

EL DERECHO DE LAS NIÑAS, NIÑOS Y ADOLESCENTES
A LA PROTECCIÓN DE SUS DATOS PERSONALES:
EVOLUCIÓN DE DERECHOS Y SU EXIGENCIA FRENTE A LAS REDES SOCIALES

Lina Ornelas

[...] la humanidad debe al niño
lo mejor que puede darle.¹

Introducción

El derecho a la vida privada es un valor que toda sociedad democrática debe respetar. Por tanto, a efecto de asegurar la autonomía de los individuos para decidir los alcances de su vida privada, debe limitarse el poder tanto del Estado como de organizaciones privadas, de cometer intromisiones ilegales o arbitrarias en dicha esfera personal. En particular, debe protegerse la información personal que niñas, niños y adolescentes proporcionan e intercambian en Internet a efecto de impedir su utilización inadecuada con fines distintos para los cuales ellos la proporcionaron.

Debe existir un balance entre asegurar la libertad de expresión en Internet de las niñas, niños y adolescentes sin que se afecte su dignidad como personas, ya que ellos tienen una expectativa razonable de privacidad al compartir su información en ambientes digitales, dado que consideran que se encuentran en un “espacio privado” sin tener consciencia plena de que son observados y monitoreados.

La evidencia muestra que en todos los países, se han verificado afectaciones al desarrollo de la personalidad de menores de edad, derivado de las invasiones a los espacios de intercambio de información e imágenes que ellos frecuentan.² Los perfiles creados son almacenados, por lo que, aún borrada dicha información en Internet, ésta podrían ser utilizada en el futuro para conculcar otros derechos y libertades de los menores de edad ya en su vida adulta. Como afectación concreta podría ilustrarse a manera de ejemplo la no obtención de un determinado empleo por el hecho de que se conozcan cuáles eran sus gustos o preferencias durante la adolescencia.

Es innegable que hay un gran interés por conocer la información de los menores de edad. Internet ha facilitado dicha tarea. Distintos actores explotan la información de este

LECTURAS

sector de la población, tales como la industria, a la cual le interesa por ejemplo, conocer hábitos de consumo, lugares visitados y su frecuencia, composición y situación de las familias, entre otros aspectos.

Por su parte, los trasgresores de la ley -ahora también virtuales- obtienen información de los propios menores de edad o bien, la extraen por otros medios, para la comisión de delitos como el secuestro, trata o explotación sexual.

Frente a la vulnerabilidad de los menores de edad y las nuevas formas de convivencia social a través de redes sociales digitales, el derecho no puede quedarse rezagado. Internet es un espacio lleno de oportunidades, es la puerta al mundo del conocimiento urbi et orbe, y uno de los nuevos roles del Estado consiste en el deber de esclarecer que no se trata de un espacio sin ley.

De tal forma que, el presente artículo se propone reflejar la evolución que han tenido los derechos humanos en general; el reconocimiento reciente de los derechos del niño y el nacimiento de un nuevo derecho fundamental a la protección de datos personales; las propuestas del Memorándum sobre la Protección de datos personales y la vida privada en las redes sociales en Internet, en particular de niños, niñas y adolescentes –Memorándum de Montevideo-, para concluir que los principios y derechos de protección de datos también resultan aplicables a este colectivo, y por tanto, el Estado debe actuar para garantizar su efectiva tutela.

Evolución de los derechos humanos

Los derechos humanos son normas que reconocen y protegen la dignidad de todos los seres humanos. Desde la perspectiva occidental de los derechos humanos, estos rigen la forma en que los individuos viven en sociedad, así como su relación con los gobiernos y las obligaciones que los gobiernos tienen para con ellos. De tal forma que, la ley de los derechos humanos obliga a los gobiernos a tomar una serie de medidas, y les impide tomar otras.

Los individuos, por su parte, también tiene responsabilidades: al hacer uso de sus derechos humanos, deben respetar los derechos de los demás. De esta forma, ningún gobierno, grupo o persona individual tiene derecho a llevar a cabo acto alguno que vulnere los derechos de los demás.

Los derechos humanos están basados en el respeto a la dignidad y el valor de cada persona como individuo y también como miembro de la sociedad. La responsabilidad para asegurar que los derechos sean respetados, protegidos y satisfechos reside finalmente en los gobiernos nacionales.

DERECHO DE NIÑAS, NIÑOS Y ADOLESCENTES

Esta responsabilidad también concierne a otros elementos de la sociedad a nivel de las instituciones internacionales, pasando por la comunidad y llegando hasta los individuos en sus familias.

Sin embargo, cabe recordar que lo que hoy se conoce como derechos humanos, es producto de la evolución histórica reflejada en generaciones de derechos. Esto es, los derechos humanos para su comprensión, han sido divididos en categorías históricas que encuentran sus orígenes en el seno de la modernidad.

Esta perspectiva evolutiva de los derechos humanos implica el reconocimiento de nuevos derechos que intentan dar respuesta, en su gran mayoría, a las nuevas necesidades históricas. Por otro lado, otros suponen la redimensión de viejos derechos.³ Tal como acontece en el fenómeno continuamente evolutivo de la sociedad tecnológica.

Derivado de lo anterior, ha prevalecido el reconocimiento de tres generaciones de derechos⁴ y se vislumbra una nueva oleada; aquella relativa a los derechos en el ciberespacio y la libertad informática.⁵ Así, cada etapa ha correspondido a un momento ideológico y social, con características particulares y rasgos diferenciadores, dependiendo de las necesidades de cada proceso evolutivo.

De tal forma que, la época burguesa del siglo XVIII marca el inicio de las etapas de los derechos humanos y, surgen de la Revolución Francesa como rebelión contra el Absolutismo. Las libertades individuales y la defensa de la persona se enmarcan como limitantes al poder público. Esta fase, se enfoca en la no injerencia con las libertades individuales y se configuran una serie de derechos relativos al aislamiento, tal como lo fue el derecho al honor, a la vida, a la integridad personal, así como el propio reconocimiento a la intimidad de la persona. Derecho que hoy, como consecuencia del desarrollo tecnológico y las nuevas formas de comunicación e información, ha sido necesario reformular en su alcance y contenido.

En consecuencia, una segunda generación de derechos humanos, encuentra sus orígenes en las luchas sociales del siglo XIX y abarca hasta ya entrado el siglo XX. Estos movimientos reivindicatorios pusieron en tela de juicio la necesidad de contemplar el catálogo de derechos y libertades de la primera generación, con una segunda oleada de derechos económicos, sociales y culturales, incorporados en la Declaración Universal de 1948, debido a los cuales, el Estado de Derecho pasa a una etapa superior, es decir, a un Estado Social de Derecho.

Dicha fase, se enfoca en garantizar los derechos de participación a través del involucramiento activo de los poderes públicos mediante prestaciones y servicios; más aun, se incorpora de una tradición del pensamiento humanista y socialista. Si bien, los derechos de primera generación defendían a los ciudadanos frente al poder estatal, en esta etapa se exige cierto grado de intervención del Estado para garantizar un acceso igualitario a los derechos de carácter económico y social, esto es, para compensar las desigualdades naturales e inherentes a todo entorno social.

LECTURAS

Cabe destacar que, en los años transcurridos desde la Declaración Universal de Derechos Humanos de 1948, y con mayor urgencia desde el final de la Guerra Fría, un gran sistema internacional de lo que se llaman instrumentos jurídicos del activismo y la defensa se ha desarrollado para proteger los derechos humanos. En otras palabras, se han integrado en los sistemas jurídicos de la gran mayoría de los Estados.

En consecuencia al intervencionismo estatal para garantizar los derechos de segunda generación, subyace la tercera generación encaminada a salvaguardar los derechos de la solidaridad. Esta generación encuentra su auge a partir de la segunda mitad del siglo XX, donde se incentiva el progreso social y la calidad de vida de todos los pueblos.

Los derechos de tercera generación, son el resultado del reconocimiento de un nuevo contexto en el que surgen necesidades humanas particulares y donde las exigencias obligan a desarrollar nuevos derechos que garanticen el acceso universal a formas más avanzadas de ciudadanía y civilidad, de libertad y de calidad de vida.

Más aun, son indicios claros que el mundo cambió drásticamente en la última mitad del siglo XX. Transformación que es perceptible en nuestros días y que tiende a continuar. Está revolución se hace latente con mayor claridad en el uso de las nuevas tecnologías, vislumbrándose así el nacimiento de una cuarta generación de derechos humanos, en los que la universalización del acceso a la tecnología, la libertad de expresión en la web y la libre distribución de la información juegan un papel fundamental y son elementos esenciales para su definición.

Gracias al desarrollo generacional de los derechos y a su incorporación en el sistema jurídico internacional, hemos podido alcanzar la difusión global de los derechos humanos. Por lo tanto, hoy se da por sentado que corresponde al Estado y a la sociedad en su conjunto, el deber de proteger a cada individuo y garantizar el respeto irrestricto a los derechos humanos en su conjunto.

Evolución de los derechos del niño

En lo que respecta a la protección del niño en particular, esta idea no es añeja, en tanto que es a finales del siglo XX cuando se reconoce a éste como sujeto de derechos. Aunado al hecho que, es en tiempos relativamente recientes que evoluciona la sociedad de la información y se precisa la protección del niño en este ámbito.

En 1945, la Carta de las Naciones Unidas estableció las bases de la Convención sobre los Derechos de los Niños -en adelante, la Convención- al exhortar a todos los países a promover y alentar el respeto por los derechos humanos y las libertades fundamentales para todos. Posteriormente, con la aprobación de la Declaración Universal de Derechos Humanos se reforzó la idea del respeto a los derechos de la infancia.

DERECHO DE NIÑAS, NIÑOS Y ADOLESCENTES

La segunda Declaración de los Derechos del Niño, adoptada en 1959, consagra algunos principios de fundamental importancia en esta materia. En particular, el derecho del niño a una protección especial se vincula con el concepto del desarrollo integral del niño, de su libertad y de su dignidad (v. Principio 2).

Posteriormente, con la Declaración de los Derechos del Niño y la consiguiente Convención, se establecen los derechos y obligaciones para asegurar el respeto irrestricto de la infancia.⁶ Este último es reconocido como el instrumento internacional por excelencia para la protección de la infancia.

