FACULTAD DE DERECHO Y CIENCIAS SOCIALES

DERECHO A LA PROTECCIÓN DE DATOS PERSONALES DE NIÑOS, NIÑAS Y ADOLESCENTES EN REDES SOCIALES (FACEBOOK).

Trabajo de Titulación presentado en conformidad con los requisitos establecidos para optar por el título de Abogada de los Tribunales y Juzgados de la República.

Profesor Guía

Ms. Lorena Naranjo Godoy

Autor

Daniela Patricia Macías Villarreal.

Año

2017

DECLARACIÓN DEL PROFESOR GUÍA

“Declaro haber dirigido este trabajo a través de reuniones periódicas con el (los) estudiante(s), orientando sus conocimientos y competencias para un eficiente desarrollo del tema escogido y dando cumplimiento a todas las disposiciones vigentes que regulan los Trabajos de Titulación”.

_____

Lorena Naranjo Godoy
Master en Derecho de las Nuevas Tecnologías
C.C.: 170829378-0

DECLARACIÓN DEL PROFESOR CORRECTOR

“Declaro haber revisado este trabajo, dando cumplimiento a todas las disposiciones vigentes que regulan los Trabajos de Titulación”.

_____

Elsa Jacqueline Guerrero Carrera
Master en Derecho mención Derecho Económico
C.C.: 200002747-0

DECLARACIÓN DE AUTORÍA DEL ESTUDIANTE

“Declaro que este trabajo es original, de mi autoría, que se han citado las fuentes correspondientes y que en su ejecución se respetaron las disposiciones legales que protegen los derechos de autor vigentes.”

_____

Daniela Patricia Macías Villarreal

C.C.: 172703733-3

AGRADECIMIENTO

A mis padres por su apoyo incondicional, a mi hermano Sebastián por ser mi fuerza, a mi tío Rodrigo por todo su cariño y aliento, a mi mejor amiga Mercedes por sus palabras, silencios oportunos. En especial a la Doctora Lorena Naranjo, por llegar a mi vida en un momento en que necesitaba de mucha iluminación, por sus consejos y por transmitir sin egoísmo su sabiduría.

Daniela

DEDICATORIA

Con mucho amor se lo dedico a mi madre y padre, dos seres maravillosos que han hecho de mi mundo un lugar feliz, me han tratado como una reina y me han enseñado a actuar con ética, solidaridad y bondad siempre. A la Doctora Lorena Naranjo que ha sido una docente excepcional, cariñosa y preocupada, pero sobre todo por ser un ser humano como muy pocos, apasionada, llena de valores y excepcional en todos los sentidos.

Daniela

RESUMEN.

El presente ensayo académico aborda el derecho a la protección de datos personales de niños, niñas y adolescentes en redes sociales (Facebook). En la actualidad, la web es interactiva, facilita el acceso a la información y permite la constante comunicación entre los sujetos que en ella intervienen. Un ejemplo de su funcionamiento son las redes sociales, entre las más destacadas Facebook.

Está red social es responsable del tratamiento de información personal de los usuarios que en ella participan. En consecuencia, la protección de los titulares de aquellos datos es fundamental, sobre todo de quienes requieren un especial cuidado al ser considerados un grupo de atención prioritaria. Los niños y adolescentes encuentran cautivador el uso de redes sociales, ya que constituyen una herramienta para ganar popularidad, mayor número de amigos y seguidores, por lo que en la mayoría de casos los niños y jóvenes no se detienen a analizar el tipo de información que comparten, lo que los expone a constantes amenazas.

A nivel mundial se han implementado iniciativas que buscan concientizar sobre la corresponsabilidad que existe entre el Estado, las redes sociales, los usuarios y en caso de menores de edad, padres y tutores, con la finalidad de evitar que se vulneren derechos mediante el tratamiento abusivo de la información personal.

Para que las redes sociales, como Facebook, sean garantes del derecho a la protección de datos personales de niños, niñas y adolescentes, es necesario que implemente medidas como la privacidad por diseño, en donde se evidencia la aplicación efectiva de los principios de calidad, seguridad y consentimiento informado; pero obligar a empresas económicamente poderosas a elevar sus estándares de protección resulta muy difícil, por lo que una solución real en el caso de niños y jóvenes, es implementar dentro de las legislaciones sanciones a padres y tutores, ya que son corresponsables del cuidado de este grupo.

ABSTRACT.

This academic essay is about the right of personal data protection of boys, girls and teenagers in social networks (Facebook). Nowadays, web is interactive, facilitate the access to the information and allow the constant communication between members that participate in it. An example of their functionality are the social networks, among the most outstanding Facebook.

This social network is responsible for the treatment of personal information of users who participate in it. Consequently, the protection of data owners is fundamental, especially those who require special care when they are considered a priority attention group. Children and adolescents find the use of social networks captivating, since they are a tool to gain popularity, more friends and followers, so in most cases children and young people do not stop to analyze the type of information that they share, which exposes them to constant threats.

At the global level, initiatives have been implemented to raise awareness of the co-responsibility that exists between the state, social networks, users and in the case of minors, parents and guardians, to avoid violating rights through abusive treatment of personal information.

In order for social networks, such as Facebook, to guarantee the right to the protection of the personal data of children and adolescents, it is necessary to implement measures such as privacy by design, which shows the effective application of the principles of quality, Security and informed consent; But forcing economically powerful companies to raise their standards of protection is very difficult, so a real solution in the case of children and young people is to implement sanctions within parents and guardians, as they are responsible for the care of this group.

ÍNDICE

INTRODUCCIÓN

Las red informática permite el desenvolvimiento de la sociedad de la información y conocimiento (Cebrián, 2008, p. 345) (Trejo, s.f., p. 11). Originalmente, la *web* clásica se caracterizaba por un diseño basado en la unidireccionalidad, es decir solo una parte generaba el contenido. Ahora, nos encontramos frente a la *web* 2.0 una realidad social dinámica (Dreyzin, Fernández, Pimentel, 2006, p.89), en donde todos los participantes se encuentran relacionados estrechamente.

Hasta finales del año 2015, internet contaba con tres punto dos billones, de usuarios activos, de este número dos billones provienen de países en vías de desarrollo (Sanou, 2015), de los cuales doce millones son ecuatorianos (INEC, 2014), siendo niños, niñas y adolescentes considerados “los mayores usuarios de Internet” (Orduz, 2012).

Barzallo define a las redes sociales como “una plataforma de comunicación en Internet que permite a los usuarios interactuar a través del intercambio de datos personales comunes que facilitan la creación de redes” (2012, p. 12), por lo tanto las redes sociales *online* son estructuras de individuos vinculados por afinidad de patrones que posibilitan la conectividad, interacción y comunicación, siendo los datos personales el eje fundamental que permite el correcto funcionamiento del sistema.

Son de distintas clases (Lara, 2008, p. 21) (Area, 2016,p. 19), pero en general se pueden distinguir tres grandes grupos (Baggiolini, 2013, p. 954) (Caldevilla, 2010, p. 12): profesionales, que permiten el desarrollo de una red de colegas; especializadas, que reúnen a los usuarios de acuerdo a ejes temáticos comunes; y generalistas o de comunicación, que permiten la interacción de individuos, facilitando que se comparta contenido multimedia (fotos, videos, música, gifts, etc.), ideas, reflexiones, preferencias, entre otros.

El uso de redes sociales es muy atractivo para niños, niñas y adolescentes, es por eso que el ochenta y tres por ciento de niños y jóvenes hace uso de las

mismas (20 Minutos Editora, 2014). Facebook, es la red social de comunicación más popular en el mundo virtual, hasta finales del segundo semestre del año 2015, tenía registrados mil quinientos cincuenta millones de perfiles, de los cuales el setenta y ocho por ciento le pertenecen a niños y adolescentes (Sanou, 2015). En Ecuador dos millones de niños, niñas y adolescentes tiene una cuenta activa en la mencionada red social (INEC, 2014).

A pesar de que la edad mínima para acceder a Facebook es de catorce años, en México, Brasil y Argentina siete millones y medio de infantes entre siete y doce años se dan de alta mintiendo acerca de su edad (Expansión, 2013). En Ecuador no existen estadísticas que muestren el número de usuarios menores a trece años que usen la red social. Facebook elimina a diario veinte mil perfiles diarios de niños menores a trece años. (El Universo, 2011).

Los principales responsables de brindar protección a niños y jóvenes son los padres o tutores, pues son los primeros llamados a cuidar de la dignidad e integridad de las niñas, niños y adolescentes a su cargo. Los proveedores de servicio, al ser quienes crean, manejan y tratan ficheros de datos automatizados, tiene un deber de cuidado, por lo que el diseño de la plataforma, debería permitir que está no sea usada como una herramienta para vulnerar los derechos del titular de la información personal. Finalmente, el Estado juega un papel de garante brindando mecanismos de efectivización de derechos.

Facebook, en su diseño, prevé la publicidad por defecto de la información, por lo que, toda aquella actividad que realizan las personas dentro de la red social, puede ser visualizada por cualquier usuario; debido a esto, niños, niñas y adolescentes se encuentran en riesgo, pues la información que comparte este grupo de la población, puede servir como una herramienta idónea, para que otras personas puedan transgredir su integridad, dignidad y derechos.

Facebook para poder funcionar correctamente requiere tratar los datos personales de los usuarios que se dan de alta y usan dicha red social. Por lo que, el objetivo principal de éste ensayo académico será el de analizar de qué

forma Facebook puede afectar el derecho a la protección de datos personales de niños, niñas y adolescentes. Para lo cual, se deberá hacer un estudio de los elementos generales del derecho a la protección de datos personales y del tratamiento que dicha red social le da a la información; además, se debe determinar la relevancia jurídica del derecho a la protección de datos personales en redes sociales de niñas, niños y adolescentes; para finalmente, establecer qué medidas efectivas se deberían aplicar para garantizar el pleno goce del derecho a la protección de datos personales en redes sociales (Facebook) en el caso de este grupo de atención prioritaria.

El presente ensayo académico se estructura de la siguiente manera:

En el primer capítulo se va a analizar al derecho de protección de datos personales y las diferentes corrientes sobre el régimen que se aplica al mismo. El segundo capítulo va a desarrollar el estudio de la relevancia del derecho a la protección de datos personales en redes sociales, en relación a niños, niñas y adolescentes. Finalmente, el tercer capítulo va a detallar qué medidas se deben implementar para garantizar efectivamente el derecho respecto de niños y jóvenes.

Para la presente investigación se realizará un análisis exegético y dogmático sobre el régimen de aplicación del derecho a la protección de datos personales a nivel mundial, con el fin de identificar la responsabilidad del proveedor de servicios de la red social Facebook como tratante de bases de datos, para la implementación de medidas que le permitan ser un garante de este derecho. Para el tratamiento del material de la investigación se empleará el ya que las fuentes principales serán libros especializados en el tema, artículos e instrumentos y normativa pertinente.

1. Derecho a la protección de datos personales y redes sociales (Facebook).

1.1. Generalidades del derecho a la protección de datos personales.

Los datos personales en la actualidad tienen un valor equiparable al del dinero, por lo que su tratamiento muchas veces vulnera los derechos de su titular, haciendo necesario que exista un régimen de protección.

El antecedente de la protección de datos, es la intimidad (Murillo, 1990, p. 78) (Guerrero, 2006, p. 22-24) (Almuzara, 2005, p. 33), que es el derecho a proteger a los seres humanos de la intromisión de terceros en los asuntos de la persona que pudiera afectar su integridad y reputación (Murillo, 1990, p. 16) (Altmark, Molina, 2012, p. 27) (Gil, Quintanilla, 2016, p. 89). Ha sufrido una gran evolución a lo largo de la historia; inicialmente se concebía solamente la protección de la esfera personal de los individuos. En la actualidad, la teoría de las esferas está superada (Aparicio, Batuecas, 2015, p. 78). El derecho a la intimidad se manifiesta en la honra, la reputación, la familia, el lugar donde una persona reside, la correspondencia, la dignidad, además de la vida privada personal.

Originalmente, se sancionaba a los medios de difusión de información tradicionales cuando se divulgaba información errónea, parcial, negativa o perjudicial (Benítez, 1997, p. 123), no se contemplaba el uso de TIC y su alta capacidad de tratar elevados volúmenes de datos, además de su incapacidad de olvidar dicha información.

Ante el rápido desarrollo de las tecnologías de la información y comunicación, aparece el derecho a la autodeterminación informativa (Davara, 2008, p. 72), en el año 1983 con “la sentencia del censo”, con el que se protege a las personas frente al tratamiento automatizado de sus datos personales (Bueno, 2014, p. 132). Es decir, los individuos son conscientes del aporte de sus datos en la red informática, por lo que mediante esté derecho surge un equilibro, en donde el

Estado cumple un papel garantista, pues brinda seguridad en el procesamiento de dicha información.

Finalmente, con la evolución de las tecnologías de la información y comunicación aparece el derecho a la protección de datos personales (Pérez, 2016, p. 14), que hace referencia a la atención y cuidado que jurídicamente se les da a las personas en relación al tratamiento por terceros de su información personal (Conde, 2005, p. 79), con el objetivo de evitar una afectación en las distintas áreas en las que pueda desenvolverse.

El derecho a la protección de datos personales, es más extenso que la autodeterminación informativa (Freixas, 2001, p. 53), ya que no solo permite la disponibilidad de los datos personales, sino que incluye principios a aplicarse durante el tratamiento de los datos y una serie de obligaciones para quien maneja la información personal.

