imposible quitar a los menores de las redes, sin menoscabar libertades y posibilidades de desarrollo respecto de los mismos. Creemos, entonces, que la responsabilidad por los mismos está contenida en el deber de cuidado de los padres.

Siguiendo con este razonamiento, serían los padres quienes deberían definir cuando y bajo que circunstancias sus hijos estarían capacitados para la utilización de dicha herramienta. Pero esta situación, previamente analizada, tiene la contrapartida de que muchas veces los padres, por falta de capacidad o interés, dejan de lado su rol y creen que consiguen una "niñera" de tiempo completo al dejar un ordenador y una conexión a Internet al alcance de los niños, en la seguridad de que por nada de lo que hagan sus hijos tendrán que responder.

Propuestas para controlar la identidad de los usuarios de las redes sociales

Considerando lo expuesto, ante la imposibilidad de contar con el Estado para el control de la identidad de los usuarios de las redes sociales, ante la necesidad de identificarlos y de encontrar la manera de responsabilizarlos (menores a través de sus padres o bien adultos), consideramos la posibilidad alternativa de *exigir a las redes sociales* que tomen *las medidas necesarias para la identificación de los usuarios*, bajo apercibimiento de *responder solidariamente por los eventuales daños causados a terceros*. Para el caso puntual de los delitos informáticos, donde no podrían ser condenadas personas jurídicas (al menos en Argentina), la eventual sanción podría ser un bloqueo para funcionar en el país (independientemente de la sanción que pudiera corresponderle a sus funcionarios y/o a otras personas físicas).

Como ejemplo de medidas podría requerirse, a la hora de inscribirse como usuario de una red social, la garantía de una tarjeta de crédito. Esto permitirá garantizar "prima facie" la identidad del usuario y su mayoría de edad, siendo que en los casos en que los padres autorizasen la utilización de estas redes por sus hijos menores de edad, prestándoles a dicho efecto los datos de su tarjeta, deberán ser mediante la misma, responsables por los daños que aquellos produjeran, con lo que posiblemente se genere una mayor conciencia y cuidado respecto de este tipo de actividades, tanto en los padres como en sus hijos. Para el hipotético caso de personas sin dicho instrumento de crédito, podría requerirse a la entidad bancaria oficial que otorgue un modo de identificación, cuyo responsable pueda ser inscripto en los registros de morosos de manera automática e inmediata al solo requerimiento fundado, basado en actividades dentro de una de estas redes sociales.

Finalmente, podría dudarse de la aceptación que podría tener una red social con estas características, pero ante esa duda caben dos respuestas a saber:

(a) Con una política de Estado fuerte como existe y se ha probado en algunos países, directamente prohibir el funcionamiento de las redes que no cumplan con este requisito u obligarlas a garantizar el cumplimiento de la responsabilidad solidaria si no exigen la referida autenticación de identidad.

(b) La conciencia de los usuarios de optar por una red segura. Es decir, si existiera la opción de realizar las mismas actividades que se realizan en Tuenti, Facebook, Orkut y demás, pero en una red donde la identidad de los usuarios esté garantizada y que esa garantía implique una responsabilidad por los actos realizados por cada usuario.

Estimo sin temor a equivocarme que, tarde o temprano, la elección de los usuarios sería por la última opción, lo que insisto, tarde o temprano, haría que el resto de las redes sociales se vuelquen a esta metodología a los fines de no perder usuarios ni encontrarse en litigios judiciales respondiendo de manera solidaria con los "delincuentes informáticos".

Conclusiones por países

A continuación, hemos decidido ir diseminando nuestras conclusiones por países, con el fin de establecer así una metodología ordenada. Debido a este sentir procedemos a dividir las conclusiones según los países investigados.

España

• La falta de regulación específica permite que los peligros que acechan a los menores en las redes sociales aumenten.

• A nivel comunitario y latinoamericano existen propuestas que permitirán erradicar los abusos a menores a través de la red.