La Convención es el tratado internacional que ha sido más ampliamente ratificado en la historia de las Naciones Unidas. Ha sido ratificada por 192 países desde que la Asamblea General de las Naciones Unidas la aprobó de manera unánime en noviembre de 1989.⁷ Si bien, es una Convención articulada ad hoc para la protección de la niñez - pues se concluyó que los menores de 18 años precisan de cuidados y protección especiales-,⁸ también es cierto que, está fundamentada en otros instrumentos internacionales como la Declaración Universal de los Derechos Humanos, el Pacto Internacional de Derechos Civiles y Políticos y el Pacto Internacional de Derechos Económicos, Sociales y Culturales.⁹ De tal forma que la normatividad internacional sobre derechos humanos contempla dentro del término niño tanto a las niñas y niños como a los adolescentes.

Es de hacer notar que el Preámbulo de la Convención reitera una frase contenida en el Preámbulo de la Declaración de 1959, que reza a la letra: “el niño, por su falta de madurez física y mental, necesita protección y cuidado especiales, incluso la debida protección legal [...]”.¹⁰

La Convención además de estar fundamentada en la Declaración de 1959 y otros instrumentos internacionales ya mencionados, está basada en diversos sistemas jurídicos y tradiciones culturales, además se compone de normas y obligaciones. Estas normas básicas -denominadas también derechos humanos- establecen derechos y libertades mínimas que los gobiernos deben cumplir y, se basan en el respeto a la dignidad y el valor de cada individuo, independientemente de su raza, color, género, idioma, religión, opiniones, orígenes, riqueza, nacimiento o capacidad.¹¹

Cabe mencionar que la Convención es el primer instrumento jurídicamente vinculante que incorpora toda la gama de derechos humanos: civiles, culturales, económicos, políticos y sociales. En 54 artículos y dos Protocolos Facultativos,¹² se definen los derechos básicos que deberán disfrutar todos los niños y niñas inherentes a su dignidad humana y desarrollo armonioso. De tal forma que, la Convención es un documento moderno que refleja una nueva visión sobre la infancia, como seres humanos y titulares de sus propios derechos.¹³

Al ser un instrumento internacional ratificado por los Estados, éstos se comprometen a cumplir con un código de obligaciones vinculantes a favor de la infancia. Al aceptar

LECTURAS

las obligaciones -mediante su ratificación o adhesión-, los gobiernos se comprometen a proteger y asegurar los derechos de la infancia y aceptan que se les considere responsables de este compromiso ante la comunidad internacional. En consecuencia, los Estados parte de la Convención están obligados a llevar a cabo todas las medidas y políticas necesarias para proteger el interés superior del niño y,¹⁴ son vigilados por el Comité de Derechos del Niño -órgano de expertos independientes que supervisa la aplicación de la Convención y los dos Protocolos, por sus Estados partes-.

En este tenor, es la sociedad en su conjunto quien debe asegurar su cumplimiento como una obligación jurídica, un imperativo moral y una prioridad en materia de desarrollo. Se entiende que es labor del Estado, la sociedad y la familia -cada uno en su ámbito de competencia- hacer cumplir las disposiciones estipuladas en la Convención. Las normas y los principios que se articulan en la Convención solamente pueden convertirse en realidad cuando sean respetados por todos, en la familia, en las escuelas y en otras instituciones que proporcionan servicios a la niñez, en las comunidades y en todos los niveles de la administración pública.

La Convención ofrece una visión del niño como individuo y como miembro de una familia y una comunidad, con derechos y responsabilidades apropiadas para su edad y etapa de desarrollo.

A este respecto, vale la pena mencionar que según la Convención, son los padres quienes tienen la responsabilidad primordial tanto de la crianza de sus hijos como de la satisfacción de las necesidades que permitan su sano desarrollo.¹⁵ En la medida en que los padres, no estén en condiciones de cumplir con estas responsabilidades por sus propios medios, el Estado tiene el deber de apoyarlos -v. arts. 18.2 y 27.3-. Esta relación de co-garantes es reafirmada por el artículo 3.2. que establece a la letra lo siguiente:

“2. Los Estados Partes se comprometen a asegurar al niño la protección y el cuidado que sean necesarios para su bienestar, teniendo en cuenta los derechos y deberes de sus padres, tutores u otras personas responsables de él ante la ley y, con este fin, tomarán todas las medidas legislativas y administrativas adecuadas”.

De tal forma que, en la medida que los padres no cumplan sus obligaciones a cabalidad, las autoridades tienen el derecho y el deber de intervenir para proteger los derechos del niño. En lo posible, la intervención consistirá en dar a los padres la orientación y el apoyo necesarios para superar los problemas que afectan la forma como cumplen estos deberes.

En este sentido, la Convención prevé disposiciones que abarcan derechos y libertades civiles, el entorno familiar, la salud básica y el bienestar, la educación, recreación, las actividades culturales y las medidas especiales necesarias para su protección.

En lo relativo a los derechos, la Convención establece principios fundamentales como

DERECHO DE NIÑAS, NIÑOS Y ADOLESCENTES

la no discriminación, el derecho a la supervivencia, al desarrollo y la opinión del niño. Asimismo, establece como principio básico contemplar en todo momento el interés superior del niño como consideración primordial en todas las medidas y decisiones que le atañen, y debe utilizarse para resolver cualquier confusión entre los diferentes derechos.

En particular, tomar en consideración los puntos de vista de los niños y las niñas se refiere a la importancia de escuchar y respetar su opinión en todas las cuestiones relacionadas con sus derechos. De ahí que la Convención ha exhortado a los países a promover una participación activa, libre y significativa de la infancia en las deliberaciones para tomar decisiones que les afecten.

Cabe destacar, para efectos del presente análisis, el artículo 16 de la Convención establece el derecho y obligación a la protección del niño, por ministerio de ley, y a letra dispone lo siguiente:

- “1. Ningún niño será objeto de injerencias arbitrarias o ilegales en su vida privada, su familia, su domicilio o su correspondencia ni de ataques ilegales a su honra y a su reputación.
2. El niño tiene derecho a la protección de la ley contra esas injerencias o ataques”.¹⁶

Por otra parte, la participación de la niñez constituye un aspecto con grandes potenciales en el vasto derecho de la infancia. También en esta área la Convención ha incorporado las bases para una profunda transformación cultural, introduciendo el principio de la autonomía progresiva de la infancia, tal como se consagra en el artículo 12.¹⁷

Asimismo, en el artículo 19 se establece la obligación del Estado a proteger al niño contra toda forma de perjuicio o abuso físico o mental, descuido o trato negligente, malos tratos o explotación, incluido el abuso sexual, mientras el niño se encuentre bajo custodia de los padres. A la letra señala lo siguiente:

- “1. Los Estados Partes adoptarán todas las medidas legislativas, administrativas, sociales y educativas apropiadas para proteger al niño contra toda forma de perjuicio o abuso físico o mental, descuido o trato negligente, malos tratos o explotación, incluido el abuso sexual, mientras el niño se encuentre bajo la custodia de los padres, de un representante legal o de cualquier otra persona que lo tenga a su cargo.
2. Esas medidas de protección deberían comprender, según corresponda, procedimientos eficaces para el establecimiento de programas sociales con objeto de proporcionar la asistencia necesaria al niño y a quienes cuidan de él, así como para otras formas de prevención y para la identificación, notificación, remisión a una institución, investigación, tratamiento y observación ulterior de los casos antes descritos de malos tratos al niño y, según corresponda, la intervención judicial”.¹⁸

LECTURAS

Por su parte, en el marco interamericano sobresalen el Pacto Interamericano de Derechos Civiles y Políticos y la Convención Americana, que reconocen el derecho del niño a “las medidas de protección que su condición de menor requiere”. Si bien, la normativa interamericana no contempla una definición explícita del niño, el artículo 4.1. de la Convención Americana precisa que el derecho a la vida “estará protegido por la ley y, en general, a partir del momento de la concepción”.¹⁹ Asimismo, en el artículo 19 relativo a los derechos del niño, se lee:

“Todo niño tiene derecho a las medidas de protección que su condición de menor requieren por parte de su familia, de la sociedad y del Estado”.²⁰

Esto es, la Convención Americana sigue lo establecido en la Convención al establecer que los niños y niñas necesitan protección especial precisamente por ser niños, y por lo tanto dependientes y potencialmente vulnerables.

Ahora bien, resulta pertinente señalar que pese a ser un tratado vinculante para los países que lo han ratificado, la Convención es un instrumento legal relativamente joven y en proceso de implementación en todos los Estados miembros.

De tal forma que, veinte años después de la aprobación de la Convención puede afirmarse que su implementación en América Latina continúa siendo un proceso dinámico y continuo no solo en su relación con las reformas legales y modelos institucionales, sino también respecto a cualquier situación nueva que pueda afectar directa o indirectamente la vida o libre desarrollo de los niños, niñas y adolescentes –tal es el caso de las tecnologías del conocimiento y la información–.

Un nuevo derecho fundamental: la protección de datos personales

Una vez que se ha abordado la evolución de los derechos humanos, conviene puntualizar que el derecho a la protección de datos personales como se concibe en la actualidad, también deviene de una transformación, desde la concepción del derecho a la vida privada y la intimidad, hasta la conformación de un nuevo derecho fundamental dotado de caracteres propios, que otorgan a la persona un haz de facultades concretas. Por tanto, se trata en sí mismo de un derecho activo.²¹

Diversos instrumentos internacionales reconocieron el derecho de toda persona a no ser objeto de injerencias en su vida privada o familiar.²² Aunado al desarrollo normativo y los avances científicos y tecnológicos, surge en Europa el germen y acuñación del derecho a la protección de datos como se desarrolla en líneas subsiguientes.