La realidad actual implica la posibilidad de identificar a las personas desde cualquier aspecto de su vida (García, 2010, p. 64), por lo que, cualquier información, por más irrelevante que pueda parecer permite reconstruir a los usuarios, haciéndolos vulnerables a cualquier transgresión de sus derechos.

Mediante la aplicación de este derecho se pretende que los usuarios tengan control sobre los datos personales que otros tratan, evitando que su mal uso pueda vulnerar los derechos de los sujetos. En otras palabras, busca proteger a las personas titulares de datos que han sido recopilados y tratados por terceros (Davara, 2008, p. 53).

La protección de datos personales garantiza la libertad informática, pues les da a los individuos “la facultad de controlar sus datos personales y la capacidad de disponer y decidir sobre ellos” (Agencia española de protección de datos, 2009).

En otras palabras, prevé la existencia del consentimiento de toda actuación que vayan a realizar terceros sobre datos del titular y además permite que las

personas conozcan y controlaren el uso y destino de datos contenidos en ficheros. Es un derecho preventivo, que protege a las personas en relación a la información que otros tratan sobre ellas. Además, es instrumental pues su efectivización garantiza otros derechos como el honor, la intimidad, el buen nombre, la honra, la propia imagen, entre otros (Escribano, 2014, p. 79).

La protección de datos personales es fundamental, pues preserva la dignidad de los individuos y fomenta el libre desarrollo de las personas. Este derecho está reconocido por diversos instrumentos internacionales entre los más importantes encontramos al Convenio 108 del Consejo de Europa sobre protección, de datos personales (1985); la 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; en la Carta de los Derechos Humanos de la Unión Europea (2000), está última reconoce este derecho como distinto del derecho a la intimidad y privacidad, dotándolo de autonomía; OCDE “Directrices relativas a la protección de la privacidad y flujos transfronterizos de datos personales” (1980), en donde se establecen principios aplicables a la protección de datos y se manifiesta su operatividad tanto en el sector público como privado. Resolución 45/95 de la Asamblea de la ONU y las Directrices para la armonización de la protección de datos personales de Iberoamérica (2007), que establecen modelos para la aplicación del derecho.

En el Ecuador, la Constitución en el artículo 66 numeral 19 manifiesta que las personas tienen derecho a la protección de sus datos personales, en donde se establece que los individuos tienen el derecho a acceder, conocer y decidir sobre sus datos personales, es decir, tienen el derecho de autorizar la difusión, recolección, archivo, procesamiento y distribución de su información personal.

Se efectiviza mediante la acción prevista en el artículo 92, *habeas data,* que tiene como objetivo garantizar el respeto y correcta aplicación de varios derechos constitucionales como la honra, buen nombre, propia imagen, olvido, acceso a la información, intimidad, la protección de datos personales, etc.

Actualmente, los seres humanos están profundamente relacionados con las TIC. Su actividad diaria en la red deja un rastro de datos que lo identifican y los hacen identificable ante terceros. Está información está sujeta a tratamiento, haciendo que su protección sea primordial.

La protección de datos personales, es un derecho que no solo brinda garantías, sino que establece principios para el manejo de información personal, además implica una serie de obligaciones para quien trata los datos personales. Permite que los individuos autoricen la recopilación y controlen el uso y destino de la información.

1.1.1. Concepto de dato personal.

El derecho a la protección de datos personales tiene como objeto proteger a las personas en relación a su información, siendo necesario el análisis de lo que son los datos personales.

Dentro del presente ensayo académico se le dará el mismo significado a información y dato, para evitar el uso repetitivo de la palabra dato; aclarando que existe una sustancial diferencia; pues, la información es un conjunto de datos estructurados en función de determinados fines, mientras que, el dato por sí solo no resuelve una consulta determinada (Aparicio, Batuecas, 2015, p. 36).

Los datos son aquella información extraída y materializada de la realidad apoyada en un soporte físico o virtual. En general, existen dos tipos de datos (Gil, Quintanilla, 2016, p. 12), los cuantitativos que son aquellos que se pueden contar o medir y los cualitativos que son los que se describen únicamente, estos a su vez, pueden ser numéricos, alfabéticos, y alfanuméricos; y pueden capturarse, verificarse, almacenarse, recuperarse y reproducirse, así como eliminarse (Bueno, 2014, p. 57), debido a que, poseen un soporte.
Los datos personales son información de personas identificadas o identificables (Gil, 2015, p. 45) (Altmark, Molina, 2012, p. 12) (Aguilar, Said, 2010, p. 109). No se restringen al nombre o apellido, sino a todo aquello que permita determinar

de forma directa o indirecta la identidad de un individuo, permiten que los flujos de información incrementen.

La Agencia Española de Protección de Datos Personales, los define como “cualquier información numérica, alfabética, gráfica, fotográfica, acústica o de cualquier otro tipo concerniente a personas físicas identificadas o identificables”. (2009).

Existen también datos personales que son de carácter sensible (Garriga, 2015, p. 156), estos hacen referencia a la salud, a la orientación sexual, ideologías y creencias, es aquella información que de ser divulgada irresponsablemente afecta a la persona gravemente (Pfeiffer, 2008, p. 13) (Joyanes, 2016, p. 12).

Actualmente, con la intervención de las TIC, sobre todo con la alta participación de personas en redes sociales se evidencia que la actividad que se realiza, como dar *like* o la dirección IP, de donde el usuario accede a su cuenta, permiten crear un perfil de las personas, permitiendo que sean identificadas e identificables (INTENCO, 2012). Haciendo evidente que el concepto de dato personal ha evolucionado, pues inicialmente, se consideraba solamente que la información como nombre, edad, número de identificación, estatura, creencias, afinidad política entre otros, eran de carácter personal.

Los datos personales han ganado un valor económico, equiparable al del dinero; en la actualidad representan el “activo intangible más importante” (Ramos, 2016), pues constituyen una fuente primordial para realizar marketing.

En consecuencia, el concepto de dato personal ha evolucionado con la participación activa de las personas en la red informática, haciendo que cualquier información, por más insignificante que pueda parecer, que permita la identificación de una persona, sea considerada de ésta categoría. A su vez, los datos personales permiten generar utilidades mediante su tratamiento y negociación, dándoles un importante valor económico.

1.1.2. Principales corrientes sobre el régimen de protección de datos personales.

Alrededor del mundo, se tienen diferentes percepciones sobre la protección de datos, entre las más importantes encontramos a:

1.1.2.1. Estados Unidos.

Para la visión estadounidense la información personal es considerada un bien con el que se puede comerciar, por lo que son los individuos los responsables de ejecutar la normativa vinculada a los datos personales.

Para la corriente estadounidense rige el autocontrol y la autoregulación, es por eso que son los individuos los encargados de activar la normativa que los ampara. Esta legislación tiene marcos de protección mínimos en materia de protección de datos, se regula desde el concepto de *privacy.* La autoregulación implica una mínima intervención de las entidades públicas y el autocontrol se ve plasmado en incluir dentro de los contratos, políticas de uso de datos y privacidad, siendo el responsable del fichero de datos el encargado de gestionar medidas de control para sí mismo.

1.1.2.2. Europa.

Bajo la visión europea, los datos personales se consideran un elemento esencial de la personalidad de los seres humanos, debido a que le dan a los individuos singularidad, en consecuencia, son intransferibles, pero su titular puede facultar a otros su recopilación, tratamiento y cesión (Davara, 2008, p. 50) (Conde, 2005, p. 29). Este derecho no protege a los datos, sino a los titulares de dicha información (Guerrero, 2006, p. 206).

Este modelo contempla la participación activa del Estado para garantizar y efectivizar el derecho, mediante la creación de instituciones especializadas (Gil,

2016, p. 112). Se le da un enfoque preventivo, en donde se les obliga a los tratantes de datos a mantener un debido cuidado y se establecen principios.

1.1.2.3. América Latina.

Países como Ecuador, Colombia, Argentina, Uruguay y México han incorporado esté derecho en sus constituciones y legislaciones especiales (Domínguez, 2016, p. 37). En Latinoamérica, si bien es cierto, se incorpora a la protección de datos como un derecho, también se integran criterios de la visión estadounidense. Se añade además a la acción de *habeas data,* como mecanismo de efectivización (Reascos, 2016, p. 46) (Pérez, 1996, p. 44-45).

Al ser un hibrido entre la perspectiva europea y estadounidense (Téllez, 2013, p. 117), para la doctrina ha sido complicado definir concretamente al modelo, pues cada país dentro de sus leyes fija conceptos distintos, sin embargo, la acción de *habeas data* ha sido una pauta que relaciona a toda la región.

La visión europea y estadounidense no son compatibles, pues la primera tiene un carácter proteccionista, en donde se promueve la garantía y protección del derecho, mientras que la segunda guarda un enfoque relacionado con la necesidad de que el individuo sea quien active los sistemas de protección, con un mínimo de intervencionismo del Estado. La concepción latinoamericana es un hibrido entre las dos corrientes previamente mencionadas, y además cada país le complementa características propias, su elemento común es la acción de habeas data.

1.1.3. Principios del derecho de protección de datos personales.

Como se mencionó en líneas anteriores, el derecho a la protección de datos personales está compuesto por una serie de principios que deben aplicarse al momento por el responsable del fichero a la hora de tratar dicha información, los cuales son:

1.1.3.1. Principio de calidad.

El principio de calidad de los datos personales abarca varias reglas, primero la existencia de racionalidad y proporcionalidad en el tratamiento de datos, esto quiere decir que la información que se recoge debe perseguir un fin específico, por otro lado, no debe manejarse de manera excesiva y debe ser pertinente (Reascos, 2016, p. 56) (Aparicio, Batuecas, 2015, p. 123). En otras palabras, solo se pueden recabar los datos necesarios para el objetivo que el tratante específicamente tenga, y para esto será imperativa la autorización del titular.

> "El principio de calidad es uno de los ejes fundamentales de la regulación del tratamiento automatizado de datos personales y exige que los datos deben ser exactos, adecuados pertinentes y proporcionados a los fines para los que han sido recogidos y tratados" (Garriga, 2010, p. 170).

Este principio implica la necesidad de explicación del propósito por el cual se recogen los datos a la persona dueña de la información, así como asegurarse de que esta finalidad sea legal y legítima (Trejo, s.f., p. 67). También, existe la obligación de que, durante el manejo de la información personal, los datos gocen de veracidad y actualización. Además, se debe garantizar el efectivo ejercicio de los derechos de acceso, rectificación, cancelación y oposición. Esto quiere decir que se requiere que los datos personales que se tratan estén relacionados con la finalidad por la cual se han obtenido, es decir que exista "clara conexión entre la información que se recaba (…) y el objetivo para el que se solicitó" (Murillo, 1993, p. 65)

Este principio tiene como prerrogativa evitar el abuso de la información personal por parte de quien la maneja, además de prevenir que terceros no autorizados o de mala fe, accedan a los mismos y puedan transgredir la integridad del titular.

1.1.3.2. Principio de consentimiento informado.

El consentimiento informado es un principio esencial para garantizar el derecho a la protección de datos personales, este debe ser libre, inequívoco, informado, específico y en algunos casos expreso (Gil, 2015, p. 64), este principio es uno de los más importantes en relación a la protección de datos personales, pues garantiza que los titulares tengan control y dominio sobre sus datos manejados por terceros.

> Las manifestaciones de los requisitos legalmente exigidos al consentimiento del afectado se realizan en la práctica a través de la información al afectado, en el momento de la recogida de sus datos de carácter personal de los extremos esenciales relacionados con el tratamiento, recabando a tal efecto su consentimiento en relación con los aspectos especifica e inequívocamente hechos constar en la mencionada información (Agencia Española de Protección de Datos, 2009).

El consentimiento informado tiene implícita una obligación para el proveedor de servicios de redes sociales, pues este debe comunicar al titular sobre el uso y destino de la información que les pertenece (García, 2010, p. 78). El consentimiento debe ser: previo, libre y revocable. En otras palabras, se debe notificar al titular con anterioridad a la solicitud de la autorización de tratar sus datos, sobre el uso, la pertinencia, la finalidad y el destino de sus datos y se debe ofrecer la opción de anular o cancelar su consentimiento.

Para el perfeccionamiento del consentimiento se requiere que sea libre y no debe estar viciado, es decir no debe obtenerse con error, fuerza o dolo (Código Civil, 2005). Lo que significa, que no debe inducirse a una confusión al titular o a algún tipo de coacción con una mala intención para obtener la autorización del titular de tratar sus datos, por lo que el objetivo del tratante debe ser claro y preciso.

1.1.3.3. Principio de seguridad.

El principio de seguridad hace referencia a las medidas que el proveedor de servicios está obligado a adoptar para el tratamiento de datos personales (Aparicio, Batuecas, 2015, p. 127), sobre todo cuando dicha información les pertenezca a menores de edad. Este principio busca que se garantice la reserva de los datos, la integridad y disponibilidad de los mismos.

Se debe aplicar durante todo el tiempo que el tratante maneja los datos personales (Campuzano, 2000, p. 192) (Serrano, 2002, p. 18), es decir desde que se recaba el dato hasta que se elimina o cancela, por lo que es importante durante el procesamiento, en el almacenamiento y el olvido.

El artículo 9 de la Ley Orgánica de Protección de Datos de Carácter Personal de España, manifiesta que: “no se registrarán datos de carácter personal en ficheros automatizados que no reúnan las condiciones que se determinan por vía reglamentaria con respecto a su integridad y seguridad y las de los centros de tratamiento, locales, equipos, sistemas y programas” (1999).