• España es el único país en el que se ha incrementado la edad mínima para poder registrarse en *Facebook* (14 años).

• En relación con los servicios que proporcionan las redes sociales, es necesario unificar tanto la normativa como los criterios de medición para hacerla efectiva y exigible a todos los operadores con independencia del lugar desde operen.

• La adecuación a los Principios de la Unión Europea para unas Redes Sociales más Seguras hecha por la red social más popular en España ofrece a sus miembros muchas ventajas respecto a la privacidad.

• Las redes sociales están comenzando a incorporar medidas de seguridad; no obstante algunas redes sociales hacen caso omiso a estas recomendaciones y demandas sociales urgentes.

• Es necesario cibereducar a padres e hijos y divulgar medidas preventivas respecto al uso de las redes sociales a través de los medios de comunicación.

• La firma electrónica puede ser la solución adecuada para evitar el anonimato de los usuarios de las redes sociales y con ello garantizar una mayor seguridad a sus miembros.

México

• El 40% de la población escolar de primaria y secundaria sufre acoso por parte de sus compañeros; esta conducta está empezando a llevarse hacia el ciberespacio a través de las redes sociales.

• La protección de los menores en la red no depende únicamente de soluciones tecnológicas o jurídicas; también requiere un uso responsable, consciente e informado por parte de todos los actores sociales.

• En materia de identificaciones, en México hace falta regular y controlar la asignación de códigos de identidad y reglamentar el uso de los mismos.

• Para identificar a los usuarios de redes sociales que tengan domicilio en la República Mexicana, se podría utilizar un código disociado del número de identificación poblacional.

• Es necesario exigir a las redes sociales que acerquen el contenido legal de sus políticas de privacidad a los usuarios a través de un lenguaje sencillo, coloquial y adecuado a la edad de quien utilizará sus servicios.

• Es preciso inculcar el sentimiento de seguridad en los menores, ya que solo de ese modo sentirán la confianza necesaria para acercarse a sus padres, familiares o profesores y comentarles la existencia de cualquier tipo de problema que surja mientras utilizan Internet.

Argentina

• Es necesario brindar información de manera accesible y abundante a los usuarios para evitar riesgos.

• Los controles de los derechos sobre los datos personales son insuficientes.

• Es difícil confiar al gobierno de un Estado el control de la identidad o del contenido en las redes sociales.

• Es imperante poder identificar a los usuarios para que respondan de sus actos en las redes.

• Las redes sociales deben tomar las medidas necesarias para la identificación de los usuarios bajo apercibimiento de que responderán solidariamente por eventuales daños causados a terceros.

• Las tarjetas de crédito podrían utilizarse para garantizar la identidad de los usuarios.

• Los usuarios deben tomar conciencia y optar por el uso de las redes sociales que más seguridad les proporcionen.

Referencias

II JUSTICIA. 2009. Memorándum sobre la protección de datos personales y la vida privada en las redes sociales en Internet, en particular de niños, niñas y adolescentes http://www.pantallasamigas.net/memorandum-montevideo-privacidad-proteccion-datos-infancia-adolescencia-menores-redes-sociales.pdf. Acceso el: 19/02/2013.

AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS (AEPD). 2012. http://www.agpd.es/portalwebAGPD/index-ides-idphp.php. Acceso el: 21/03/2013.

ALAMILLO DOMINGO, I. 2010. *Robo de identidad y protección de datos*. Cizur Menor, Aranzadi, 324 p.

BUJOSA VADELL, L. 2008. Proceso penal europeo y enjuiciamiento de menores. *Justicia: Revista de Derecho Procesal*, **3-4**:129-178.

CASADO ORTIZ, R.; ONTIVEROS BAEZA, E. 2006. *Claves de la alfabetización digital*. Madrid, Fundación Telefónica, 317 p.