En 1967 se constituyó en el seno del Consejo de Europa una Comisión Consultiva para estudiar las tecnologías de información y su potencial agresividad hacia los derechos

de las personas, especialmente en relación con su derecho a la intimidad. Como fruto de la Comisión Consultiva surgió la Resolución 509 de la Asamblea del Consejo de Europa sobre los “derechos humanos y nuevos logros científicos y técnicos”.²³

En un momento posterior, surgen diversas leyes nacionales alrededor de Europa. De tal forma que en 1977 era aprobada la Ley de Protección de Datos de la República Federal Alemana, mucho más ambiciosa que su predecesora del Land de Hesse. En 1978 corresponde el turno a Francia mediante la publicación de la Ley de Informática, Ficheros y Libertades, aún vigente. Otros países entre los que se emitió regulación en la materia son Dinamarca con las leyes sobre ficheros públicos y privados (1978), Austria con la Ley de Protección de Datos (1978) y Luxemburgo con la Ley sobre la utilización de datos en tratamientos informáticos (1979).²⁴

Hacia la década de los años ochenta -cuando comienzan a utilizarse las primeras computadoras personales o PC's surgen los instrumentos normativos en los que se plasma un catálogo de derechos de los ciudadanos para hacer efectiva la protección de sus datos, así como las medidas de seguridad a observar por parte de los responsables de los ficheros. Es en esta década cuando desde el Consejo de Europa se dio un respaldo definitivo a la protección de la intimidad frente a la potencial agresividad de las tecnologías, siendo decisivo para ello la promulgación del Convenio Número 108 para la protección de las personas con respecto al tratamiento automatizado de los datos de carácter personal -en adelante, el Convenio 108-.²⁵

De modo que, existen diversos instrumentos internacionales que dan fundamento al derecho a la protección de datos personales entre los que destacan los que se desarrollan brevemente a continuación.

Directrices de la Organización para la Cooperación y el Desarrollo Económico

La recomendación de la Organización para la Cooperación y el Desarrollo Económico -OCDE- en la que se contienen las “Directrices relativas a la protección de la intimidad y de la circulación transfronteriza de datos personales” -en adelante, directrices de la OCDE-,²⁶ fue adoptada el 23 de septiembre de 1980, y constituye el primer instrumento en el ámbito supranacional que analiza a profundidad el derecho a la protección de datos de carácter personal.²⁷

Estas Directrices se emiten partiendo de una realidad innegable que la OCDE vislumbró y que se traduce en tres problemáticas centrales, a saber:

El uso de la tecnología para el tratamiento de datos personales, las posibilidades bastante extendidas de almacenamiento, contrastación, vinculación, selección y acceso a los mismo que en combinación con la informática y la tecnología de telecomunicaciones, pueden poner los datos personales simultáneamente a disposición de miles

LECTURAS

de usuarios en lugares geográficamente dispersos y la creación de redes complejas de datos nacionales e internacionales.

El peligro que representa las disparidades en las legislaciones nacionales tendentes a conciliar la protección de la información de carácter personal con la transmisión de enormes cantidades de datos a través de las fronteras nacionales, a fin de impedir vulneraciones a los derechos fundamentales de los titulares de esa información como el almacenamiento ilícito de datos personales o el abuso o la revelación no autorizada de los mismos.

La diversidad en las legislaciones nacionales que trae como consecuencia restricciones a la circulación u obstáculos a la libre circulación transfronteriza de los datos personales, ocasionando graves trastornos en importantes sectores de la economía.

Su adopción se fundamenta en la constatación por parte del Consejo de la OCDE de la inexistencia de uniformidad en la regulación de esta materia en los distintos Estados miembros, lo que dificultaba el flujo de los datos personales entre los mismos.²⁸

Las directrices de la OCDE se componen de 5 secciones fundamentales. En la primera parte, se establecen las definiciones aplicables, la parte segunda señala los principios básicos relativos al tratamiento de los datos personales. Por su parte, la tercera sección está dedicada a las transferencias internacionales de datos y la cuarta trata, en términos generales, sobre los medios de implantación de los principios básicos expuestos en las partes anteriores. Finalmente, la quinta tiene que ver con cuestiones de asistencia mutua entre los países miembros.

De manera específica, el Capítulo II de dichas directrices señala los siguientes principios básicos en materia de protección de datos personales:

“Principio de limitación de la recogida

7. Debería haber límites en la recogida de datos personales y tales datos deberían recabarse mediante medios lícitos y justos y, en su caso, con el conocimiento o consentimiento del sujeto de los datos.

Principio de calidad de los datos

8. Los datos personales deberían ser pertinentes a los efectos para los que se vayan a utilizar y, en la medida necesaria a tales efectos, deberían ser exactos y completos, y mantenerse al día.

Principio de especificación de la finalidad

9. Los efectos para los cuales se recojan los datos personales deberían especificarse en el momento de la recogida, a más tardar, y la posterior utilización quedar limitada al cumplimiento de tales efectos o de aquellos otros que no sean incompatibles con los mismos y que se especifiquen en cada ocasión en que se cambie la finalidad.

Principio de limitación de uso

10. Los datos personales no deberían revelarse, hacerse disponibles o utilizarse de

DERECHO DE NIÑAS, NIÑOS Y ADOLESCENTES

otro modo a efectos que no sean los especificados conforme al Apartado 9, salvo:

- a) con el consentimiento del sujeto de los datos, o
- b) por imperativo legal.

Principio de salvaguardas de seguridad

11. Los datos personales deberían protegerse, mediante salvaguardas de seguridad razonables, frente a tales riesgos como pérdida de los mismos o acceso, destrucción, uso, modificación o revelación no autorizados.

Principio de apertura

12. Debería haber una política general de apertura respecto a avances, prácticas y políticas con respecto a los datos personales. Deberían existir medios fácilmente disponibles para establecer la existencia e índole de los datos personales, y de las principales finalidades para su uso, así como la identidad y domicilio del controlador de los datos.

Principio de participación individual

13. La persona debería tener derecho a:

- a) recabar, del controlador de los datos o de otro modo, confirmación de si el controlador tiene o no tiene datos correspondientes a la misma;
- b) hacer que se le comuniquen los datos correspondientes a ella dentro de un plazo razonable, por una cuota en su caso, que no sea excesiva, de manera razonable y de una forma que le resulte fácilmente inteligible;
- c) que se le den los motivos para ello, en virtud de los subapartados a) y b), si su solicitud fuere denegada y ella pueda impugnar tal denegación, y
- d) impugnar los datos que se refieran a ella y, si la impugnación prospera, hacer que se supriman, rectifiquen, completen o modifiquen los mismos.

Principio de responsabilidad

14. El controlador de datos debería ser responsable del cumplimiento de las medidas que den efecto a los principios expuestos más arriba”.

En resumen, la OCDE con la emisión de estas Directrices intenta equilibrar dos valores básicos fundamentales, a saber: la protección de los datos personales y la libre circulación de estos mismos a nivel internacional.

Convenio Número 108 para la protección de las personas con respecto al tratamiento automatizado de los datos de carácter personal

El Convenio 108 es creado con el propósito de garantizar a los ciudadanos de los Estados contratantes, el respeto de sus derechos y libertades.²⁹ Entró en vigor el 1 de octubre de 1985, en particular para proteger el derecho a la vida privada frente a los tratamientos

LECTURAS

de datos personales, conciliando el respeto a ese derecho y la libre circulación de la información entre los Estados.

De esta forma el Convenio 108 constituye el primer instrumento de carácter vinculante para los Estados en el que se plasman los principios de la protección de los datos de carácter personal.

En términos del artículo 1, el objeto y fin del Convenio 108 es garantizar, en el territorio de cada Estado Parte, a cualquier persona física sean cuales fueren su nacionalidad o su residencia, el respeto de sus derechos y libertades fundamentales, concretamente su derecho a la vida privada, con respecto al tratamiento automatizado de los datos de carácter personal correspondientes a dicha persona.

En cuanto a su ámbito de aplicación, el Convenio 108 se aplica, en general a los tratamientos automatizados de datos de personas físicas, sin perjuicio de lo cual los Estados miembros podrán aplicar el Convenio a los datos de personas jurídicas y a los tratamientos manuales de datos, aunque tal circunstancia no se imponga obligatoriamente en el Convenio.

El artículo 5 establece los principios rectores que trazan el tratamiento automatizado de los datos de carácter personal:

Tratamiento leal y legítimo.

Principio de finalidad: los datos personales deben ser tratados únicamente para finalidades determinadas y legítimas y no utilizados de una forma incompatible con dichas finalidades.

Principio de proporcionalidad: los datos deben ser adecuados, pertinentes y no excesivos en relación con las finalidades para las cuales se hayan registrado.

Principio de calidad: los datos personales deben ser exactos (puestos al día).

Conservación de datos: la información de carácter personal debe ser conservada de tal forma que permita la identificación de los titulares durante un período de tiempo que no exceda del necesario para las finalidades para las cuales se hayan registrado.

Es importante mencionar que la firma del Convenio 108 no proporcionó la suficiente protección homogénea en materia de protección de datos que se había esperado. Esto se debió esencialmente a la naturaleza del Convenio, en virtud de que el mismo, a pesar de tener una naturaleza vinculante, establecía únicamente unos principios mínimos, permitiendo que, posteriormente, fueran los Estados firmantes los que los desarrollaran. Por este motivo se ha mantenido de forma unánime que el punto más débil del Convenio 108 fue, y sigue siendo, su aplicación. Es decir, se deja que sean los Estados miembros los que apliquen y desarrollen los principios contenidos en el Convenio y, de la misma forma, se les da libertad para aplicar las excepciones a los mismos.³⁰

Resolución 45/95 de la Asamblea General de la Organización de las Naciones Unidas

La Resolución 45/95 de la Asamblea General de la Organización de las Naciones Unidas del 14 de diciembre de 1990,³¹ contiene fundamentalmente una lista básica de principios en materia de protección de datos personales con un ámbito de aplicación mundial. Se mencionan, entre otros, los principios de licitud, exactitud, finalidad, acceso y no discriminación.

Los principios consignados en la Resolución 45/95 deben ser aplicables a todos los archivos informatizados públicos y privados, pudiendo extenderse dicha aplicación a los archivos manuales y a las personas jurídicas que contengan alguna información relativa a personas físicas, mediante la expedición de disposiciones especiales.³²

Ahora bien, la lista básica de principios reconocidos por esta Resolución son:

Principio de legalidad y lealtad: la información relativa a las personas no debe ser recogida o procesada por métodos desleales o ilegales.

Principio de exactitud: las personas responsables de la compilación de archivos o aquellas responsables de mantenerlos, tienen la obligación de llevar a cabo comprobaciones periódicas acerca de la exactitud y pertinencia de los datos registrados y garantizar que los mismos se mantengan de la forma más completa posible.