“El concepto de seguridad debe abarcar tanto la confidencialidad de la información como la disponibilidad e integridad de la misma” (Gil, 2016, p. 71) (Garriga, 2010, p. 176).

El principio de seguridad implica una obligación para quien trata datos personales, pues este debe garantizar que solamente quien esté autorizado pueda acceder y conocer sobre la información, además proveer un sistema con medidas y configuraciones que puedan proteger los derechos del titular de los datos personales.

Para garantizar el derecho a la protección de datos personales es necesario la aplicación de los principios de calidad, consentimiento y seguridad (Domínguez, 2016, p. 77), pues en efecto estos permiten que sea el usuario quien tenga el control absoluto sobre la información relacionada con él.

1.2. El tratamiento de datos personales en Facebook.

Este ensayo académico se limita a analizar la red social más importante en el mundo virtual, Facebook, esta red social recopila y trata todo tipo de información. Los más importantes, al ser su giro de negocio, son los datos de carácter personal (Noain, 2015, p. 303).

1.2.1. ¿Por qué es la red social más utilizada?

Facebook, para su funcionamiento requiere que los usuarios de la misma proporcionen información (Agustinoy, Monclús, 2016, p. 56), posibilitando su interacción con los demás participantes; es decir, por medio de su actividad, como él envió de una invitación, la comunicación, sus relaciones, el contenido multimedia compartido (fotos, videos, música, etc.), las ideas, las reflexiones, los sentimientos, los pensamientos, su conformidad o disconformidad con el contenido aportado por otros, el proveedor de servicios puede desarrollar criterios para que los usuarios tengan la capacidad de desenvolverse de forma direccionada únicamente a sus intereses.

Para formar parte de Facebook las personas deben crear un perfil, para luego utilizarlo y en caso de no estar conformes eliminarlo; es por eso, que es posible afirmar que existen tres etapas de participación de los usuarios en la red social (Baggiolini, 2013, p. 963): registro, uso y cancelación (Facebook, 2015):

a) Registro: en esta etapa se crea un perfil, en donde el usuario aporta información como su nombre, apellido, edad, sexo, dirección, número telefónico, además, se vincula el correo electrónico, se configura una contraseña, se ingresan datos como formación educativa, estado civil, lugares, preferencias, ideologías, objetivos, fotos, entre otros; esto con la finalidad de que los demás usuarios puedan identificar al dueño del perfil, es decir, se hace a la persona identificable ante terceros.

Para darse de alta en la red social, se debe cumplir con el requisito de tener como mínimo catorce años, sin embargo, muchos niños menores a esta edad participan dentro de la misma; debido a esto, Facebook hace esfuerzos diarios para identificar estos perfiles con la finalidad cerrarlos, evitando que menores se expongan a los peligros que acarrea la red.

b) Uso: una vez creado el perfil del usuario, este se dispone a desarrollar actividades dentro de Facebook, como la actualización y aportación de información, dentro de esta fase se perfecciona el perfil, debido al monitoreo continuo de dicha actividad. Cada acción que se efectúa, como dar *like* permite al proveedor de servicios conocer sobre las preferencias, gustos o aquellas cosas que le desagradan a la persona, posibilitándole adaptar el perfil del usuario a sus necesidades, evitándole perder el tiempo en servicios que no utiliza, le molestan o le incomodan.

c) Cancelación: Para el usuario implica el darse de baja de la red social; es la última intervención que realizan las personas dentro de la misma. En cualquier momento, aquellos que cuentan con un perfil de Facebook, pueden eliminarlo.

Formar parte de esta red social, implica otorgar información. Facebook, es una red social gratuita en apariencia (Noain, 2015, p. 290); permite que los usuarios creen un perfil, usen y se den de baja, sin pagar dinero, pero se debe tomar en cuenta que en la actualidad la información es una fuente importante de ingresos (Aguilar, Said, 2010, p. 207) (Zamora, 2006, p. 21), por lo que el costo es permitir que el proveedor de servicios trate los datos que los individuos aportan.

Actualmente, Facebook es la red social con mayor número de usuarios a nivel mundial, haciéndola la más influyente. Los usuarios tienen tres momentos de participación, en donde aportan datos que permiten que otros individuos los reconozcan.

1.2.2. Sujetos que participan en Facebook.

Facebook cuenta con varios actores, como: proveedor de servicio, usuarios, creadores de aplicaciones, clientes, empresas asociadas, anunciantes, entre otros (Alim, Ewemie, Kalibal, Thornton, s.f., p. 45) (Serrano, 2002, p. 27). Cada uno de estos participantes cumple con una determinada función y realiza varias acciones en la red social.

a) Proveedor de servicios: es aquel que diseña, administra y da soporte, es decir, es el que brinda el servicio (Borrás, 2013, p. 16); es el encargado de la recopilación y tratamiento de datos. Es la compañía que ofrece el diseño de biografía y sus servicios conexos.

b) Usuarios: son aquellas personas naturales o jurídicas que hacen uso del servicio prestado por el proveedor de Facebook. La mayoría de usuarios en esta red social son niños, niñas y adolescentes. En Estados Unidos, el 82% de usuarios son infantes y jóvenes (Facebook, 2010). En Ecuador dos millones de niños, niñas y adolescentes cuentan con un perfil activo en la mencionada red social (INEC, 2014). Con la finalidad de que los niños no expongan sus datos, no se permite que menores de catorce años puedan suscribirse (Facebook, 2015).

c) Clientes (anunciantes y desarrolladores de información): son participantes importantes dentro del desarrollo de la red social, ya que, mediante la adquisición de bases de datos monitoreadas por el proveedor de servicios, son una fuente de financiamiento para el mismo. El 65% de los ingresos de Facebook proviene de la publicidad (Instituto Internacional de Marketing, 2015). Para el usuario aparentemente el servicio que presta Facebook es gratuito, si se considera que en el aspecto monetario las personas que se dan de alta en la mencionada red social no pagan dinero por ser parte de la misma.

Pero, debe considerarse que el precio es el de ceder sus datos personales, para que sean utilizados para estudios de mercado por anunciantes y desarrolladores de información, con la finalidad de incrementar sus ganancias y a su vez para

que Facebook pueda financiarse y siga prestando dicho servicio (Ornelas, 2011, p. 115).

d) Creadores de aplicaciones: son personas que desarrollan de forma externa aplicaciones como juegos: cuestionarios, entre otras (Velasco, 2013, p. 23). Para poder hacerlo, los creadores de aplicaciones acceden y tratan las bases de datos proporcionadas por el proveedor del servicio.

Dentro de los actores previamente mencionados, es importante incluir a aquellas personas que, a pesar de no haberse dado de alta dentro de la red social Facebook, forman parte de la misma, esto debido a que, otros usuarios han manejado su información en diversas actividades, como en fotos, menciones, invitaciones, publicaciones, etc. (Facebook, 2014) (Santos, 2005, p. 43). Estos terceros al igual que los usuarios de la red social, merecen protección sobre sus datos compartidos y manejados en la misma.

Al haber analizado a los actores que intervienen en Facebook podemos evidenciar que cada uno es importante para su funcionamiento, pues cumplen con roles específicos que permiten el correcto desenvolvimiento de la dinámica de la red social; sin embargo, se puede constatar que el tratamiento de la información que usuarios proporcionan es aprovechada por los demás participantes para obtener beneficios sobre los mismos, y en algunas ocasiones dicha recopilación y manejo pueden acarrear transgresiones a los datos personales.

1.2.3. Política de Facebook en relación a datos personales.

Facebook es una red social que evidencia el constante tráfico de información, recopila y trata datos personales; por lo que, es importante analizar qué tipo de información recoge, el uso y el destino de la misma, para lo cual se hará un análisis de la política de datos de la red social. (Anexo 1).

De forma general, puede recoger información sobre acciones personales, acciones de terceros, redes, conexiones, pagos, dispositivos, sitios web, aplicaciones, socios y empresas de la red social (Facebook, 2016) (Sans, 2009, p. 113) (Alim, Ewemie, Kalibal, Thornton, s.f., p. 49). Los usuarios pueden usar distintos servicios dentro de Facebook, por lo que, el tipo de información que compile el servidor está relacionado con la clase de prestación o función que las personas utilicen (Garriga, 2015, p. 153):

a) Acciones personales: mientras se hace uso de la red social Facebook, los usuarios disponen de un número indeterminado de servicios, como compartir contenido, enviar mensajes, o la forma de interacción. De estas actividades el servidor puede compendiar información como, por ejemplo, la frecuencia que se usa un servicio, la duración de la utilización del mismo, fecha, hora y lugar en que una foto fue capturada y compartida, contenido de los mensajes que se envían, *likes*, búsquedas, entre otros.

b) Acciones de terceros: de la misma forma se recopila información sobre un usuario, cuando terceros desarrollan actividades en donde incluyen datos sobre esa persona (Facebook, 2016); como fotos en donde aparece, mensajes que le envían, la sincronización de contactos, etc.

c) Redes y conexiones: la red social también recopila aquella información relacionada a la interacción a las personas y grupos a los que el usuario pertenece.

d) Pagos: información sobre los datos ligados a la tarjeta con la que se efectúen compras dentro de Facebook; como compra de juegos o aplicaciones, donaciones, entre otros; está información incluye detalles sobre la transacción como: el envío, autenticación, facturación, entre otros.

e) Dispositivo: datos sobre y generados por cualquier tipo de dispositivo del que un usuario accede a su cuenta (Facebook, 2015). Con la finalidad de que el usuario goce de conectividad entre los distintos instrumentos que utilice.

f) Sitios web y aplicaciones: todo lo relacionado a los sitios web y aplicaciones relacionadas con la red social, es decir, se registra la visita, la duración de la misma y la forma en que se usa dicho sitio o aplicación.

g) Socios: los socios de Facebook proporcionan datos sobre los usuarios, acerca de la forma en que se relacionan con el mismo.

h) Empresas de Facebook: al igual que los socios, las empresas de la red social generan y proporcionan información sobre los usuarios y su forma de interactuar con los mismos (Facebook, 2015).

La red social usa la información con cuatro finalidades básicas: a) comunicarse directamente con el usuario, esto quiere decir que envía mensajes de marketing para dar a conocer mejor los servicios de la red social, así como cualquier asunto importante relacionado con la compañía; b) para evaluar de que forma la publicidad es relevante para el usuario, mejorando así los sistemas de anuncios y servicios; c) para proporcionar, mejorar y desarrollar servicios, con el objetivo de mejorar el servicio; d) y para fomentar la seguridad y protección (Facebook, 2014).

1.2.4. Conflicto de puerto seguro.

Que Facebook sea una empresa estadounidense, implica una transferencia internacional de datos pertenecientes a usuarios de otros países, lo que significa la existencia de un conflicto, pues estos manejan criterios diferentes.

Europa tiene una visión incompatible con E.E.U.U., debido a esto, el 26 de julio del 2000 se celebró el *Safe Harbor Agreement*, con la finalidad de armonizar estas dos concepciones, haciendo que exista una política de protección apropiada (Facebook, 2014).

Este acuerdo fija principios rectores que las empresas estadounidenses que manejan datos de ciudadanos europeos deben cumplir (Joyanes, 2016, p. 128), además, impone la necesidad de que las mencionadas compañías creen medidas de seguridad para el manejo de la información, así como el reconocimiento de derechos de acceso, rectificación, cancelación y oposición, adicionalmente, requiere la implementación de procesos de seguimiento y sanción en caso de que se presenten transgresiones.

Sin embargo, el acuerdo de puerto seguro en su aplicación evidenció problemas como la multiplicidad de legislaciones y una diversidad de instituciones con competencias insuficientes, por lo que, los principios contemplados en el convenio no bastaron para garantizar un adecuado tratamiento en los datos personales.

En el año 2013 el ciudadano austriaco Maximilliam Schrems hizo un reclamo al *Data Protection Commissioner* con sede en Irlanda, para que se prohibiera la transferencia de sus datos a Estados Unidos, requerimiento que le fue negado.

Luego, presentó un recurso ante la *High Court* de Irlanda, que realizó un análisis, enfatizando que la legislación estadounidense no era compatible con la de la Unión Europea, pues instituciones como el NSA o el FBI, podían realizar operaciones de vigilancia e interceptación selectiva sin necesidad de justificación alguna, lo que era totalmente contrario a la Constitución Irlandesa, ya que está prevé un principio de proporcionalidad, en donde debía argumentarse por qué se iban a realizar dichas acciones.

Una vez realizada esta reflexión, la *High Court* decidió suspender el proceso, para plantear uno ante el Tribunal de Justicia de la Unión Europea, pues el estudio de la validez o no del acuerdo, les concernía a todos los miembros.

Mediante sentencia de 06 de octubre de 2015, el Tribunal de Justicia de la Unión Europea declaró la invalidez del acuerdo, por las siguientes razones: a) Falta de fiabilidad en el autocertificación, pues no existían mecanismos suficientes para

constatar que se cumplan con los principios establecidos en el acuerdo. b) No habían garantías de que las empresas estadounidenses contemplen medidas suficientes para la protección de datos. c) Se permitía que las empresas vulneren datos en caso de que se sospeche una afectación a la seguridad nacional o el interés público, sin necesidad de justificarlo. d) Se prevé mecanismos de solución pacífica y alternativa, como arbitraje en materia comercial, pero nada se dice sobre aquellos conflictos que radican en el mal manejo de datos personales y e) la falta de legislación en Estados Unidos, que garantice efectivamente los derechos de las personas en relación a la transferencia de información.