CHACÓN MEDINA, A. 2003. Una nueva cara de Internet: el acoso. *Revista Ética-Net*, **1**:1-10.

COMISIÓN EUROPEA. 2009. Self-regulation for a Better Internet for Kids. Disponible en: http://ec.europa.eu/digital-agenda/en/self-regulation-better-internet-kids. Acceso el: 15/11/2013.

D.O.U.E. 2009. IV. Plan de Acción Plurianual 2009-2013 relativo a la justicia en red Europea. 31 mar.

ESPAÑA. 1999. Ley 15/1999. Ley Orgánica de Protección de Datos de Carácter Personal (LOPD). 13 dec.

GUNDÍN, F. 2012. *Ciberbullying* o *ciberacoso:* el oscuro lado criminal de las redes sociales. *Revista de Derecho Penal*, **36**:67-93.

HEREDIA, C. 2010. Sigue sin explicarse filtración del RENAUT. *El Siglo de Durango.* Disponible en: http://www.elsiglodedurango.com.mx/noticia/283173.sigue-sin-explicarse-filtracion-del-renaut.html. Acceso el: 15/11/2013.

IDOLOGY. 2013. Disponible en: http://www.idology.com/. Acceso el: 15/11/2013.

MÉXICO. 2010a. Constitución Política de los Estados Unidos Mexicanos. Disponible en: http://www.ordenjuridico.gob.mx/Constitucion/cn16.pdf. Acceso el: 15/11/2013.

MÉXICO. 2010b. Ley Federal de Protección de Datos Personales en Posesión de los Particulares. Disponible en: http://www.normateca.gob.mx/Archivos/50_D_2414_05-07-2010.pdf. Acceso el: 15/11/2013.

MÉXICO. 2010c. Ley Federal de Protección al Consumidor. Disponible en: http://www.normateca.gob.mx/Archivos/66_D_3582_11-11-2013.pdf. Acceso el: 15/11/2013.

MONSORIU FLOR, M. 2009. *Manual de redes sociales en Internet: aprende a usar Tuenti, Facebook, Fotolog, Myspace, etc., ¡mejor que tus hijos!* España, Creaciones Copyright, 250 p.

NUEVA ZELANDA. 2011. Tesorería. Electronic Identify Verification Bill. August 30, 2011. Department of Internal Affairs. Regulatory Impact Statement. Disponible en: http://www.treasury.govt.nz/publications/informationreleases/ris/pdfs/ris-dia-eiv-aug11.pdf. Acceso el: 15/11/2013.

PEW RESEARCH. 2014. Disponible en: http://www.pewinternet.org/. Acceso el: 04/02/2014.

RAMÍREZ J.C.; PEÑALOZA M.C. 2006. La coordinación en las políticas públicas: elementos e institucionalidad. Comisión Económica para América Latina y el Caribe (CEPAL). Disponible en: http://www.eclac.cl/dds/noticias/paginas/4/26924/Paper_RamirezyPenaloza.pdf. Acceso el: 15/11/2013.

REZNIKOV, B. 2007. Can I See Some ID? Age Verification Requirements for the Online Liquor Store. *Shidler Journal for Law, Commerce & Technology*, **4**(5):1-13.

SOSA, M. 2010. CNDH: 40% de estudiantes sufre bullying. *El Universal,* Disponible en: http://www.eluniversal.com.mx/notas/707516.html. Acceso el: 01/07/2014.

STUDY LINK. 2012. The igovt logon service. Disponible en: http://www.studylink.govt.nz/about-studylink/media-releases/2012/igovt-is-here-2.html Acceso el: 01/07/2014.

TUENTI. 2012a. Disponible en: http://blog.tuenti.com/importante-crecimiento-de-usuarios-en-tuenti/. Acceso el: 15/11/2013.

TUENTI. 2012b. Disponible en: www.tuenti.com. Acceso el: 15/11/2013.

Submetido: 22/01/2014
Aceito: 24/03/2014