Principio de especificación de la finalidad: la finalidad a la que vaya a servir un archivo y su utilización en términos de dicha finalidad debe ser especificada, legítima y, una vez establecida, recibir una determinada cantidad de publicidad o ser puesta en conocimiento de la persona interesada.

Principio de acceso de la persona interesada: cualquiera que ofrezca prueba de su identidad tiene derecho a saber si está siendo procesada información que le concierne y a obtenerla de forma inteligible, sin costes o retrasos indebidos; y a conseguir que se realicen las rectificaciones o supresiones procedentes en caso de anotaciones ilegales, innecesarias o inexactas, y, cuando sea comunicada, a ser informado de sus destinatarios.

Principio de no discriminación: sin perjuicio de los casos susceptibles de excepción, no deben ser recogidos datos que puedan dar origen a una discriminación ilegal o arbitraria, incluida la información relativa a origen racial o étnico, color, vida sexual, opiniones políticas, religiosas, filosóficas y otras creencias, así como la circunstancia de ser miembro de una asociación o sindicato.

Principio de seguridad: deben adoptarse medidas adecuadas para proteger los archivos tanto contra peligros naturales, pérdida o destrucción accidental, como peligros humanos que se traducen en acceso no autorizado, uso fraudulento de los datos o la contaminación mediante virus informáticos.

Autoridad garante: el derecho de cada país debe designar a una autoridad que, de acuerdo con su sistema jurídico interno, vaya a ser responsable de supervisar la ob-

LECTURAS

servancia de los principios establecidos. Esta autoridad deber ser imparcial, independiente frente a las personas o agencias responsables de procesar y establecer los datos y con competencia técnica.

Transferencias internacionales: debe existir un flujo libre de datos personales entre los Estados en el cual se establezcan garantías suficientes de protección a la vida privada.

Directiva 95/46/CE sobre protección de personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de esos datos

La Directiva 95/46, fue aprobada con un doble objetivo: por un lado garantizar el derecho a la vida privada reconocido en el artículo 8 del Convenio Europeo de Derechos Humanos, en particular por lo que respecta al tratamiento de datos personales, ampliando los principios ya recogidos en otras normas internacionales y otorgando un mayor nivel de protección dentro de la Comunidad, sin disminuir el ya existente; y, por otro lado, impedir la restricción de la libre circulación de los datos personales en todos los Estados miembros de la Unión Europea.³³

El proyecto de Directiva 95/46, se inspira esencialmente en la doctrina constitucional alemana y en la ley francesa de 1978. Sin embargo, los trabajos se paralizaron, dado que diversos estados consideraron que no era posible la aprobación por parte de las instituciones comunitarias de una norma reguladora de un derecho fundamental de los ciudadanos, al no tener tal hecho cabida en las normas rectoras del Derecho Comunitario vigentes en ese momento.³⁴

A partir de ese momento, los trabajos se centraron en la necesidad de adoptar un texto de Directiva 95/46 referido a la adopción de un marco comunitario que garantice la libre circulación de los datos de carácter personal, no pudiendo los Estados miembros invocar el derecho a la protección de datos como justificación para impedir dicha libre circulación.³⁵ En ese sentido, la directiva resultaba indispensable para la consecución de mercado único.

Finalmente, la Directiva 95/46 fue aprobada el 24 de octubre de 1995. Con base en esta directiva, los Estados miembros de la Unión Europea han transpuesto en sus normas nacionales los principios que regulan un derecho fundamental sin entorpecer el flujo de información.

Citando a Puente Escobar,³⁶ las innovaciones introducidas por la Directiva 95/46/CE pueden esquematizarse de la siguiente manera:

La ampliación del ámbito de aplicación.

La regulación del encargado del tratamiento

El desarrollo de los principios de calidad.

DERECHO DE NIÑAS, NIÑOS Y ADOLESCENTES

El “interés legítimo” como legitimador del tratamiento.
La cláusula sobre la libertad de expresión.
El reconocimiento del derecho de oposición.
El reconocimiento de los derechos relacionados con las decisiones individuales automatizadas.
El desarrollo de sistemas de autorregulación sectorial.
El régimen sistemático de las transferencias internacionales de datos.
El reforzamiento de las funciones de las autoridades de protección de datos.
La creación del Grupo del Artículo 29.

En materia de principios, la Directiva 95/46/CE dispone en el artículo 6 lo que a continuación se indica:

“Artículo 6.-

1. Los Estados miembros dispondrán que los datos personales sean:

- a) tratados de manera leal y lícita;
- b) recogidos con fines determinados, explícitos y legítimos, y no sean tratados posteriormente de manera incompatible con dichos fines; no se considerará incompatible el tratamiento posterior de datos con fines históricos, estadísticos o científicos, siempre Y cuando los Estados miembros establezcan las garantías oportunas;
- c) adecuados, pertinentes y no excesivos con relación a los fines para los que se recaben y para los que se traten posteriormente;
- d) exactos y, cuando sea necesario, actualizados; deberán tomarse todas las medidas razonables para que los datos inexactos o incompletos, con respecto a los fines para los que fueron recogidos o para los que fueron tratados posteriormente, sean suprimidos o rectificados;
- e) conservados en una forma que permita la identificación de los interesados durante un período no superior al necesario para los fines para los que fueron recogidos o para los que se traten ulteriormente.

Los Estados miembros establecerán las garantías apropiadas para los datos personales archivados por un período más largo del mencionado, con fines históricos, estadísticos o científicos....

Carta de Derechos Fundamentales de la Unión Europea

La Carta de Derechos Fundamentales de la Unión Europea,³⁷ fue aprobada el 7 de diciembre de 2000 por la Cumbre de Jefes de Estado y de Gobierno celebrada en la ciudad de Niza, Francia. Reconoce entre otras cuestiones, el derecho a la protección de datos con el carácter de fundamental en su artículo 8 al establecer que toda persona tiene

LECTURAS

derecho a la protección de los datos de carácter personal que le conciernan, sin hacer mención a la intimidad o a la vida privada. También el artículo 8 señala que “el respeto de estas normas quedará sujeto al control de una autoridad independiente”.

De esta forma, a partir de la aprobación de la Carta de Derechos Fundamentales de la Unión Europea, la protección de los datos de carácter personal se configura como un derecho fundamental y autónomo del derecho a la intimidad y a la privacidad de las personas. Cabe precisar a este respecto, que en su artículo 7 aborda los derechos de manera separada, recoge el derecho a la vida privada y familiar.³⁸

Ahora bien, cabe mencionar que paralelamente ha habido un rico desarrollo jurisprudencial que por razones de espacio no se desarrollará exhaustivamente, sin embargo, es importante señalar en concreto el caso particular del Tribunal Constitucional Español, el cual arrojó luz sobre el contenido y alcances del derecho a la protección de datos personales en su sentencia 292 del 30 de noviembre de 2000,³⁹ por la cual definió los contornos de este nuevo derecho al establecer a la letra lo siguiente:

“7... [E]l contenido del Derecho fundamental a la protección de datos consiste en un poder de disposición y de control sobre los datos personales que faculta a la persona para decidir cuáles de esos datos proporcionar a un tercero, sea el Estado o un particular, o cuáles puede este tercero recabar, y que también permite al individuo saber quién posee esos datos personales y para qué, pudiendo oponerse a esa posesión o uso. Estos poderes de disposición y control sobre los datos personales, que constituyen parte del contenido del Derecho fundamental a la protección de datos se concretan jurídicamente en la facultad de consentir la recogida, la obtención y el acceso a los datos personales, su posterior almacenamiento y tratamiento, así como su uso o usos posibles, por un tercero, sea el Estado o un particular”.

Sin afán de exhaustividad, los instrumentos internacionales aquí referidos dan forma y contenido al derecho de la protección de datos, al tiempo de sentar las bases para su reconocimiento y difusión en otras regiones del mundo.

La Carta de Derechos Fundamentales de la Unión Europea fue aprobada el 7 de diciembre de 2000 por la cumbre de Jefes de Estado y de Gobierno celebrada en la ciudad de Niza, Francia. Reconoce entre otras cuestiones, el derecho a la protección de datos con el carácter de fundamental en su artículo 8 al establecer que toda persona tiene derecho a la protección de los datos de carácter personal que le conciernan, sin hacer mención a la intimidad o a la vida privada. También el artículo 8 señala que “el respeto de estas normas quedará sujeto al control de una autoridad independiente”.

De esta forma, a partir de la aprobación de la Carta de Derechos Fundamentales de la Unión Europea, la protección de los datos de carácter personal se configura como un derecho fundamental y autónomo del derecho a la intimidad y a la privacidad de las per-

DERECHO DE NIÑAS, NIÑOS Y ADOLESCENTES

sonas. Cabe precisar a este respecto, que en su artículo 7 aborda los derechos de manera separada, recoge el derecho a la vida privada y familiar.

La protección de datos personales de niñas, niños y adolescentes

Como se ha venido desarrollando, a nivel internacional se han realizado valiosos esfuerzos por establecer reglas para el tratamiento e intercambio de información de las personas al tiempo que se respeta su privacidad. Ese equilibrio se ha podido plasmar en leyes que prevén los principios y derechos de los titulares de los datos, así como el diseño de instituciones que podrían denominarse como “órganos garantes” de la adecuada protección de datos, con independencia y facultades de sanción.

Empero, no existe un modelo único de regulación a este respecto. Por un lado, contamos con el modelo europeo, que podría denominarse como universal al ser comprensivo para la protección de los datos personales (ya que prevé los principios, derechos, procedimientos y autoridad independiente) el cual ha sido adoptado con matices e innovaciones importantes por países como Canadá. Por otra parte, existen modelos sectoriales en los que conviven algunas regulaciones específicas y mecanismos de autorregulación. En este último grupo podríamos ubicar a los Estados Unidos de América y al propio México.⁴⁰

Es importante mencionar que en el ámbito europeo, así como en Canadá, las autoridades en materia de protección de datos han promovido intensamente el derecho a la protección de datos de menores a través de campañas de sensibilización dirigidas a padres y educadores, folletos informativos, creación de sitios en Internet de autoayuda, concursos, entre otros mecanismos para fomentar el conocimiento y alcances de este derecho fundamental.

Hay que recordar que la definición de dato personal adoptada de manera quasi generalizada en el ámbito internacional, señala que se trata de información relativa o concerniente a una persona física, identificada o identificable. En ese sentido, el ámbito de protección es hacia la persona en relación con el tratamiento que se dé a su información, la cual se puede encontrar en posesión de los gobiernos o de los particulares.