Para que Facebook pudiera seguir usando información de usuarios pertenecientes a la Unión Europea, debía hasta el 6 de enero del año 2016, informar al Registro General de la Agencia Española de Protección de Datos Personales sobre la continuidad de la transferencia de datos y los mecanismos que se han adoptado para garantizar un tratamiento correcto de datos personales.

Condición que se sometió a una serie de negociaciones que desencadenó la creación del Marco de Escudo de la privacidad Unión Europea-Estados Unidos el 12 de Julio de 2016, al que Facebook se adhirió con la finalidad de continuar usando los datos de los usuarios europeos. Este documento recoge derechos fundamentales que pretenden proteger a los ciudadanos en relación a la información que compañías norteamericanas manejan, en donde se establecen obligaciones para los proveedores de servicios, para la administración estadounidense y mecanismos de revisión (Facebook, 2016).

En general, la información que Facebook recopila, permite crear un perfil del usuario que lo hace identificable, característica primordial de los datos personales (Pfeiffer, 2008, p. 47), es por eso que, no es erróneo afirmar que la red social es responsable de la compilación, uso y destino que se le dé a los mismos, sin embargo, el usuario es responsable a la hora administrar la información que comparte con la mencionada red social.

Facebook evidencia el dinamismo de la web y el elevado tráfico de datos personales, es la red social más utilizada en el mundo, basando su giro de negocio en la información que sus usuarios proporcionan; ha contribuido a una nueva concepción de datos personales que abarca acciones, ubicación, conexiones, pagos, entre otras; dando como resultado que los datos que en apariencia pueden ser carentes de importancia, puedan ser aprovechados y a su vez mediante su tratamiento, se pueden transgredir a los titulares de dichos datos.

2. Relevancia jurídica del derecho a la protección de datos personales en relación a niños, niñas y adolescentes.

2.1. La de datos personales en relación a niños, niñas y adolescentes en redes sociales (Facebook).

Diariamente, dentro del entorno de las redes sociales como Facebook los individuos están constantemente compartiendo información concerniente a su persona (Zamora, 2006, p. 17) (INTENCO, 2012), lo que en la mayoría de casos implica el desconocimiento sobre el destino y manejo de la misma por parte de los usuarios, facilitando el mal uso, distribución o difusión de los datos, generando que los individuos se encuentren ante constantes vulneraciones a sus derechos.

Facebook, es una compañía que tiene su sede en Estados Unidos, California, por lo que, su visión sobre el tratamiento de información personal va ligada a la concepción del autocontrol y la autoregulación (Benítez, 1997, p. 119) (Campuzano, 2000, p. 162), lo que quiere decir que son los individuos los responsables de hacer cumplir las normas referentes al tratamiento de sus datos personales.

Niños, niñas y adolescentes constituyen una parte de la población que requiere especial protección respecto de su integridad y dignidad; es evidente que su

cercanía con la tecnología y la red informática ha permitido que su relación con este entorno sea muy confortable; a su vez, gozan de los mismos derechos que los adultos, pero requieren un amparo especial en sus derechos, debido a que constituyen un grupo de atención prioritaria, tienen está característica, ya que se encuentran en una etapa de aprendizaje, en donde necesitan la orientación y cuidado de adultos para su integral desarrollo (Martínez, Rallo, 2010, p. 83). En Internet, sobre todo en redes sociales como Facebook, los menores se encuentran frente a varios peligros correspondientes a la publicidad y apertura de los datos personales que comparten a diario (Simon, 2009, p. 62).

> “Para los niños, niñas y adolescentes, las TIC son el modo “nativo” de comunicación entre ellos y de interacción con el mundo, por eso se los llama nativos digitales. En octubre de 2010, UNICEF realizó una investigación sobre el uso de las redes sociales entre los adolescentes, que mostró que estas –sobre todo Facebook– son las herramientas de comunicación más utilizadas”. (p. 2).

Niños y adolescentes no poseen la madurez suficiente para desenvolverse en dicho sistema, generando en ellos una despreocupación y desconocimiento sobre los peligros que corren (Vizcaíno, 2001, p. 198) (Aparicio, Batuecas, 2015, p. 90); los riesgos antes descritos son de distinta categoría, y una de las causas más frecuentes de los mismos, es la facilidad con la que los niños, niñas y adolescentes revelan sus datos dentro del espacio cibernético.

La relación de niños y jóvenes con las redes sociales es una muestra de la evolución de la sociedad, pero a su vez este vínculo implica que se deben hacer esfuerzos para proteger los derechos de niños y adolescentes en este entorno (Altmark, Molina, 2012, p. 113). La UNICEF ha declarado la necesidad de implementar garantías reforzadas para preservar la dignidad de niños, niñas y adolescentes; por lo que, los Estados deben adoptar medidas que garanticen efectivamente los derechos de las personas, sobre todo en materia de niñez y adolescencia, pues requieren una protección especial.

Este principio de protección especial está directamente relacionado con el derecho a la protección de datos personales en redes sociales como Facebook (Muñoz, 2016, p. 128) (Velasco, 2013, p. 36), pues obliga la creación de herramientas y políticas por parte del proveedor del servicio para dar primordial atención a la preservación de la información relacionada con menores e impone la participación conjunta de la familia para resguardar a niños y jóvenes en relación a sus datos. Para garantizar los derechos de este grupo es necesario un esfuerzo conjunto entre las organizaciones estatales e internacionales, el proveedor de servicio y la familia (Tello, 2013, p. 102) (Bueno, 2014, p. 164). Facebook, debería prestar mayor atención a este grupo en relación a sus datos personales, ya que su falta de criterio, los hace blancos fáciles de abuso y por ende más propensos a la vulneración de sus derechos.

Con la finalidad de proteger a los usuarios jóvenes e infantes, Facebook ha implementado una serie de funciones de perfil (Facebook, 2016) (Rodríguez, Urrutia, 2012, p. 69). Primero, cuenta con herramientas que le permiten al usuario seleccionar con qué personas comparte contenido. Segundo, mediante un software limita la interacción de menores con desconocidos. Tercero, tiene configuraciones de privacidad, que pueden ser activadas por el niño o adolescentes con la finalidad de que sus datos no sean visualizados por otras personas. Si bien es cierto, estas medidas tienen el objetivo de brindar seguridad, no son suficientes para garantizarla.

Las herramientas que le permiten al usuario seleccionar con qué personas comparte contenido, son un mecanismo que le permite al menor de edad, configurar que personas pueden ver lo que ha publicado o compartido; lo cual es útil, pero a la vez insuficiente, pues se deja a criterio del menor que puede o no ser visto por el público, cuando se ha establecido que por su falta de madurez requieren de guía y protección especial.

El sistema que limita la interacción con desconocidos, es un software que tiene la funcionalidad de reducir las relaciones con aquellos usuarios que no se tiene ningún tipo de vínculo (Garriga, 2015, p. 167). Lo que puede ser útil, pero pierde

sentido al momento en que un usuario al que el menor no conoce, envía una solicitud de amistad y ésta es aceptada, debido a la falta de cuidado y madurez en el proceder del niño o joven, pues para este grupo es importante ganar popularidad y aumentar el número de seguidores, lo que genera un riesgo inminente.

Las configuraciones de privacidad, se componen por una serie de pasos que el menor debe seguir, para evitar la publicidad de sus datos. Sin embargo, estas configuraciones, en muchos casos, no son ejecutadas, por lo que los datos de niños, niñas y adolescentes son públicos, permitiendo que corran riesgos en la *web* (Cebrián, 2008, p. 362). Estas funcionalidades tienen el objetivo de proteger al menor de los riesgos a los que conlleva su interacción en la red social con otros usuarios, no obstante, no son adecuadas, dado que los menores no gozan de un nivel de prudencia y sensatez suficiente para ejecutarlas de forma correcta, por consiguiente, necesitan la supervisión de un adulto que observe su buen desenvolvimiento. Pero debe existir una corresponsabilidad, pues es necesaria la supervisión de los padres sobre la actividad, pero también debe ser el proveedor de servicios quien implemente medidas eficientes y eficaces para garantizar su protección.

Con la intención de evitar transgresiones en la integridad y dignidad de los menores de edad, la red social realiza campañas informativas, intentando concientizar en niños y jóvenes sobre la importancia de ser cautelosos con su información, así como lo primordial de no aceptar solicitudes de extraños. Además, en cada actividad que realizan los menores, envían alertas permanentes en donde anuncian que consecuencias podría traer dicho acto. Está medida está bien direccionada, pero sola no surte efecto, pues en la mayoría de los casos son ignorados por el usuario.

Facebook, también tiene la política de no permitir que niños menores a catorce años se den de alta en la red social, sin embargo, como ya se había mencionado en párrafos anteriores, hasta el 2015 en los países de México, Brasil y Argentina siete millones y medio de niños entre siete y doce años se dan de alta mintiendo

acerca de su edad. Por lo que, al igual que las funcionalidades antes descritas, este requisito es insuficiente para preservar los derechos de menores de edad.

Los proveedores de servicio de redes sociales, en el año 2009 suscribieron el *"Safer Social Networking Principles for the EU",* ya que consientes de las constantes amenazas que sufren los menores de edad, establecieron principios de autorregulación para proteger a niños, niñas y adolescentes de ataques, contenidos inapropiados o el acceso y uso ilícito de sus datos con la finalidad de lesionar sus derechos. En este sentido Facebook aumento a 14 años la edad mínima para darse de alta en la red social.

Todas las herramientas, políticas, funciones y configuraciones, si bien son insuficientes están direccionadas a la protección de los datos de menores en relación a otros usuarios que pudieren usar la información para cometer delitos, pero nada se ha hablado de garantizar el derecho a la protección de datos, en relación al tratamiento por parte del proveedor de servicios, sus filiales y clientes, al momento de usar dichos datos para provechos de marketing o económicos, que si bien no lesionan de forma grave a los menores, de igual forma vulneran sus derechos, ya que se abusa de su criterio en formación para explotar la venta de productos o servicios.

Facebook, con el paso del tiempo, debido a las exigencias de las legislaciones y de los acuerdos internacionales en la materia, han implementado mecanismos mínimos de protección, ya que su visión sobre la información es meramente lucrativa, por lo que es necesario exigir que se cumplan estándares más altos por parte de la red social. La protección de datos personales en la red social Facebook, no está plenamente garantizada, es verdad que se han incluido políticas y herramientas con este objetivo, pero no son suficientes, pues no lo hacen de forma integral.

2.1.1. Conductas lesivas.

Exponer datos de niños, niñas y adolescentes en redes sociales como Facebook, implica enfrentarlos a varios riesgos. La falta de conciencia a la hora de hacer pública la información personal de los niños y jóvenes permite que se vulneren los derechos de este grupo. La importancia de proteger a los datos personales radica en el evitar que se cometan lesiones en su integridad y dignidad (Antúnez, 2016, p. 84).

Los niños y adolescentes son un grupo que desarrolla a diario actividades dentro de las redes sociales como Facebook, en algunos casos este desenvolvimiento implica que hagan públicos sus datos (Freixas, 2001, p. 45), facilitando que terceros accedan a ellos y mediante su tratamiento lesionen sus derechos.

Prácticas como el *cyberbullying*, *sexting* y *grooming* ponen en riesgo el honor, la intimidad, la honra y buen nombre de los menores (Escribano, 2014, p. 86) (Area, 2016, p. 20). Estas prácticas son posibles, dada la sencillez con la que las personas acceden a la información de los niños y adolescentes, a la falta de mecanismos de protección de dichos datos y la escasez de conciencia que existe en los menores a la hora de ejecutar actividades en redes sociales.

Si bien es cierto, son terceros ajenos al proveedor de servicios quienes cometen estás prácticas, es Facebook quien proporciona la plataforma y está obligado a brindar mecanismos de protección de la información personal con la finalidad de evitar que sea usada como un medio para el cometimiento de estos delitos.

El ciberacoso o *cyberbullying,* es una práctica que se realiza mediante el uso de TIC. Son agresiones causadas por medio de la divulgación o difusión de datos personales, que pueden o no ser verdaderos (Ornelas, 2011, p. 126). Engloba, prácticas como la creación de perfiles falsos en Facebook y otras redes sociales, la recopilación no autorizada de información sobre la víctima, el monitoreo continuo de la actividad que el usuario realiza en la red social, injurias, calumnias, la publicación de información falsa, destrucción de datos, entre otras actividades que tienen como finalidad el amedrentar al menor para obtener algún beneficio.

El *sexting* comprende la transferencia, mediante el uso de medios tecnológicos, de contenido erótico y pornográfico, por ejemplo, mediante *Facebook Messenger*, está práctica es muy común en adolescentes (Santos, 2005, p. 59). De esta actividad surge la difusión y divulgación no autorizada de este contenido por parte de su autor, lo que en algunos casos puede también desencadenar un delito de pornografía infantil. Se evidencia que la información como fotografías o formas de expresión sexual, que en apariencia son carentes de importancia, constituyen datos personales que al ser vulnerados afectan la reputación del menor, transgrediendo su derecho al honor, intimidad, buen nombre y sobre todo sus derechos sexuales.

El g*rooming* es uno de los delitos más preocupantes en relación a la participación de niños y jóvenes en redes sociales como Facebook, pues la publicidad de sus datos como su edad, los hacen susceptibles de adultos que buscan menores con el objetivo de crear lazos emocionales, para evitar que se cohíban, poder abusar sexualmente de ellos y en algunos casos integrarlos a organizaciones de pornografía infantil y trata de personas. De esta práctica es evidente que la falta de protección en el dato personal del niño o adolescente lo hace vulnerable al ataque a su dignidad e integridad.

Otras conductas lesivas comunes, menos graves ya que no vulneran la dignidad sexual de los menores o su reputación, son aquellas relacionadas a estudios de mercado y *marketing* dirigido (Gil, Quintanilla, 2016, p. 115) (Instituto Internacional de Marketing, 2015), ya que se pretende llegar con productos o servicios a niños y adolescentes incentivando el consumismo.

Si bien es cierto se necesita de la autorización de los padres para realizar pagos, se hace llegar el mensaje de que es necesaria la adquisición para ganar popularidad o evitar el aburrimiento, lo que puede parecer inofensivo, si no se considera que el criterio de los menores no está formado y es más fácil influir de forma negativa en sus preferencias, haciendo que ejerzan presión sobre sus padres.

Existen varias formas de lesionar los derechos de niños, niñas y adolescentes mediante el tratamiento de sus datos personales, unas más graves que otras. La falta de reflexión y análisis a la hora de hacer pública la información personal de menores, los expone a prácticas como el ciberacoso, sexting o grooming, lo que transgrede su integridad, intimidad, honra y buen nombre, pues facilita que personas malintencionadas hagan un uso doloso de sus datos. Además, su falta de criterio y madurez los hacen susceptibles de aprovechamiento por parte de desarrolladores de aplicaciones, o compañías para incentivar el consumo de productos o servicios, lo que genera la vulneración a su dignidad e integridad.

2.1.2. Especial protección al interés superior de los niños, niñas y adolescentes.

De acuerdo a la Constitución del Ecuador del año 2008, niños, niñas y adolescentes son un grupo que requiere prioridad en la atención, esto debido a su condición de vulnerabilidad respecto de los demás actores de la sociedad (Simon, 2009, p. 43). En este sentido el artículo 44 prevé lo siguiente:

> “El Estado, la sociedad y la familia promoverán de forma prioritaria el desarrollo integral de las niñas, niños y adolescentes, y asegurarán el ejercicio pleno de sus derechos; se atenderá al principio de su interés superior y sus derechos prevalecerán sobre los de las demás personas (...)” (Constitución, Art. 44).

De lo que podemos deducir que tanto la sociedad, la familia y el Estado, entendido como una organización dotada con funciones y facultades dadas por el pueblo, están obligados a proteger plenamente los derechos de niños y jóvenes (Rodríguez, Urrutia, 2012, p. 65) (Tello, 2013, p. 96).

Bajo éste mismo criterio la Convención sobre los derechos de los niños, en su artículo 3 numeral 1 promulga lo siguiente:

> “En todas las medidas concernientes a los niños que tomen las instituciones públicas o privadas de bienestar social, los tribunales, las

> autoridades administrativas o los órganos legislativos, una consideración primordial a que se atenderá será el interés superior del niño" (Convención sobre los derechos de los niños, Art 3.1).

De lo que se evidencia la aplicación a nivel mundial de este principio. Las redes sociales como Facebook, forman parte de una sociedad globalizada, en donde niños, niñas y adolescentes son agenten activos de participación, por lo que considerar su protección es primordial a la hora de brindar el servicio.

De este criterio, se puede afirmar que Facebook está obligado a hacer un esfuerzo mayor para brindar la seguridad a este grupo, no solo debe cumplir con estándares mínimos exigidos por las leyes o acuerdos internacionales, sino que debe trabajar constantemente para brindar la certeza de protección para el integral desarrollo de niños y adolescentes.

2.1.3. Aplicación de los principios del derecho a la protección de datos personales en el caso de niños, niñas y adolescentes.

Los niños, niñas y adolescentes gozan de una protección especial, por lo que es necesaria la observancia de los principios que rigen al derecho de protección de datos personales.

2.1.3.1. Principio de calidad.

En líneas anteriores se manifestó que el principio de calidad garantiza que el titular del fichero de datos personales, recabe información pertinente y no excesiva, adicionalmente se requiere está únicamente sea usada para los fines que el titular ha autorizado.

Mediante la aplicación de este principio se garantiza que los datos personales de niños, niñas y adolescentes, no sean utilizados para actos o hechos ilícitos, asegurando que la dignidad de niños y jóvenes no sea violentada.

2.1.3.2. Principio de seguridad.

Del análisis previo sobre este principio podemos concluir que se debe garantizar la confidencialidad, integridad y disponibilidad de los datos (Aparicio, Batuecas, 2015, p. 127). Su aplicación es primordial en relación a niños, niñas y adolescentes, debido a que se requiere mayor pericia a la hora de brindar medidas que efectivicen el derecho a la protección de datos personales.

2.1.3.3. Principio de consentimiento informado.

En relación a niños, niñas y adolescentes, el análisis de este principio es fundamental, desde el punto de vista de la capacidad. El Código Civil Ecuatoriano establece que todas las personas son capaces mientras la ley no establezca lo contrario, dando como resultado el estudio de esta figura desde la óptica de las incapacidades.

En el artículo 1463 del Código Civil se enlista a los absolutamente incapaces, entre ellos están los impúberes, que de acuerdo al artículo 21 del mismo cuerpo normativo son los varones menores de 14 años y la mujer que no ha cumplido 12 años, mientras que a los jóvenes que se encuentren dentro del rango de 13 a 18, los categoriza como relativamente incapaces.

Para efectos del consentimiento, los impúberes no pueden autorizar el tratamiento de sus datos, mientras que los adolescentes pueden hacerlo siempre y cuando tengan la aprobación de sus representantes, que pueden ser padres o tutores, por lo que, en redes sociales para que su consentimiento sea válido los jóvenes de 13 a 18 años deben contar con el permiso de sus padres para formar parte de la misma.

2.2. Principales iniciativas internacionales para la protección de niños, niñas y adolescente en relación a sus datos personales en redes sociales.

2.2.1. Child Online Protection Initiative (COP).

En este sentido, la Unión Internacional de Telecomunicaciones un organismo especializado de la ONU para las TIC, implemento la *Child Online Protection Initiative* en el año 2008, en adelante COP, con el objetivo principal instaurar una experiencia segura y educar a los todos los niños sobre su actividad en línea.

Está iniciativa desarrolla cinco puntos clave: medidas legales, medidas técnicas y de procedimiento, estructuras organizacionales, creación de capacidad y la cooperación internacional.

a) Medidas legales: La COP diseña criterios y directrices legales para que los Estados miembros las implementen en sus legislaciones internas. Adicionalmente, se encarga de hacer seguimiento de las leyes implementadas por los países en relación al tema.

b) Medidas técnicas y de procedimiento: Realiza recomendaciones y normas clave para que la experiencia de niños y adolescentes en la *web* sea segura.

c) Estructuras organizacionales: La COP promueve y fomenta la creación de organizaciones a nivel mundial para facilitar la implementación de las medidas en los países miembros.

d) Creación de capacidad: Está iniciativa realiza varios eventos a nivel mundial con la finalidad de educar a los niños sobre la actividad en línea que realizan, a los padres sobre cómo supervisar a sus hijos y a los proveedores de servicio sobre cómo brindar una experiencia segura y amigable a los menores de edad.

e) Cooperación internacional: Está iniciativa impulsa la creación de acuerdos con el objetivo de eliminar los riesgos para los niños y jóvenes en la red.

Se han implementado directrices: a) para niños y jóvenes, en donde se da a conocer a los menores sobre los distintos peligros que existen en el espacio cibernético y las consecuencias que acarrea el no tener cuidado en las actividades en línea que realiza. b) Para padres, tutores y educadores que incluyen recomendaciones para que guíen y supervisen las acciones en línea de los niños y adolescentes, haciendo que la experiencia *online* sea positiva. c) Para la industria de las TIC, en donde se facilitan sugerencias sobre como brindar un servicio seguro. d) Para los responsables políticos, con la finalidad de ayudar en la planificación de estrategias de protección para cada país.

2.2.2. Memorándum de Montevideo.

Con esta misma finalidad, en Latinoamérica, se ha creado el “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, en donde se presentan recomendaciones a ser tomadas en cuenta por todos los países de la región de Iberoamericana, con el objetivo de aminorar los peligros que acarrea ser parte de una red social para menores de edad (Seminario de Derechos, Adolescentes y Redes Sociales en Internet, 2009, p. 1-15).

Este documento incluye a) recomendaciones para los estados y entidades educativas para la prevención y educación para los niños, niñas y adolescentes; b) recomendaciones para los Estados sobre el marco legal; c) recomendaciones para la aplicación de leyes por parte de los Estados; d) recomendaciones en materia de políticas públicas y e) recomendaciones para la industria.

Uno de los objetivos principales de este documento es proclamar la integración de los Estados de Iberoamérica, con la finalidad de que se adopten medidas de protección eficientes en las legislaciones internas, armonizándolas. Buscando una unidad que pueda plantear acuerdos similares al de *Safe Harbor*.

El 27 y 28 de julio del año 2009, se llevó a cabo en Montevideo el Seminario de Derechos, Adolescentes y Redes Sociales en Internet, al que asistieron

representantes de Brasil, Ecuador, Canadá, España, Uruguay, México, Colombia y Argentina, en donde se discutió sobre los problemas que surgen de la intervención de menores de edad en Internet, en especial sobre su actividad en redes sociales. En base al debate generado sobre el tema, el Instituto de Investigación para la Justicia crea el Memorándum de Montevideo, con el objetivo de que los participantes se comprometan a seguir las recomendaciones para brindar mayor seguridad a los niños y jóvenes en redes sociales.

Es importante también mencionar que Facebook en conjunto con la UNICEF, se han propuesto la meta de enviar mensajes masivos mediante sus servicios para alertar a padres e hijos, sobre los riesgos que se corre cuando se hace pública la información personal y no se toman las medidas de seguridad necesarias para protegerla (UNICEF, 2011, p. 23).

Estas iniciativas tienen el objetivo común de hacer de Internet y las redes sociales un espacio seguro para niños, niñas y adolescentes, ya que se considera que este grupo requiere de una especial protección, pues como se mencionó anteriormente constituyen un grupo vulnerable. Sin embargo, estas medidas no han sido suficientes, pues el nivel de inseguridad, sobre todo para niños, niñas y adolescentes se eleva a diario y el Derecho no ha sido lo suficientemente dinámico para poder salvaguardar la integridad en especial de los menores de edad, quienes requieren mayor atención.

3. Construcción de redes sociales (Facebook) garantes del derecho a la protección de datos personales de niños, niñas y adolescentes.

El cuidado y protección de niños, niñas y adolescentes en relación a sus datos personales en redes sociales requiere la implementación de medidas que garanticen efectivamente este derecho, sobre todo en este grupo de atención prioritaria.

3.1. Privacidad por diseño.

Es sustancial hablar de la contraposición que existe entre la publicidad por defecto (Lara, 2008, p. 17) frente a la privacidad por diseño. Facebook, es una red social que maneja la publicidad por defecto, en donde es el usuario el llamado a realizar todos los actos para evitar que sus datos sean públicos, es decir que, mediante configuraciones y herramientas, puede o no limitar lo que terceros pueden ver.

Privacy by design o privacidad por diseño, nace en los años noventa, debido a la propuesta de Ann Cavoukian, comisionada para la información y la privacidad de Ontario, de transformar los sistemas de protección de datos personales (s.f., p. 1), reformando el enfoque en donde se necesita el cometimiento de la infracción para activar el sistema, proponiendo un modelo preventivo y dejando de lado la visión correctiva.

Lo que se pretende es que los proveedores de servicio implementen medidas que cumplan estándares efectivos de protección, en donde la confidencialidad de la información sea manejada por defecto, dándoles la oportunidad a los individuos de decidir sobre la publicidad de sus datos (Martínez, Rallo, 2010, p. 192).

La privacidad por diseño permite el correcto funcionamiento del derecho a la protección de datos personales (Muñoz, 2016, p. 134), en donde la reserva de la información del titular del perfil no es una opción únicamente, sino más bien la regla general, en donde las personas son quienes controlan que datos son públicos o no. Es el deber ser (Noain, 2015, p. 231), pues busca que el dominio sobre la información personal le pertenezca únicamente al titular. Es preventiva no correctiva, ya que busca brindar protección integral a los usuarios en relación a su información personal, pues la configuración de privacidad es predeterminada.

Facebook, maneja una plataforma de publicidad de la información por defecto, haciendo necesario que sean las personas quienes mediante configuraciones accedan a la privacidad de sus datos, lo que en el caso de niños, niñas y adolescentes los hace vulnerables a los peligros de la red y la violación de derechos por la misma compañía.

La red social no implementa la privacidad por diseño pues al ser la información es considerada una fuente de ingresos (Castelló, 2010, p. 35), lo que se pretende es tener un acceso más sencillo por parte de quien trata datos para financiarse de mejor manera.

La publicidad por defecto es conveniente para solventar la necesidad de las compañías proveedoras de servicio de acceder, recabar y manejar datos personales, que posteriormente serán un activo de la compañía (Castelló, 2010, p. 35), ya que pueden ser transferidos o compartidos para distintos fines. La privacidad por diseño es una medida de autoregulación por parte de las redes sociales y gira entorno a siete principios (Cavoukian, s.f., p. 3):

3.1.1. Proactividad y prevención: Está es una de las características principales de este modelo, pues no busca que existan transgresiones a los derechos del titular para que se active el sistema de protección, sino que garantiza la integridad y dignidad de los individuos anticipadamente, evitando la aparición de vulneraciones. Facebook evidentemente no cumple con este principio, ya que se basa en un modelo de autoregulación y autocontrol, donde es el usuario el encargado de hacer cumplir la normativa en relación a los datos del que es titular y reclamar en caso de que existan transgresiones a sus derechos.