Por lo anterior, puede decirse válidamente que las niñas, niños y adolescentes gozan, en tanto que son personas, del derecho a la protección de sus datos personales, el cual se traduce en la debida observancia de una serie de principios y derechos, tutelados a través de un procedimiento, ante una autoridad independiente como se verá en el siguiente apartado.

La falta de dicha observancia ha traído consigo no solo la violación del derecho de protección de datos personales, sino implicaciones en el desarrollo social, psicológico y emocional de muchos de los menores. Existen innumerables casos ilustrativos de las consecuencias de dicha carencia, que por razones de espacio no podemos exponer, sin embargo, se describen cuatro casos ilustrativos y recientes al final del documento para

LECTURAS

mayor referencia.

La propuesta del Memorándum de Montevideo sobre la protección de datos personales y la vida privada en las redes sociales en Internet, en particular de niños, niñas y adolescentes

Ahora toca el turno de explicar las distintas propuestas del Memorándum sobre la protección de datos personales y la vida privada en las redes sociales en Internet, en particular de niños, niñas y adolescentes, mejor conocido como Memorándum de Montevideo –en adelante, el Memorándum –, para lograr la efectiva protección de los datos personales de las niñas, niños y adolescentes, en éste ámbito.

Hasta este punto, cabe destacar que el servicio de redes sociales ha sido definido por el Grupo de Trabajo de Protección de Datos (Artículo 29), como las “plataformas de comunicación en línea que facilitan a los individuos a crear o unirse a una red con usuarios de ideología afín. En el sentido legal, las redes sociales son servicios sociales de información, como se definen en el artículo 1, párrafo 2 de la Directiva 98/34/EC y reformada por la Directiva 98/48/EC”.⁴¹

Ahora bien, el objeto de la elaboración del Memorándum nace del reconocimiento de los riesgos a los que están sujetos los menores al momento de navegar en Internet. Los niños, niñas y adolescentes conciben el espacio virtual como un espacio privado, con la posibilidad de actuar y expresarse libremente sin estar plenamente conscientes sobre el control de su información y las implicaciones existentes. Esto genera “bienestar físico y psicológico, así como espiritual” como se ha demostrado desde la psicología”.⁴²

Más claro, el derecho a la protección de datos personales y la privacidad de los menores se traduce en la no injerencia, el respeto a su dignidad e identidad como personas. Si bien es cierto, el avance tecnológico y la vinculación de los menores con las nuevas tecnologías representa un elemento del proceso evolutivo de la sociedad, también es cierto que este nuevo espacio debe ser regulado para proteger los derechos de la niñez en todos sus ámbitos. Mismos, que al no ser garantizados tendrían implicaciones en su desarrollo y en la estigmatización social consiguiente.⁴³

Por lo que hace a las redes sociales, el uso que de ellas hacen los niños, niñas y adolescentes y los abusos a los que podrían ser sujetos, a continuación se abordan las secciones modulares en referencia a la protección de datos y la responsabilidad del Estado y de la Industria. Si bien, el Memorándum aborda diferentes aristas de la problemática, en las secciones sucesivas se analizan respecto de la aplicación al derecho fundamental de la protección de datos personales y las implicaciones en la vida presente y futuro de los menores.⁴⁴

Recomendaciones para los Estados sobre el marco legal

A este respecto, cabe destacar el numeral 6 denominado “Recomendaciones para los Estados sobre el marco legal” que a la letra establece lo siguiente:

DERECHO DE NIÑAS, NIÑOS Y ADOLESCENTES

“6. La protección de los datos personales requiere del desarrollo de una normativa nacional, aplicable al sector público y privado, que contenga los derechos y principios básicos, reconocidos internacionalmente, y los mecanismos para la aplicación efectiva de la misma. Los Estados deberán tomar en especial consideración, en la creación y en el desarrollo de dichas normativas, a las niñas, niños y adolescentes”.

La mención anterior tiene varias implicaciones relativas a la protección de los datos personales de los menores. La primera es que los Estados que utilicen como principios orientadores el Memorándum de Montevideo a la hora de legislar en materia de protección de datos personales deberán contemplar, entre otros los aspectos que se señalan a continuación.

En principio, el ámbito de aplicación de la norma debiera ser para entes públicos -el Estado en todos sus niveles de gobierno- así como para entes privados. La emisión de una ley de protección de datos brindaría la garantía a toda persona -incluidos los menores de edad- de que su información será manejada conforme a lo que establezca esta ley, por lo que si bien, el Memorándum se enfoca a la protección de menores de edad, se recomienda la expedición de una norma de aplicación general, dado que los principios y derechos que se desarrollan en los siguientes párrafos, también son transversalmente aplicables sin distinción de edad, aunque explicaremos las variaciones en su ejercicio al caso concreto.

Una novedad del Memorándum es la recomendación al legislador de tomar en cuenta en el proceso legislativo y de diseño de la norma, la opinión de las niñas, niños y adolescentes, sobre todo, en aquellas disposiciones particulares que se refieran a la forma en que debe llevarse a cabo el tratamiento de su información en Internet, de modo que ellos puedan aportar su opinión.

Los principios de protección de datos

En cuanto a los principios de protección de datos, existe un consenso más o menos generalizado a nivel internacional en reconocer los siguientes:

- Consentimiento;
- Información;
- Finalidad;
- Proporcionalidad;
- Calidad y
- Seguridad

Es importante mencionar que como premisa principal el proveedor de toda red social

LECTURAS

digital debiera comprometerse al tratamiento leal de los datos que no se traduce en otra cosa sino en el hecho de efectuarlo con estricto apego y respeto a los derechos del titular de la información.

Por ello, el consentimiento es el principio rector del derecho a la protección de datos personales dado que se trata del poder de disposición del titular de la información para decidir quién, cómo, cuándo y para qué utiliza sus datos, pudiendo oponerse a dicha utilización.

Aquí hay un punto importante a dilucidar y es el tema de la edad ya que no existe consenso acerca de a partir de qué edad se considera que un niño es maduro para poder ejercer su consentimiento y por tanto, manifestar su voluntad para otorgar su información personal. Dicha cuestión dependerá de la legislación que adopte cada país y de conformidad a ello, se establecerían las modalidades para expresar el consentimiento.

Ahora bien, otra complejidad se presenta a la hora de comprobar por parte de la industria, que realmente se obtuvo el consentimiento de un menor con la edad establecida por ley. Ello implica el desarrollo de mecanismos para conocer de manera fehaciente, la madurez del titular del dato.

En cuanto al principio de información, este se traduce en la obligación del proveedor de una red social digital de dar a conocer las reglas de privacidad con que cuentan, los propósitos y finalidades para los cuales serán utilizados los datos y/o transmitidos a terceros, así como el nombre del responsable de su tratamiento. También se conoce como el principio de la transparencia en el tratamiento de la información ya que se está utilizando información ajena y por tanto, debe ventilarse de qué manera se hará uso de la misma y bajo qué condiciones podrá el titular de los datos, ejercer los derechos a que se refiere el próximo apartado.

Veamos ahora el principio de finalidad que consiste en que los datos se recaban para cierto objeto concreto y conocido de antemano. Si la finalidad cambia, es necesario obtener el consentimiento del titular para poder utilizar los datos para nuevos objetivos.

Por su parte, el principio de proporcionalidad se traduce en que al tener el tratamiento una finalidad concreta, los datos que se recaban deberán ser directamente proporcionales a dicho fin, por lo que este principio indica que debe darse un tratamiento mínimo a la información, ya que en la medida que se obtenga más, podría rebasarse el fin primario. A este principio también se le conoce como principio de minimización del tratamiento de datos.

En lo que respecta al principio de calidad de los datos, éste consiste en mantenerlos actualizados y puestos al día de modo que reflejen verazmente la información acerca de una persona. Un dato inexacto es un dato falso y no rectificarlo podría acarrear consecuencias nefastas.

Finalmente, los datos deben estar seguros, es decir, íntegros y accesibles sólo para aquellos que estén autorizados para ello, como se verá más adelante.

DERECHO DE NIÑAS, NIÑOS Y ADOLESCENTES

Los derechos de las niñas, niños y adolescentes en materia de protección de datos
Por lo que ve a los derechos del titular de los datos, también hay coincidencia internacional en reconocer los siguientes:

- Acceso;
- Rectificación;
- Cancelación, y
- Oposición.

Para saber cómo se despliegan los derechos de las niñas, niños y adolescentes a la protección de sus datos personales, el Memorándum en el apartado denominado “Recomendaciones para los Estados sobre el marco legal” en su numeral 8 establece lo siguiente:

“8. Los Estados deben legislar el derecho que tienen las niñas, niños y adolescentes directamente o por medio de sus representantes legales, a solicitar el acceso a la información que sobre sí mismos se encuentra en bases de datos tanto públicas como privadas, a la rectificación o cancelación de dicha información cuando resulte procedente, así como a la oposición a su uso para cualquier fin”.

De acuerdo con dicho numeral, queda claro que los menores de edad podrían solicitar acceso a la información personal que de ellos se conserve, manipule y transmita en las redes sociales. Este derecho se relaciona directamente con el principio de información, ya que solo mediante un aviso de privacidad en el que se establezca la persona responsable del tratamiento de los datos, así como los derechos que tiene el titular de la información, los menores de edad podrán conocer qué información se detenta de ellos.

También deben poder solicitar la rectificación de datos erróneos o desactualizados para su puesta al día. Este derecho se relaciona directamente con el principio de calidad a que se hizo referencia en el apartado anterior. Finalmente, podría pedirse la cancelación del dato que trae como consecuencia la supresión o eliminación de dicha información. Cabe mencionar que en este punto es importante establecer mecanismos efectivos de supresión total de la información, porque en ocasiones se solicita eliminar una invitación a formar parte de una red social y esta sigue apareciendo ad infinitum, sin que sea respetada la voluntad del interesado o titular del dato.

El derecho de oposición también debe poder ejercitarse cuando los datos se hayan obtenido sin el consentimiento de los menores de edad (por encontrarse en fuentes de acceso público por ejemplo) y en este caso, la consecuencia sería la cancelación del dato.