3.1.2. Privacidad como configuración predeterminada: Lo que se pretende es que el titular sea quien tenga el dominio de los datos, por lo que las herramientas están orientadas a que su utilización mantenga la confidencialidad de la información. De la plataforma podemos deducir que la configuración predeterminada en Facebook es “Público”, en donde son los individuos quienes deben realizar operaciones para evitar la publicidad de su información.

3.1.3. Privacidad incrustada en el diseño: La estructura de las plataformas de redes sociales mantendrá la debida reserva de los datos personales como base fundamental de su arquitectura. Si bien, el giro del negocio de Facebook es la difusión de contenidos y por ende debería trabajar con privacidad por diseño; sin embargo, para proteger a las personas se deben implementar en la estructura mecanismos de control para que el usuario pueda conocer y disponer sobre el uso y destino de sus datos. La estructura y arquitectura de la red social Facebook, evidencia la publicidad por defecto, en donde no se prevé la debida confidencialidad de los datos.

3.1.4. Funcionalidad total: Complementa la seguridad y la confidencialidad de la información. Facebook, no goza de funcionalidad total. No se implementa en la plataforma la seguridad y confidencialidad de los datos.

3.1.5. Seguridad extremo a extremo: Se garantiza un nivel óptimo de protección. En donde el responsable del tratamiento de datos personales, debe garantizar la seguridad de la información en todas las etapas de tratamiento, incluso en el olvido.

Facebook, no aplica esté principio pues de sus políticas podemos evidenciar que solo se hace responsable cuando los datos son manejados por la compañía y sus filiales, pero se desliga de garantizar el derecho respecto de sus clientes (Facebook, 2016).

3.1.6. Visibilidad y transparencia: Se prevé el cumplimiento de los principios que rigen a la protección de datos personales. Como se ha descrito con anterioridad. Facebook únicamente implementa ínfimamente los principios que rigen a la protección de datos, en donde su intención no es ser un agente garante del derecho, sino únicamente continuar tratando datos personales.

3.1.7. Enfoque centrado en el usuario: Se prioriza a los usuarios y por ende se los protege. La red social considera que el tratamiento de datos personales

es un negocio rentable y lucrativo, por lo que su giro de negocio se centra en el uso y manejo de la información personal de los usuarios. En donde, es importante la información, no el individuo.

La privacidad por diseño es un ideal en donde no solo se aplican niveles de protección por cumplir normativas, sino que su desarrollo sea la forma predeterminada de actuar por parte de las compañías. Niños, niñas y adolescentes son un grupo que se beneficiaria de la aplicación de este concepto por parte de Facebook, ellos requieren un estándar más alto de protección, por lo que cumplir con este modelo, garantiza el efectivo goce del derecho a la protección de datos y de otros derechos mediante este, debido a que es un derecho instrumental.

Debido a las constantes transgresiones de derechos que niños y adolescentes sufren por la falta de protección respecto de su información, a nivel internacional se han implementado iniciativas, que, si bien han contribuido a la concientización, no han logrado obligar que Facebook implemente en su giro de negocio el respeto y garantía del derecho a la protección de datos personales de adultos, mucho menos de niños, niñas y adolescentes. Del grupo de iniciativas e investigaciones respecto del derecho a la protección de datos personales, nos llevan a concluir que la tendencia en relación al mismo es implementar cada vez más altos estándares de protección.

Facebook, únicamente cumple con estándares mínimos de protección que se le exigen para continuar tratando datos, en otras palabras, no toma plena conciencia de la aplicación del derecho, no le interesa la seguridad, sino solo seguir obteniendo rentabilidad de los datos. Facebook maneja criterios de publicidad por defecto que no garantizan el pleno goce de este derecho, especialmente en el caso de niños, niñas y adolescentes que requieren un mayor cuidado y atención, por su condición de vulnerabilidad.

Los Estados, las organizaciones que promulgan la protección de niños, niñas y adolescentes, mediante la integración deben trabajar conjuntamente para en

bloque obligar que redes sociales como Facebook y todos los responsables de ficheros automatizados de datos personales integren cada vez mayores lineamientos y seguridades que garanticen el derecho.

Facebook debería reconocer un mayor nivel de protección para el caso de niños, niñas y adolescentes, pues solo podrán mantener un adecuado nivel de confianza en los usuarios si implementa herramientas y configuraciones que protejan efectivamente a niños y jóvenes. Los datos personales son un bien económicamente rentable, por lo que para seguir lucrando de esta información deberá implementar medidas que garanticen el pleno goce de sus derechos.

3.2. Responsabilidad parental como medida de protección efectiva.

Del análisis previamente realizado se puede evidenciar que Facebook es una compañía que en la realidad goza de mucho poder y exigirle que tome medidas efectivas para garantizar el derecho a la protección de datos personales como país es una utopía. Por lo que, una medida eficaz para efectivizar este derecho podría ser la implementación de sanciones a los padres en los casos en que niños y adolescentes sufran algún tipo de agravio debido a la falta de cuidado y supervisión de la actividad que realizan en la red.

La responsabilidad parental implica una serie de obligaciones de los padres o tutores en relación a sus hijos, niños y adolescentes. El artículo 100 del Código de la Niñez y Adolescencia manifiesta que “El padre y la madre tienen iguales responsabilidades en la dirección y mantenimiento del hogar, en el cuidado, crianza, educación, desarrollo integral y protección de los derechos de sus hijos e hijas comunes”.

En el Ecuador la protección y cuidado de los derechos de niños, niñas y adolescentes le corresponde al Estado, a la sociedad y a los padres o tutores, por lo que, en el caso específico de su actividad en la red como es el caso de

Facebook, son padres o tutores, los primeros llamados a velar por que no se vulnere su integridad y dignidad.

La implementación de sanciones a padres o tutores solo aplica en los casos en que las conductas lesivas a niños, niñas y adolescentes se refieren a actividades que afecten su integridad, en donde la plataforma es usada como medio para actividades que denigran la dignidad de este grupo como el s*exting, cyberbullying* o *grooming*.

Para las conductas lesivas que hacen referencia a el tratamiento de ficheros de datos para realizar marketing dirigido o incentivar el consumo en niños y jóvenes en donde ejercen presión sobre sus padres, no se puede sancionar a los mismos, ya que esto no depende del cuidado que se le dé a este grupo, sino más bien a un uso o manejo abusivo de las bases de datos, por parte del titular del fichero, es decir el proveedor del servicio, en específico Facebook.

En el caso concreto del derecho a la protección de datos personales, la privacidad por diseño es la respuesta para un efectivo cuidado de niños, niñas y adolescentes, sin embargo, poder exigirle que compañías como Facebook la implementen, es muy complicado debido a su poder económico.

CONCLUSIONES.

Actualmente, los datos personales son el bien intangible más importante en el campo económico. Facebook, basa su giro de negocio en el tratamiento de dicha información. Niños, niñas y adolescentes encuentran atractivo el uso de la red social, por lo que la recolección, manejo y destino de datos, pertenecientes a este grupo de atención prioritaria, implica un nivel alto de responsabilidad para Facebook, quien se beneficia de la información, pues la exposición pública de los datos puede facilitar la vulneración de la integridad y dignidad de niños y jóvenes. La edad mínima para contar con un perfil en la red social es de catorce años, a pesar de esta política, niños y niñas menores a trece años se dan de alta mintiendo acerca de su edad. Lo señalado evidencia la falta de aplicación de principios del derecho a la protección de datos en la estructura de la plataforma de Facebook.

Alrededor del mundo se han desarrollado diferentes corrientes sobre el régimen de protección del derecho, el caso europeo es paradigmático ya que evidencia que mediante la integración, se ha logrado que compañías económicamente poderosas como Facebook, eleven sus estándares de protección, así mismo en el caso específico de niños, niñas y adolescentes, a nivel internacional se han implementado iniciativas como el Child Online Protection (Organización de la ONU) y el Memorándum de Montevideo que formulan recomendaciones para los responsables de ficheros y los demás actores, que son: el usuario, padres o tutores, escuelas y el Estado, que si bien no son medidas de obligatoria aplicación, son el inicio de la creación de criterios que permitan exigir la correcta aplicación del derecho a la protección de datos personales en relación a niños y jóvenes y su actividad en redes sociales.

Niñas, niños y adolescentes gozan de los mismos derechos que los adultos pero se debe promover su desarrollo integral dándole prioridad a su interés, es decir priorizando sus derechos sobre el de los demás. El Estado, los padres o tutores y la sociedad son los responsables de brindar un cuidado especial a este grupo de atención prioritaria. Niños y jóvenes son usuarios de la red, por lo que su

actividad en la web y sobre todo en redes sociales como Facebook debe estar debidamente resguardada.

Facebook, ha reconocido que niños menores a trece años pueden crear un perfil, debido a esto y asumiendo su responsabilidad ha creado un software para identificar estas cuentas abiertas, en donde se miente acerca de la edad, con la finalidad de eliminarlas definitivamente. Pero está medida no es suficiente para ser una red social garantista del derecho a la protección de datos personales, en consecuencia implementar la privacidad por diseño sería un remedio efectivo para salvaguardar a los jóvenes frente a los riesgos que trae su actividad en la red. Otra solución es la de la de sancionar a padres o tutores en los casos en los que hayan faltado a su deber de cuidado.

REFERENCIAS

Agencia Española de Protección de Datos Personales. (2009). *El derecho fundamental a la protección de datos de carácter personal.* Recuperado el: 13 de noviembre de 2016, de: http://eprints.ucm.es/22832/1/T34731.pdf

Aguilar, D. Said, E. (2010). Identidad y subjetividad en las redes sociales virtuales: caso de Facebook. *Red de Revistas Científicas de América Latina, el Caribe, España y Portugal*, 12, 190-207.

Agustinoy, A. Monclús, J. (2016). *Aspectos Legales de las redes sociales.* Barcelona, España: Bosch.

Alim, H. Ewemie, E. Kalibal, Z. Thornton, M. (s.f.). *Facebook as Organization.* Wilmington, Estados Unidos: Wilmington University.

Almuzara, C. (2005). *Estudio práctico sobre la protección de datos de carácter personal.* Valladolid, España: Lex Nova.

Altmark, D. Molina, E. (2012). *Tratado de derecho informático.* Buenos Aires, Argentina: La ley.

Antúnez, N. (2016). *Fortalecimiento de herramientas para la protección de datos personales frente al debilitamiento del principio de consentimiento.* Salamanca, España: Congreso Iberoamericano de Derecho Informático.

Aparicio, J. Batuecas, A. (2015). *En torno a la privacidad y la protección de datos en la sociedad de la información.* Granada, España: Comares.

Area, M. (2016). Las redes sociales en Internet como espacios para la formación del profesorado. *Razón y Palabra primera revista en Iberoamérica especializada en comunicología,* 63. Recuperado el 13 de noviembre de 2016, de: http://www.razonypalabra.org.mx/n63/marea.html

Baggiolini, L. Castro, S. (2013). La temporalidad de las redes y los dispositivos. *Companam*, s/n, 950-978.

Ballesterini, F. Morduchowicz, R. Marcon, A. Sylvestre, V. (2010). *Los adolescentes y las redes sociales.* Buenos Aires, Argentina: Ministerio de Educación.

Barzallo, J. (2012). *Nuevas tendencias sociales y el cloud computing.* Quito, Ecuador: Congreso Iberoamericano de Derecho Informático.

Benítez, L. (1997). Derecho a la autodeterminación informativa y acción de habeas data en Iberoamérica. *Revista Jurídica de la Facultad de*

Ciencias Jurídicas y Sociales de la Universidad de Talca, 3, p. 116-145.

Borrás, O. (2013). *Manual de Facebook.* Madrid, España: Gabinete de Tele-Educación.

Bueno, F. (Cood.) (2014). *FODERTICS II: Hacia una justicia 2.0. Estudio sobre Derecho y nuevas tecnologías.* Salamanca, España: Ratio Legis.

Bueno, F. (Cood.) (2015). *FODERTICS. Estudios sobre nuevas tecnologías y justicia 3.0.* Granada, España: Comares.

Bueno, F. (Cood.) (2015). *FODERTICS. Estudios sobre nuevas tecnologías y justicia 4.0.* Granada, España: Comares.

Caldevilla, D. (2010). Las redes sociales: tipología, uso y consumo de las redes 2.0 en la sociedad digital actual. *Revista ICONO, 33*, 45-68.

Campuzano, H. (2000). *Vida privada y datos personales.* Madrid, España: Editorial Tecnos.

Castelló, A. (2010). *Estrategias empresariales en la Web 2.0: Las redes sociales.* Alicante, España: ECU.

Cavoukian, A. (s.f.). *Privacidad por diseño, los 7 principios fundamentales.* Ontario, Canadá: Instituto de Privacidad y Big Data.

Cebrián, M. (2008). La web como red social de comunicación e información. *Revistas científicas complutenses*. *14,* 345-361.

Código Civil. (2005). Actualizado a octubre de 2010. Quito: Corporación de Estudios y Publicaciones.

Conde, C. (2005). *La protección de datos personales: un derecho autónomo con base en los conceptos de intimidad y privacidad.* Madrid, España: Dykinson S.A.

Constitución de la República del Ecuador. (2008). Registro Oficial 449 de 20 de octubre de 2008. Reformas en Registro Oficial- Suplemento de 13 de julio de 2011.

Davara, M. (2008). *Manual de Derecho Informático.* Navarra, España: Thomson – Aranzadi.

Dreyzin, A. Fernández, D. Pimentel, L. (2006). *Internet, comercio electrónico y sociedad de la información.* Sao Paulo, Brasil: Decita.

Domínguez, E. (2016). *La protección legal de los datos personales y el spam en el Derecho Argentino.* Buenos Aires, Argentina: UNM.

El Universo. (2011). *Facebook elimina 20 mil perfiles diarios de menores de 13 años.* Quito, Ecuador.

Escribano, P. (2014). *Algunas cuestiones sobre la problemática jurídica del derecho a la intimidad, al honor y a la propia imagen en Internet y en las redes sociales.* Tesis de maestría. Universidad de Catalunya.

Expansión. (2013). *Facebook expulsa a 20 000 usuarios menores de 13 años cada día.* México D.F. México: CNN.

Facebook. (2010). *Política de privacidad de Facebook.* Recuperado el 12 de noviembre de 2016, de: http://gent.uab.cat/pamias/sites/gent.uab.cat.pamias/files/Pol%C3%ADtica%20de%20privacidad%20de%20Facebook.docx_.pdf

Facebook. (2015). *Declaración de derechos y responsabilidad.* Recuperado el 12 de noviembre de 2016, de: https://es-es.facebook.com/legal/terms

Facebook. (2016). *Política de datos.* Recuperado el 26 de septiembre de 2016, de: https://www.facebook.com/privacy/explanation

Freixas, G. (2001). *La protección de datos de carácter personal en el Derecho Español.* Barcelona, España: Bosch.

García, I. (2010). *Comportamientos activos de usuarios 2.0.* Santiago de Compostela, España: OBS.

Garriga, A. (2015). *Nuevos retos para la protección de datos personales.* Madrid, España: Dykinson.

Gil, E. (2016). *Big data, privacidad y protección de datos.* Madrid, España: Ministerio de la Presidencia.

Gil, J. Quintanilla, G. (2016). *Gobierno abierto y datos vinculados: conceptos, experiencias y lecciones con base en el caso mexicano.* México D.F., México: CLIH

Guerrero, M. (2006). *El impacto de internet en el derecho fundamental a la protección de datos de carácter personal.* Navarra, España: Arazandi

Instituto Internacional de Marketing. (2015). *Facebook se lleva el 65% de los ingresos por publicidad en redes sociales.* Madrid, España: Reasonwhy.

INTENCO. (2012). *Guía para usuarios: identidad digital y reputación online.* Madrid, España: Ministerio de Industria, Energía y Turismo.

Jiménez, A. (2016). *Por un marco legal para los delitos contra l identidad de las*

personas en México. México D.F., México: Senado de México.

Joyanes, L. (2016). *Big data, análisis de grandes volúmenes de datos en organizaciones.* México D.F., México: Alfaomega Grupo Editor.

Lara, T. (2008). *La nueva esfera pública los medios de comunicación como redes sociales.* Recuperado el 13 de noviembre de 2016, de: https://telos.fundacióntelefonica.com/telos/articulocuaderno.asp@idarticulo=98rev=76htms#n5

Martínez, R. Rallo, A. (2010). *Derecho y redes sociales.* Pamplona, España: Aranzadi S.A.

Maximilliam Schrems vs. Acuerdo de Puerto seguro. (2015). 06 de Octubre de 2015. Sentencia en el asunto C-362/14.

Murillo, L. (1990). *El derecho a la autodeterminación informativa.* Madrid, España: Tecnos.

Murillo, L. (1990). *Informática y protección de datos personales.* Madrid, España: Cetro de estudios constitucionales.

Muñoz, L. (Cood.) (2016). *Hacia una justicia 2.0. Actas del XX Congreso Iberoamericano de Derecho Informático.* Salamanca, España: Ratio Legis.

Noain, A. (2015). *La protección de la intimidad y vida privada en Internet: la integridad contextual y los flujos de información en las redes sociales (2004-2014).* Madrid, España: Ministerio de la Presidencia.

Orduz, R. (2012). *Niños, jóvenes los mayores usuarios de Internet.* Bogotá, Colombia: Corporación Colombia Digital.

Ornelas, L. (2011). *Protección de datos personales en las redes sociales digitales: en particular de niños y adolescentes.* México D.F., México: Instituto Federal de Acceso a la Información y Protección de Datos.

Pérez, A. (1996). *Manual de informática.* Barcelona, España: Ariel.

Pérez, F. (Cood.) (2016). *El derecho de Internet.* Barcelona, España: Atelier.

Pfeiffer, M. (2008). *Derecho a la privacidad, protección de los datos sensibles.* Bogotá, Colombia: Unbosque.

Ramos, K. (2016). *El valor económico de los datos personales.* Revista Mexicana Consultoría. Recuperado el 13 de noviembre de 2016, de: http://revistaconsultoria.com.mx/el-valor-economico-de-los-datos-personales/

Reascos, L. (2016). *Los delitos contra los datos personales y el habeas data en la Ley 1273 de 2009.* Bogotá, Colombia: Derecho y Realidad.

Rodríguez, N. Urrutia, V. (2012). *Retratos de juventud.* Bilbao, España: Observatorio Vasco de la juventud.

Sanou, B. (2015). *ICT Facts & Figures: The world in 2015.* Ginebra, Suiza: Internacional Telecomunication Union.

Sans, A. (2009). *Las redes sociales como herramientas para el aprendizaje colaborativo: una experiencia con Facebook.* Santiago, Chile: Mentalidad web.

Santos, D. (2005). *Nociones generales de la Ley Orgánica de Protección de Datos.* Madrid, España: editorial Tecnos.

Seminario de Derechos, Adolescentes y Redes Sociales en Internet. (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.* Recuperado el 07 de diciembre del 2016, de: http://clicseguro.sep.gob.mx/archivos/Memorandum_Montevideo.pdf

Serrano, M. (2002). *El derecho fundamental a la protección de datos, Derecho español y comparado.* Madrid, España: Thomson Civitas.

Simon, F. (2009). *Derechos de la niñez y adolescencia: De la convención sobre los derechos del niño a las legislaciones integrales.* Quito, Ecuador: Cevallos.

Tello, L. (2013). *Intimidad y extimidad en las redes sociales. Las demarcaciones éticas de Facebook.* Recuperado el 20 de octubre de 2016, de: www.revistacomunicar.com/índice/artículo.php?numero=41-2013-20

Trejo, R. (s.f.). *La sociedad de la información y sus laberintos.* México D.F., México: UNAM.

UNICEF. (2011). *Internet segura.* Recuperado el 07 de diciembre de 2016, de: https://www.unicef.org/argentina/spanish/Unicef_InternetSegura_web.pdf

Velasco, M. (2013). *Redes sociales y usuarios cuestiones sobre su regulación.* Catalunya, España: Universidad de Oberta.

Vizcaíno, M. (2001). *Comentarios a la Ley Orgánica de Protección de Datos de carácter personal.* Madrid, España: Civitas.

Zamora, M. (2006). *Redes sociales en internet.* Recuperado el: 12 de septiembre de 2016, de: webjam.upload.53.amazonaws.com

20 Minutos Editora (2014) Facebook cambia su política de privacidad y publicidad e incluye pagos y localización. Recuperado el: 12 de noviembre de 2016, de: http://www.20minutos.es/noticia/2295965/0/facebook-cambios/forma-pago/publicidad-localizacion

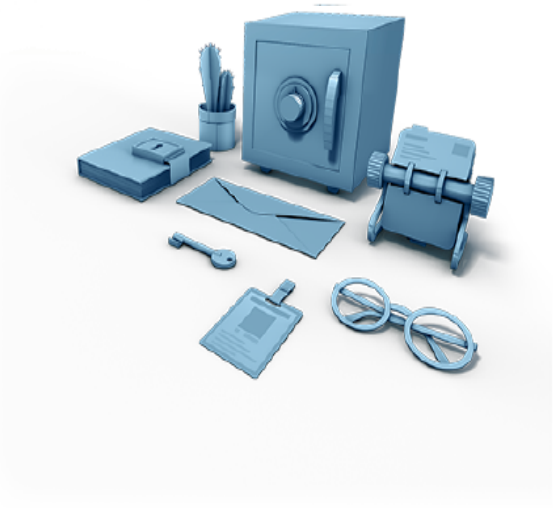
ANEXOS

Política de datos de Facebook.

Política de datos

Te damos la posibilidad de compartir contenido como parte de nuestra misión de hacer del mundo un lugar más abierto y conectado. En esta política se describe el tipo de información que recopilamos, cómo se utiliza y cómo se comparte. Puedes encontrar más herramientas e información en Aspectos básicos de la privacidad.

Cuando consultes nuestra política, recuerda que se aplica a todas las marcas, los productos y los servicios de Facebook que no dispongan de una política de privacidad independiente o que estén sujetos a esta política, los cuales reciben el nombre de "Servicios de Facebook" o "Servicios".



Volver arriba

¿Qué tipo de información recopilamos?

En función de los Servicios que utilices, se recopilan diferentes tipos de información relacionada contigo.

Tu actividad y la información que proporcionas.
Recopilamos el contenido y otros datos que proporcionas cuando usas nuestros Servicios, como al abrir una cuenta, al crear o compartir

- Página Facebook Site Governance
- Aviso sobre el Escudo de la privacidad Unión Europea-Estados Unidos

contenido y cuando envías mensajes o te comunicas con otros usuarios. La información puede corresponder a datos incluidos en el contenido que proporcionas o relacionados con este, como el lugar donde se hizo una foto o la fecha de creación de un archivo. También recopilamos información sobre el uso que haces de los Servicios; por ejemplo, el tipo de contenido que ves o con el que interactúas, o la frecuencia y duración de tus actividades.

La actividad de otros usuarios y la información que proporcionan.
Asimismo, recopilamos el contenido y la información que otras personas proporcionan cuando usan nuestros Servicios y que puede incluir información sobre ti; por ejemplo, cuando alguien comparte una foto en la que apareces, te envía un mensaje o sube, sincroniza o importa tu información de contacto.

Tus redes y conexiones.
Recopilamos información sobre las personas y los grupos a los que estás conectado y cómo interactúas con ellos; por ejemplo, las personas con las que más te comunicas o los grupos con los que te gusta compartir contenido. También recopilamos la información de contacto que proporcionas si subes, sincronizas o importas esta información (por ejemplo, una libreta de direcciones) desde un dispositivo.

Información sobre pagos.
Si usas nuestros Servicios para efectuar compras o transacciones financieras (por ejemplo, cuando compras algo en Facebook, realizas una compra en un juego o haces una donación), recopilamos datos sobre la compra o transacción. Esta información incluye tus datos de pago, como tu número de tarjeta de crédito o de débito y otra información sobre la compra o transacción. Esta información incluye tus datos de pago, como tu número de tarjeta de crédito o de débito y otra información sobre la tarjeta, así como otros datos sobre la cuenta y sobre autenticación, además de información de facturación, envío y contacto.

Información sobre el dispositivo.
Recopilamos información acerca de ordenadores, teléfonos u otros dispositivos donde instales o desde los que accedas a nuestros Servicios, así como la información generada por dichos dispositivos, dependiendo de los permisos que hayas concedido. Podemos asociar la información que recopilamos de tus diferentes dispositivos; de este modo, nos resulta más sencillo prestar Servicios coherentes en todos ellos. Estos son algunos ejemplos de la información de dispositivos que recopilamos:

- Atributos como el sistema operativo, la versión de hardware, la configuración del dispositivo y los nombres y tipos de programas informáticos y archivos, la carga de la batería y la intensidad de la señal, así como datos de identificación del dispositivo.
- Ubicaciones del dispositivo, incluida la posición geográfica específica obtenida, por ejemplo, a través de señales de GPS, Bluetooth o Wi-Fi.
- Información sobre la conexión, como el nombre del operador de telefonía móvil o del proveedor de servicios de internet, el tipo de navegador, el idioma y la zona horaria, el número de teléfono móvil y la dirección IP.

Información de sitios web y aplicaciones que utilizan nuestros Servicios.

Recopilamos información cuando visitas o utilizas sitios web y aplicaciones de terceros que usan nuestros Servicios (por ejemplo, cuando ofrecen nuestro botón "Me gusta" o el inicio de sesión con Facebook, o cuando usan nuestros servicios de medición y publicidad). Dicha información incluye datos acerca de los sitios web que visitas y las aplicaciones que utilizas, el uso que haces de nuestros Servicios en dichos sitios web y aplicaciones, así como datos que el desarrollador o el editor de la aplicación o del sitio web te proporciona a ti o a nosotros.

Información de socios externos.
Recibimos información sobre ti y tus actividades dentro y fuera de Facebook que nos proporcionan socios externos; por ejemplo, información de un socio cuando ofrecemos servicios de forma conjunta o de un anunciante acerca de tus experiencias o interacciones con él.

Empresas de Facebook.
Recibimos información acerca de ti que nos proporcionan empresas pertenecientes a Facebook u operadas por Facebook, de conformidad con sus condiciones y políticas. Obtén más información acerca de estas empresas y sus políticas de privacidad.

¿Cómo utilizamos esta información?