LECTURAS

El procedimiento de tutela y autoridad independiente

Pasando a otro tema nodal del Memorándum, vale la pena resaltar la mención especial que hace a los “mecanismos para la aplicación efectiva de la norma”. Esta cuestión se refiere a la necesidad de que en los marcos normativos correspondientes se prevea un procedimiento de tutela de derechos de protección de datos; dicho procedimiento debería ser efectivo, expedito y gratuito, además de poder desahogarse ante una autoridad independiente.

La autoridad no necesariamente tendría que ser —aunque idealmente sí— una autoridad especializada en protección de datos personales. Dicha tarea bien podrían llevarse a cabo por las defensorías del pueblo o comisiones de derechos humanos, las procuradurías o los jueces. Por ello, resulta relevante que el procedimiento sea expedito y claro para no hacer nugatorio el derecho.

Recomendaciones para la Industria en materia de protección de datos

Las recomendaciones concretas del Memorándum a la industria establece que las empresas que proveen los servicios de acceso a Internet, aquellas que desarrollan las redes sociales digitales, o bien, las aplicaciones que éstas contienen, deben comprometerse de manera decidida en materia de protección de datos personales y la vida privada —en particular de niñas, niños y adolescentes—, a cooperar con los sistemas de justicia nacionales, desarrollar campañas de prevención y desarrollo de capacidades, entre otros instrumentos mediante compromisos o códigos de conducta, que deben incluir:

“ 19. No permitir la recopilación, tratamiento, difusión, publicación o transmisión a terceros de datos personales, sin el consentimiento explícito de la persona concernida. Se debe restringir el uso de la información recogida con cualquier otra finalidad diferente a la que motivó su tratamiento, y en especial a la creación de perfiles de comportamiento.

También se señala que en el caso de niñas y niños se deberá considerar la prohibición de tratamiento de datos personales. En el caso de adolescentes se deberá tener en cuenta los mecanismos de controles parentales de acuerdo a la legislación de cada país, de los que deben darse una información clara”.

Dado que en varios países ya existe la obligación para la industria de establecer controles para limitar la información que las niñas y niños proporcionan en Internet, de igual forma, el Memorándum señala de manera contundente que la industria deberá considerar la prohibición de llevar a cabo el tratamiento de datos de niñas y niños, con lo cual se busca limitar la recolección y almacenamiento de información solo al caso de los adolescentes.⁴⁵

Lo anterior tiene una lógica subyacente y es el hecho de que a partir de cierta edad, el ser humano comienza a ser consciente de su voluntad y de los efectos de sus actos u

DERECHO DE NIÑAS, NIÑOS Y ADOLESCENTES

omisiones. En la infancia, la inocencia e inmadurez de las niñas y niños los lleva a intercambiar toda la información que les sea solicitada acerca de sí mismos, así como de sus padres, hermanos y amigos, a cambio de conseguir puntos para ver a sus mascotas favoritas. Aquí tenemos una clara tensión entre el modelo de negocio de juegos para niños en redes sociales y los derechos de la niñez.

Conviene entonces recordar que el artículo 16 de la Convención sobre los derechos de los niños establece que no serán objeto de injerencias en su vida privada, por lo que la prohibición al tratamiento de sus datos no surge en el Memorándum, sino que más bien se retoma de los derechos del niño reconocidos en los instrumentos internacionales. En otras palabras, la actividad que actualmente lleva a cabo la industria al recabar información que los propios niños proporcionan en redes sociales, tiene claros vicios del consentimiento, por lo que podría ponerse en tela de juicio la licitud de dicha actividad.

Ahora bien, en el caso de los adolescentes, de acuerdo con las edades que cada país determine, éstos podrían proporcionar algunos de sus datos, siempre y cuando puedan conocer de manera clara las reglas del juego, el cual podría denominarse “intercambio de privacidad a cambio de diversión” como veremos más adelante.

Otras recomendaciones a la industria en materia de protección de datos, establecen lo siguiente:

20. Proteger la vida privada debería ser la característica general y por defecto en todas las redes sociales digitales, bases de datos y sistemas de comunicación, entre otros. Los cambios en el grado de privacidad de su perfil de usuario que se quieran realizar deben ser sencillos y sin costo alguno.

21. Las reglas sobre privacidad de las páginas web, servicios, aplicaciones, entre otros, deberían ser explícitas, sencillas y claras, explicadas en un lenguaje adecuado para niñas, niños y adolescentes.

Se deberá proveer información sobre los propósitos y finalidades para los cuales se utilizarán los datos personales, así como las transmisiones que se realicen a terceros. De igual modo se deberá indicar la persona o personas responsables del tratamiento de la información...

Esta mención es importante, ya que dicha recomendación se traduce en la obligación de la industria de proveer los llamados avisos de privacidad para dar cumplimiento al principio de información antes abordado. En ese sentido, el aviso deberá transmitir de forma clara y sencilla las reglas sobre privacidad, los propósitos y finalidades para los cuales serán utilizados los datos y/o transmitidos a terceros, así como el nombre del responsable de su tratamiento, dado que si no se le puede identificar claramente, tampoco podrían ejercitarse los derechos de acceso, rectificación, cancelación u oposición. A mayor abundamiento, el Memorándum establece lo siguiente:

LECTURAS

Se debe igualmente ofrecer un enlace hacia los “parámetros de privacidad” en el momento de la inscripción, conteniendo una explicación clara sobre el objeto de dichos parámetros.

Debe hacerse accesible igualmente un aviso sobre el hecho de que la red social ha preseleccionado los parámetros, si éste es el caso, y que pueden ser cambiados en todo momento, según las preferencias de las niñas, niños y adolescentes.

Sería deseable igualmente que se cambien los “parámetros por defecto” de los contenidos personales, para que puedan ser únicamente accesibles por los amigos y las redes que el usuario determine.

22. Toda red social digital debe indicar explícitamente en la parte relativa a la “publicidad” contenida en su política de privacidad, sobre los anuncios publicitarios e informar claramente, en especial a niñas, niños y adolescentes, sobre el hecho de que las informaciones personales de los perfiles de los usuarios se emplean para enviar publicidad según cada perfil. Se deberá evitar publicidad que no sea adecuada para las niñas, niños y adolescentes.

23. Toda red social digital debe indicar de manera clara la razón que motiva el exigir ciertos datos personales y en particular, la fecha de nacimiento en el momento de la inscripción y la creación de una cuenta. Se debe por tanto explicar que la fecha de nacimiento exigida tiene por objeto el poder verificar la edad mínima permitida para poder crearse una cuenta en la red social digital.

Se debe precisar igualmente cómo se van a utilizar estos datos de carácter personal que hay que facilitar de manera obligatoria.

La industria deberá implementar mecanismos para una verificación fehaciente de la edad de niñas, niños y adolescentes para la creación de una cuenta de usuario y/o acceder a determinado contenido.

24. Toda red social digital, sistema de comunicación o base de datos debería contar con formas de acceso a la información, rectificación y eliminación de datos personales, para usuarios o no usuarios, tomando en consideración las limitantes de la ley.

Toda red social digital debe elaborar una política accesible a los usuarios en materia de conservación de la información, en virtud de la cual los datos personales de los usuarios que han desactivado su cuenta sean suprimidos totalmente de los servidores del servicio, tras un periodo de tiempo razonable. Asimismo se deberá eliminar la información de no usuarios, considerando un límite razonable de conservación cuando han sido invitados a ser parte de las redes. Las redes sociales digitales no deben utilizar la información de no usuarios.

Las dos opciones que permitan desactivar y suprimir las cuentas deben ser totalmente visibles para los usuarios, que deben poder comprender qué supone cada opción en cuanto a la gestión por parte del servicio de los datos contenidos en dichas cuentas.

DERECHO DE NIÑAS, NIÑOS Y ADOLESCENTES

Se tiene que informar a los usuarios de las obligaciones de privacidad frente a terceros, dicha política debe ser explícita, clara y visible.

25. Debe impedirse la indexación de los usuarios de las redes sociales digitales por parte de los buscadores, salvo que el usuario haya optado por esta función. La indexación de información de niñas y niños debe estar prohibida en todas sus formas, en el caso de adolescentes éstos deben autorizar de forma expresa la indexación de sus datos mínimos”.

Uno de los aspectos que más han preocupado a las autoridades de protección de datos en el mundo, así como a otros actores importantes, es el hecho de que la información que se “sube” a las redes sociales se indexa a buscadores en Internet. Lo anterior significa que si la gente no está consciente de ello y no cuenta con la información necesaria ni los mecanismos para oponerse a esa acción, toda la información que considera que comparte únicamente con sus “amigos” en la red, también puede ser conocida y copiada por el resto de la gente que pueda tener acceso a buscadores comunes de información. Bastaría entonces con buscar el nombre de una niña, niño o adolescente, para que cualquier persona sin ser su “amigo” pueda saber todo lo que hace y quienes forman parte de su círculo social, además de otra información derivada.

Por ello, en el caso particular de las redes sociales digitales, se ha solicitado por autoridades como la Comisaria Europea para la Sociedad de la Información, que dichas redes garanticen que “al menos” las cuentas de los menores de edad sean “privadas por defecto e inaccesibles” a través de los buscadores de la red. Lo anterior busca la mayor protección de los menores al asegurar que no sean indexados sus datos en las herramientas para la búsqueda de información en Internet, impidiendo con ello seguir su rastro.⁴⁶

En lo que respecta al acceso por parte de terceros, el Memorándum en cuestión dispone lo siguiente:

“26. Toda red social digital debe establecer las medidas necesarias para limitar el acceso por parte de los terceros que desarrollan las diferentes aplicaciones que el servicio ofrece (juegos, cuestionarios, anuncios, entre otros), a los datos personales de los usuarios cuando éstos no sean necesarios ni pertinentes para el funcionamiento de dichas aplicaciones.

La red social tiene que asegurar que los terceros que desarrollan aplicaciones en sus plataformas únicamente podrán acceder a los datos personales de los usuarios con el consentimiento expreso de estos. La red social digital debe asegurarse que los terceros desarrolladores soliciten únicamente la información indispensable, pertinente y no excesiva para el uso de dicha aplicación.

Es igualmente importante que se tomen las medidas necesarias para evitar toda comunicación de datos personales de aquellos usuarios que no han decidido expresamente por ellos mismos el instalar alguna aplicación”.