Nos apasiona crear experiencias atractivas y personalizadas para las personas. Usamos toda la información de la que disponemos para poder ofrecer y mantener nuestros Servicios. El procedimiento es el siguiente:

Proporcionar, mejorar y desarrollar los Servicios.
Lo que nos permite ofrecerte nuestros Servicios, personalizar el contenido y proponerte sugerencias es el uso que hacemos de esta información. Nos ayuda a comprender cómo utilizas nuestros Servicios y cómo interactúas con ellos y con las personas o el contenido a los que estás conectado y que te interesan, tanto dentro como fuera de ellos.

También usamos la información de la que disponemos para ofrecerte accesos directos y sugerencias. Por ejemplo, podemos sugerir a un amigo tuyo que te etiquete en una foto comparando sus fotos con la información que hemos recopilado de tus fotos del perfil o de otras en las que se te ha etiquetado. Si esta opción está activada en tu cuenta, puedes controlar si quieres que propongamos a otros usuarios que te etiqueten en fotos a través de la configuración de "Biografía y etiquetado".

Cuando tenemos información sobre la ubicación, la utilizamos para adaptar nuestros Servicios a tus necesidades y a las de otras personas; por ejemplo, te ayudamos a registrar visitas y a encontrar eventos u ofertas en tu zona, o a indicarles a tus amigos que te encuentras cerca de

ellos.

Realizamos encuestas y estudios, probamos funciones en fase de desarrollo y analizamos la información de la que disponemos para evaluar y mejorar los productos y servicios, desarrollar nuevos productos o funciones y llevar a cabo auditorías y actividades dirigidas a resolver problemas.

Comunicarnos contigo.
Usamos tu información para enviarte mensajes de marketing, darte a conocer nuestros Servicios e informarte acerca de nuestras políticas y condiciones. También la utilizamos para responderte cuando te pones en contacto con nosotros.

Mostrar y medir anuncios y servicios.
Utilizamos la información de la que disponemos para mejorar nuestros sistemas de publicidad y medición con el fin de mostrarte anuncios relevantes, tanto en nuestros Servicios como fuera de ellos, y medir la eficacia y el alcance de los anuncios y servicios. Obtén más información sobre cómo anunciarte en nuestros Servicios y cómo controlar el modo en que se usa tu información para personalizar los anuncios que ves.

Fomentar la seguridad y la protección.
Con la información de la que disponemos podemos verificar cuentas y actividades, así como fomentar la seguridad y la protección en nuestros Servicios y en otros de terceros; por ejemplo, investigando actividades sospechosas o infracciones de nuestras condiciones o políticas. Nos esforzamos por proteger tu cuenta; para ello, recurrimos a equipos de ingenieros, sistemas automáticos y tecnología avanzada, como el cifrado y el aprendizaje automático. Asimismo, ofrecemos herramientas de seguridad fáciles de usar que añaden un nivel extra de protección a tu cuenta. Para obtener más información sobre cómo fomentar la seguridad en Facebook, accede al servicio de ayuda sobre la seguridad de Facebook.

Utilizamos cookies y tecnologías similares para prestar y mantener nuestros Servicios, además de cada uno de los usos expuestos y descritos en este apartado de nuestra política. Consulta nuestra Política de cookies para obtener más información.

Volver arriba

¿Cómo se comparte esta información?

Compartir contenido en nuestros Servicios
Los usuarios utilizan nuestros Servicios para conectar y compartir contenido entre sí. Para que esto sea posible, compartimos tu información de las siguientes formas:

Personas con las que te comunicas y compartes contenido.
Cuando compartes contenido y te comunicas usando nuestros Servicios, eliges el público que puede ver lo que compartes. Por ejemplo, si publicas algo en Facebook, seleccionas el público de la publicación, que puede ser

un grupo específico de personas, todos tus amigos o los miembros de un grupo. Del mismo modo, cuando utilizas Messenger, también eliges las personas a las que quieres enviar fotos o mensajes.

La información pública es cualquier información que compartes con el público en general, la información de tu perfil público o el contenido que compartes en una página de Facebook o en otro foro público. Cualquier persona puede ver la información pública dentro o fuera de nuestros Servicios; también es posible consultar estos datos o acceder a ellos a través de los motores de búsqueda en internet, las API y los medios tradicionales, como la televisión.

En algunos casos, las personas con las que te comunicas y compartes información pueden, a su vez, descargar o compartir con otras personas dicho contenido dentro y fuera de nuestros Servicios. Cuando haces un comentario en la publicación de otra persona o haces clic en "Me gusta" en el contenido que ha publicado en Facebook, esa persona decide quién puede ver tu comentario o Me gusta. Si la configuración de privacidad del contenido es "Público", tu comentario también será público.

Personas que ven contenido que otros usuarios comparten acerca de ti.
Otras personas pueden usar nuestros Servicios para compartir información sobre ti con los destinatarios que elijan. Por ejemplo, pueden compartir una foto en la que aparezcas, mencionarte o etiquetarte en un lugar determinado en una publicación o compartir información sobre ti que tú hayas compartido con ellos. Si te preocupa algo que haya publicado un usuario, puedes usar las herramientas de denuncia social para pedir ayuda a alguien de confianza de forma rápida y sencilla. Más información.

Aplicaciones, sitios web e integraciones de terceros en nuestros Servicios o que usan nuestros Servicios.
Cuando utilizas aplicaciones, sitios web u otros servicios de terceros que emplean nuestros Servicios o están integrados en ellos, estas plataformas pueden recibir información acerca de lo que publiques o compartas. Por ejemplo, si juegas a un juego con tus amigos de Facebook o utilizas los botones "Comentar" o "Compartir" de Facebook en un sitio web, el desarrollador del juego o el sitio web pueden obtener información sobre tus actividades en el juego o recibir un comentario o enlace que compartas desde su sitio web en Facebook. Además, si descargas o utilizas estos servicios de terceros, estos pueden acceder a tu perfil público, que incluye tu nombre o identificador de usuario, tu intervalo de edad, tu país e idioma, tu lista de amigos y cualquier otro dato que compartas con ellos. La información que recopilan estas aplicaciones, sitios web o servicios integrados está sujeta a sus propias condiciones y políticas.

Obtén más información sobre cómo puedes controlar la información personal que tú u otras personas compartís con estas aplicaciones y sitios web.

Compartir información dentro de las empresas de Facebook.
Compartimos la información que tenemos sobre ti dentro del grupo de

nuestras empresas.

Nuevo propietario.
Si cambian la propiedad o el control de la totalidad o de parte de nuestros Servicios o de sus activos, podemos transferir tu información al nuevo propietario.

Compartir información con socios externos y clientes
Colaboramos con empresas que nos ayudan a prestar nuestros Servicios y a mejorarlos, o que utilizan productos publicitarios o relacionados; gracias a ellas, podemos gestionar nuestras empresas y proporcionar servicios gratuitos a personas de todo el mundo.

Estos son los tipos de colaboradores externos con los que podemos compartir información sobre ti:

Servicios de publicidad, medición y análisis (solo información que no permita la identificación personal).
Queremos que la publicidad que encuentres en Facebook sea tan relevante e interesante como el resto de la información que veas en nuestros Servicios. Con este objetivo, utilizamos toda la información que tenemos acerca de ti para mostrarte anuncios relevantes. No compartimos información mediante la que se te pueda identificar (esto es, información como tu nombre o tu dirección de correo electrónico que pueda utilizarse para contactar contigo o para identificarte) con socios de publicidad, medición ni análisis, a menos que nos des permiso para ello. Podemos proporcionar a estos socios información acerca del alcance y la eficacia de su publicidad sin incluir información que te identifique, o podemos combinar la información relativa a ti con otra de tal forma que no se te pueda identificar. Por ejemplo, podemos informar a un anunciante acerca del rendimiento de sus anuncios, del número de personas que han visto sus anuncios o que han descargado una aplicación tras ver un anuncio; también podemos proporcionar a estos socios información demográfica que no les permita identificarte (por ejemplo, "mujer de 25 años residente en Madrid a la que le gusta la ingeniería de software"), para ayudarles a conocer a su público o a sus clientes, pero solo una vez que el anunciante haya aceptado cumplir nuestras Normas para anunciantes.

Consulta tus preferencias de publicidad para entender por qué ves un determinado anuncio en Facebook. Puedes ajustar estas preferencias si quieres controlar y administrar la publicidad que ves en Facebook.

Proveedores generales, proveedores de servicios y otros socios.
Transferimos información a proveedores generales, proveedores de servicios y otros socios de todo el mundo que nos ayudan a mantener nuestro negocio prestando servicios de infraestructura técnica, analizando el uso que se hace de nuestros Servicios, midiendo la eficacia de los anuncios y servicios, ofreciendo atención al cliente, facilitando los pagos o realizando investigaciones académicas y encuestas. Estos socios deben cumplir estrictas obligaciones de confidencialidad que se ajustan a esta Política de datos y a los acuerdos que suscribimos con ellos.

¿Cómo puedo administrar o eliminar información sobre mí?

Puedes administrar el contenido y la información que compartes al usar Facebook mediante la herramienta Registro de actividad. También puedes descargar información asociada a tu cuenta de Facebook con nuestra herramienta Descarga tu información.

Almacenamos los datos durante el tiempo necesario para facilitarte productos y servicios, a ti y otros usuarios, incluidos los descritos anteriormente. La información asociada a tu cuenta se conservará hasta que la cuenta se elimine, a menos que ya no necesitemos los datos para ofrecer los productos y servicios.

Puedes eliminar tu cuenta en cualquier momento. Cuando eliminas tu cuenta, eliminamos lo que hayas publicado, como tus fotos y actualizaciones de estado. Si no quieres eliminar la cuenta pero quieres dejar de usar Facebook por un tiempo, puedes desactivarla. Para obtener más información sobre cómo desactivar o eliminar tu cuenta, haz clic aquí. Ten en cuenta que la información sobre ti que otras personas hayan compartido no forma parte de tu cuenta y no se retirará cuando la elimines.

¿Cómo respondemos a requerimientos legales o evitamos que se produzcan daños?

Podemos acceder a tu información, conservarla y compartirla en respuesta a un requerimiento legal (como una orden de registro, orden judicial o citación) si creemos de buena fe que la ley así lo exige. Esto puede incluir la respuesta a requerimientos legales de jurisdicciones ajenas a los Estados Unidos cuando creamos de buena fe que la legislación de esa jurisdicción exige dicha respuesta, que afecta a los usuarios en dicha jurisdicción y que resulta coherente con estándares reconocidos internacionalmente. Es posible que también accedamos, preservemos y compartamos información cuando creamos de buena fe que es necesario para detectar, evitar y combatir el fraude y otras actividades ilegales; para protegerte a ti, a otras personas y a nosotros, también como parte de investigaciones, así como para evitar que se produzcan muertes o daños físicos inminentes. Por ejemplo, podemos proporcionar información a socios externos acerca de la fiabilidad de tu cuenta con el fin de prevenir el fraude y las conductas ilícitas dentro y fuera de nuestros Servicios. Es posible que consultemos, procesemos o conservemos la información que recibamos sobre ti (incluida información sobre transacciones financieras relativa a compras realizadas con Facebook) durante un período prolongado de tiempo cuando esté sujeta a una solicitud u obligación judicial, una investigación gubernamental o

investigaciones relacionadas con posibles infracciones de nuestras políticas o condiciones, o bien para evitar daños. También podemos conservar información sobre las cuentas que se han desactivado por incumplir nuestras condiciones y guardar sus datos durante un mínimo de un año para evitar que se repitan conductas abusivas o infracciones de nuestras condiciones.

Volver arriba

Funcionamiento de nuestros servicios globales

Facebook puede compartir información por vías internas en el seno de su grupo de empresas o con terceros con los fines que se describen en esta política. La información recopilada dentro del Espacio Económico Europeo ("EEE") puede, por ejemplo, transferirse a países de fuera del EEE a los efectos descritos en esta política. Usamos cláusulas contractuales estándar aprobadas por la Comisión Europea, adoptamos otros medios conforme la legislación de la Unión Europea y obtenemos tu consentimiento para legitimar la transferencia de datos del EEE a los Estados Unidos y otros países.

Utiliza la información que incluimos más adelante para ponerte en contacto con nosotros en caso de tener alguna duda o consulta. También intentaremos resolver todos los conflictos que puedan surgir en relación con nuestras políticas y prácticas de privacidad a través de TRUSTe . Puedes ponerte en contacto con TRUSTe desde su sitio web.

Volver arriba

Notificación de los cambios que se produzcan en esta política

Te avisaremos antes de realizar cambios en esta política y te daremos la oportunidad de consultar la política actualizada y hacer los comentarios que consideres pertinentes antes de seguir utilizando nuestros Servicios.

Volver arriba

Cómo hacer llegar tus dudas a Facebook

Para obtener más información sobre la privacidad en Facebook, consulta Aspectos básicos de la privacidad. Si tienes preguntas acerca de esta política, puedes ponerte en contacto con nosotros utilizando la siguiente información:

Si vives en Estados Unidos o en Canadá:

Ponte en contacto con Facebook, Inc. a través de internet o por correo postal en la dirección:

Facebook, Inc.
1601 Willow Road
Menlo Park, CA 94025

Si vives en otro país:

La entidad de control de datos responsable de tu información es Facebook Ireland Ltd., con quien te puedes poner en contacto a través de internet o por correo postal en la dirección:

Facebook Ireland Ltd.
4 Grand Canal Square
Grand Canal Harbour
Dublin 2 Ireland

Fecha de la última actualización: 29 de septiembre de 2016