LECTURAS

De nuevo, el hilo se rompe por lo más delgado. De entrada, hay que reconocer que existe un interés claro de la industria en identificar a las personas con sus gustos, necesidades y hábitos de consumo, para que a partir de ello, puedan ofrecerles bienes o servicios ad-hoc. A esta actividad se le denomina *behavioral targeting*.

Sabido lo anterior, es necesario que el proveedor de la red social digital establezca medidas para que terceros desarrolladores de las aplicaciones que se ofrecen (como los juegos), estén limitados en cuanto al acceso a los datos personales de los usuarios, de lo contrario se tiene entonces a un sinnúmero de polizontes que aprovechan estos esquemas abiertos.

Por ello, se recomienda la programación de filtros especiales para que dichos terceros sólo puedan obtener aquella información que el titular ha consentido expresamente “compartir” y no toda aquella que se encuentra en su cuenta.

Finalmente, el Memorándum hace una mención relevante a la seguridad de la información que se vierte en las redes sociales, al señalar lo siguiente:

29. La industria debe establecer medidas de índole técnica y operativa para garantizar la seguridad de la información, en particular la integridad, disponibilidad y confidencialidad.

Queda claro con lo anterior que la observancia de los principios y derechos en materia de protección de datos personales no serviría de mucho, si no se prevén las medidas necesarias para impedir la pérdida, destrucción o acceso no autorizado de la información contenida en redes sociales, las cuales pueden llegar a conformar archivos inmensos con datos de millones de personas, que permiten la creación de perfiles detallados y complejos que mal utilizados, pueden provocar violaciones a otros derechos y libertades como ya se ha dicho. 47

Conclusiones

Como se desprende de la larga marcha que han emprendido los derechos humanos, al tiempo que evolucionó la ciencia y la tecnología surgió un nuevo derecho fundamental a la protección de datos personales y la necesidad de desplegar sus mecanismos de tutela, para la efectiva protección de las niñas, niños y adolescentes.

Es claro que la protección de los datos personales como un derecho fundamental y autónomo, contempla en su amplio espectro la salvaguarda de los menores, por el simple hecho de ser. Sin embargo, la realidad nos demuestra la urgente necesidad de comprometernos en todos los niveles para que no se irrumpa en ese ámbito, por demás delicado. La afectación en la vida presente y adulta de los niños, niñas y adolescentes no

DERECHO DE NIÑAS, NIÑOS Y ADOLESCENTES

solo pone en riesgo su integridad personal sino además su desarrollo en todas las esferas de su crecimiento. De ahí, la urgente necesidad de regular las nuevas tecnologías, que si bien nos acercan cada día más, no vienen exentas de peligros.

Si bien los Estados no han adoptado un modelo único para la tutela del derecho a la protección de datos, cuando se trata de proteger a la infancia, las cosas cambian. El ejemplo quizá más palpable sea el hecho de que en los Estados Unidos de América existe una ley para proteger la privacidad de los niños cuando navegan en Internet, sin que exista una ley marco en materia de protección de los datos personales de otros sectores de la población.⁴⁸ Es por ello que dado que existe consenso en cuanto a la necesidad de proteger a los menores de edad en general en Internet y más recientemente en redes sociales, es necesario actuar para garantizar una tutela efectiva.

Existe la urgente necesidad de que los Estados comiencen a establecer mecanismos integrales de protección que arranquen con la expedición de normatividad en materia de protección de datos, pero que además de manera sistémica, se contemple la prevención a través del fomento educativo sobre los riesgos que enfrentan y las alternativas con que cuentan las niñas, niños y adolescentes al utilizar redes sociales digitales. Lo anterior también implicará necesariamente el involucramiento de los poderes judiciales, para que una vez que se han conculcado los derechos de los menores de edad, estos puedan ser resarcidos. Es un deber del Estado y una obligación democrática.

La confianza y la seguridad en la utilización del Internet y, en particular de las redes sociales, son aspectos fundamentales en la construcción de una sociedad mundial de información segura y abierta a todos. Ello urge la inmediata cooperación internacional y de abordar la ciber-seguridad de forma holística, resolviendo cuestiones jurídicas, técnicas, orgánicas y procedimentales.

De igual forma, la protección de la infancia en el ámbito tecnológico necesita de los padres. Las barreras tecnológicas instaladas en algunas páginas de Internet, como filtros o mecanismos de verificación de edad e identidad, no han sido suficientes para garantizar un uso seguro de la red a niños y adolescentes. Es necesaria la combinación de estas medidas técnicas con otros elementos, como la supervisión de los padres, la educación, el refuerzo de la ley y la puesta en marcha de políticas de seguridad entre los proveedores y las páginas que alojan redes sociales. La protección de los datos personales y de la integridad del niño demandan un esfuerzo conjunto.

Así como se establece en la Convención sobre los Derechos del Niño, los Estados deben tomar las medidas apropiadas para garantizar su protección y bienestar. La experiencia demuestra que el nivel de responsabilidad de un gobierno para implementar acciones concretas en este rubro, determina la importancia que se otorga a la conformación de sociedades futuras.

De ahí que la socialización del Memorándum de Montevideo, contribuye a los esfuerzos de la región encaminados a salvaguardar y proteger a las niñas, niños y adoles-

LECTURAS

centes ante los cambios tecnológicos y las nuevas formas de vida. Más aun, coadyuva a la transformación cultural que comprende la construcción de la ciudadanía desde el mismo momento en que empieza la vida, y en la fase más importante de formación del ser humano: la infancia.

La protección de sus datos y vida privada en las redes sociales digitales es un paso más a favor de su desarrollo integral, y una obligación de cada Estado miembro. Imprescindible, por tanto, incluir en la agenda nacional el desarrollo de las políticas públicas en esta materia.

Referencias bibliográficas

- Anaya Muñoz, Alejandro et.al. (2005) Glosario de términos básicos sobre derechos humanos, Comisión de Derechos Humanos del Distrito Federal, Universidad Iberoamericana Ciudad de México, México.
- Arenas Ramiro, Mónica (2006). El derecho fundamental a la protección de datos personales en Europa, Tirant lo Blanch, Valencia, España.
- Derecho Internacional de los Derechos Humanos: Normativa, jurisprudencia y doctrina de los sistemas universal e interamericano (2004). Oficina de Colombia del Alto Comisionado de las Naciones Unidas para los Derechos Humanos, Bogotá, Colombia.
- Caney, Simon y Peter Jones (eds.) (2001), Human Rights and Global Diversity, Frank Cass Publishers, London.
- Friedman, Milton (1990), The Republic of choice. Law, Authority and Culture, Harvard University Press, Cambridge.
- Jourard, S.M. (1966), "Some Psychological aspects of Privacy", Law and Contemporary Problems, Duke University School of Law, no. 31., Durham, NC.
- Murillo de la Cueva, Pablo y José Luis Piñar Mañas (2009). El derecho a la autodeterminación informativa, Fundación Coloquio Jurídico Europeo, Madrid.
- Newell, P.B. (1994), "A System of Model Privacy", Journal of environmental Psychology, Publisher Academic Press, no. 14., U.K.
- Piñar Mañas, José Luis (2005), "El derecho fundamental a la protección de datos personales", Protección de Datos de Carácter Personal en Iberoamérica: II Encuentro Iberoamericano de Protección de Datos, La Antigua-Guatemala, 2-6 de junio de 2003, Valencia, España.
- (2008), ¿Existe la Privacidad?, CEU Ediciones, Madrid.
- Oñate, Araceli e Iñaki Piñuel (2007), Mobbing Escolar, Ediciones CEAC, Madrid.
- Puente Escobar, Agustín (2005), "Breve descripción de la evolución histórica y del marco normativo internacional de la protección de datos de carácter personal", Protección de Datos de Carácter Personal en Iberoamérica: II Encuentro Iberoamericano de Protección de Datos, La Antigua-Guatemala, 2-6 de junio de 2003, Valencia, España.
- Pupavac, Vannesa (1998), "The Infantilization of the South and the UN Convention on the Rights of the

DERECHO DE NIÑAS, NIÑOS Y ADOLESCENTES

Child", Human Rights Law Review, University of Nottingham, Centre for Human Rights, March, U.K.

Rodríguez Palop, María Eugenia (2002), La nueva generación de derechos humanos. Origen y justificación, Dykinson-Universidad Carlos III de Madrid, Madrid, España.

Vasak, Karel (1982), International Human Rights Vol. 1., Greenwood Press, San Francisco, EUA.

Vincent, R.J. (1999), Human Rights and International Relations, Cambridge University Press, Cambridge.

Sitios consultados en Internet

Alto Comisionado de las Naciones Unidas para los Derechos Humanos. <http://www2.ohchr.org/spanish/law/crc.htm>

Carta de Derechos Fundamentales de la Unión Europea.

https://www.agpd.es/portalweb/canaldocumentacion/legislacion/union_europea/common/pdfs/B.1-cp--Carta-de-los-Derechos-Fundamentales.pdf

Convención Americana sobre Derechos Humanos.

<http://www.oas.org/Juridico/spanish/tratados/b-32.html>

Convenio para la Protección de los Derechos y las Libertades Fundamentales.

<http://www.acnur.org/biblioteca/pdf/1249.pdf>

Convenio 108 para la protección de las personas con respecto al tratamiento automatizado de los datos de carácter personal.

https://www.agpd.es/portalweb/canaldocumentacion/legislacion/consejo_europa/convenios/common/pdfs/B.28-cp--CONVENIO-N-1o--108-DEL-CONSEJO-DE-EUROPA.pdf

Children's Online Privacy Protection Act, 1998.

<http://www.ftc.gov/ogc/coppa1.htm>

Preámbulo de la Declaración de los Derechos del Niño de 1959. Documento de Naciones Unidas A.G.

res. 1386 (XIV), 14 U.N. GAOR Supp. (No. 16), p. 19, ONU Doc. A/4354 (1959). <http://www.iin.oea.org/BADAJ2/pdf/Normativa%20ONU/Declaraci%C3%B3n%20de%20los%20Derechos%20de%20Ni%C3%B1os%201959.pdf>

Declaración Universal de los Derechos del Hombre.

<http://www.un.org/es/documents/udhr/>

Directrices relativas a la protección de la intimidad y de la circulación transfronteriza de datos personales de la Organización para la Cooperación y Desarrollo Económicos.

https://www.agpd.es/portalweb/canaldocumentacion/legislacion/organismos_internacionales/ocde/common/pdfs/OCDE-Directrices-sobre-protecci-oo-n-de-privacidad-Trad.pdf

Documento de trabajo 1/08 sobre la protección de datos personales de los niños. Unión Europea.

https://212.170.242.196/portalweb/canaldocumentacion/docu_grupo_trabajo/wp29/2008/common/menores_es.pdf

El Universal. Lunes 28 de septiembre de 2009. "Reclutadores de empleo buscan información en redes sociales".

LECTURAS

- <http://www.eluniversal.com.mx/articulos/55885.html>
- Guidelines on Child Online Protection. Presentado en Unión Internacional de Telecomunicaciones el 5 de Octubre de 2009.
<http://www.itu.int/osg/csd/cybersecurity/gca/cop/guidelines/index.html>
- Ley Federal de Transparencia y Acceso a la Información Pública (México).
<http://www.ifai.org.mx/>
- Nota informativa publicada por la Agencia Española de Protección de Datos del 15 de octubre de 2009. Barómetro de septiembre de 2009 del CIS. “La AEPD destaca la alta desconfianza de los ciudadanos españoles en la seguridad de sus datos en Internet”.
<http://www.alfa-redi.org/noticias.shtml?x=11602>
- Opinión 5/2009 sobre redes sociales en línea del grupo de Trabajo de Protección de Datos de la Comisión Europea. http://ec.europa.eu/justice_home/fsj/privacy/index_en.htm
- Página oficial de Internet de la Organización de Estados Americanos. <http://www.oas.org/Juridico/spanish/tratados/b-32.html>
- Pacto Internacional de Derechos Civiles y Políticos.
<http://www.cinu.org.mx/onu/documentos/pidcp.htm>
- Recomendaciones Derechos de niños y niñas deberes de los padres y madres 2008. España.
<http://www.ftc.gov/ogc/coppa1.htm>
- Resolución 45/95 de la Asamblea General de la Organización de las Naciones Unidas.
https://www.agpd.es/porta/web/canal/documentacion/legislacion/organismos_internacionales/naciones_unidas/common/pdfs/D.3BIS-cp--Directrices-de-Proteccion-de-Datos-de-la-ONU.pdf
- Revista de derecho informático Alfa-Redi.
<http://www.alfa-redi.org/rdi.shtml>
<http://www.alfa-redi.org/noticias.shtml?x=11602>
- Revista Informador.
<http://www.informador.com.mx/tecnologia/2009/144861/6/filial-de-deutsche-telekom-pierde-datos-personales-de-clientes-estadounidenses.htm>
- Texto constitucional mexicano reformado en su artículo 16. <http://www.diputados.gob.mx/LeyesBiblio/>
- Tribunal Constitucional de España. Sentencia 292 del 30 de noviembre de 2000.
<http://www.tribunalconstitucional.es/es/jurisprudencia/Paginas/Sentencia.aspx?cod=7467>

Casos ilustrativos

Algunos casos prácticos sobre el uso y abuso de las redes sociales para el acoso y explotación de menores, se exponen a continuación:

Caso 1: Una adolescente británica a la cárcel por bullying⁴⁹ en Facebook.

País: Reino Unido de la Gran Bretaña (Worcester, Inglaterra).

Fecha: 24 de agosto de 2009.

Disponible en el vínculo: <http://www.direct.gov.uk/en/YoungPeople/HealthAndRelationships/Bullying/>

DERECHO DE NIÑAS, NIÑOS Y ADOLESCENTES

DG_070501

Exposición de caso.

Una adolescente de 18 años se ha convertido en la primera persona encarcelada en Gran Bretaña por hacer 'bullying' e intimidar a una compañera de instituto a través de una la red social.

Keeley Houghton había acosado a Emily Moore durante la etapa en la que acudieron juntas al colegio. Houghton se jactaba en su página de Facebook de que iba a matar a su compañera.

La joven inglesa fue condenada a tres meses de encierro en una institución para delincuentes juveniles, tras declararse culpable de acoso. Houghton también recibió una orden de restricción que impide acercarse a Emily Moore, ya sea por internet o por cualquier otro medio.

Observaciones

A este respecto, cabe destacar que el gobierno británico ha implementado la campaña "Laugh at it and you are part of it",⁵⁰ que pretende generar consciencia sobre el ciberbullying y sus consecuencias sociales.

Caso 2: Viví un infierno, todo por ser buen estudiante

País: Colombia.

Fecha: 6 de septiembre de 2009.

Disponible en: <http://www.eltiempo.com/archivo/documento/MAM-3606418>

Exposición de caso.

El adolescente, que hoy tiene 13 años, estudiaba en un prestigioso colegio de Bogotá. Ingresó en cuarto de primaria. Sus padres lo matricularon allí porque el plantel donde estudiaba no era bilingüe.

"Venía de un colegio muy estricto -cuenta él-. Estaba acostumbrado a la disciplina, y muchas cosas que enseñaban, ya las sabía. Me la empezaron a montar de nerdo".

Y por eso, por ser estudioso y respetuoso, un par de compañeros empezaron a hacerle la vida imposible. Además de golpearlo e insultarlo a diario, lo excluían todo el tiempo. Lo dejaban solo a la hora del descanso, no le permitían jugar con ellos.

Todo se complicó cuando las agresiones trascendieron al escenario virtual. En el Messenger era costumbre que cada uno de los compañeros de curso pusiera, en su estado, un mensaje insultante hacia él. Hacían concursos de la mejor frase, y él las veía cuando se conectaba.

Todo el tiempo recibía mensajes en su correo electrónico y en su celular. El adolescente, narró: "Empecé a tener pensamientos malos, a perder las ganas de vivir. Quise morirme, no quería ser el rechazado del curso".

Tal fue la presión que, según su médico de cabecera, sufrió un bloqueo de la hormona del crecimiento

Caso 3: Ciberbullying: Cuatro adolescentes demandados por crear un perfil falso en Facebook.

País: Estados Unidos de América

Fecha: 29 de septiembre de 2009.

Liga disponible: <http://cyberbullying.us/blog/lori-drew-officially-acquitted.html>

<http://arstechnica.com/tech-policy/news/2009/09/that-obscene-racist-may-be-fake-4-sued-for-profile-prank.ars>

Exposición de caso.

Cuatro adolescentes han sido acusados por crear un perfil falso de un compañero en Facebook, presentándolo como racista y sexualmente obsceno, y en continua búsqueda de nuevos amigos para expandir su red social. El perfil fue suficientemente creíble para hacerse de 580 amigos. Al respecto, la madre del adolescente

LECTURAS

ha puesto una demanda en contra de los cuatro adolescentes, acusándolos de difamación y por causar stress emocional severo a su hijo.

Aparentemente, los cuatro estudiantes difamaron el nombre de un compañero, usando fotografías y registrando información real en sus datos de contacto, como su número celular. Asimismo, el grupo también expuso numerosas frases obscenas, racistas y sexuales.

El grupo, en nombre del adolescente, efectuaba comentarios denigrantes en contra de los demás miembros asociados en su página. Lo que resultó en un severo desgaste emocional, implicaciones para sus familiares –al tener que cambiar de club social, transporte escolar, etc.–, gastos económicos, entre otros. La demanda fue hecha ante la Corte de Illinois y busca además del castigo, compensar los daños.

Caso 4.

País: España (Cádiz).

Fecha: 15 de junio de 2009.

Disponible en: http://www.elpais.com/articulo/sociedad/ciberamigo/chantajea/elpepisoc/20090615elpepisoc_5/Tes

Mi “ciberamigo” me chantajeaba. Ingresa en prisión un joven que acosó desde Cádiz a más de 250 mujeres, muchas de ellas menores, a través de la red.

Exposición de caso.

El detenido en Chipiona (Cádiz) era, en realidad, varón y tenía 24 años pero se había inventado hasta 12 personalidades distintas para ganarse la confianza de sus víctimas de diferentes maneras. Durante semanas habló con ellas a través de Internet. Se intercambiaron palabras en el chat, mensajes por correo y fotografías en algunas redes sociales como Facebook.

Cuando la amistad se consolidaba y reunía material suficiente, él desvelaba su verdadero rostro. El que amenazaba y chantajeaba a las que supuestamente eran sus amigas. Así engañó a 250 personas, la mayoría mujeres y menores. La Policía le detuvo una vez en octubre del año pasado. Pero siguió actuando. A la segunda le han llevado a prisión.

El método usado por este delincuente cibernético se conoce como grooming, nacido de la revolución que ha supuesto el auge de programas de mensajería instantánea, chats, redes sociales donde es fácil encontrar amigos pero no siempre con buenas intenciones. La operación policial que ha acabado con el arresto y encarcelamiento de este joven se ha hecho pública justo cuando el Ministerio del Interior ha emprendido una campaña para advertir de los riesgos de poner en Internet datos e imágenes privados, sobre todos, de menores. El detenido conocía estas facilidades y dominaba la técnica informática y las fórmulas para obtener de sus víctimas lo que buscaba.

La policía conoció los hechos a través de una denuncia registrada en Madrid. Una joven reveló que alguien al que había conocido en Internet la estaba chantajeando. Ella misma le había entregado, en virtud de la confianza ganada, una foto con una imagen suya desnuda. Ahora su supuesto amigo cibernético le amenazaba con difundirla y humillarla públicamente si no le entregaba semanalmente un vídeo de contenido sexual en el que ella apareciera. Esa denuncia permitió seguir la pista al acosador. La Brigada de Investigación Tecnológica del Cuerpo Nacional de Policía le localizó en octubre de 2008 en Chipiona y se le intervinieron dos ordenadores portátiles y dos discos duros. Fue detenido pero quedó en libertad.

El material intervenido fue analizado y se constató la existencia de más víctimas. Este descubrimiento abrió una nueva investigación que se ha prolongado todos estos meses y que ha permitido cifrar en 250 las víctimas, la mayoría de ellas mujeres y menores de todo el territorio español, aunque también había extranjeras. El acosador no se limitó a utilizar la información personal que sus víctimas le habían cedido voluntariamente, sino también usó programas de control remoto para acceder al contenido de cuentas de correo electrónico y los archivos personales de sus ordenadores.