Universidad Internacional de La Rioja

Facultad de Derecho

Máster Universitario en Protección de Datos

La protección de datos y las redes sociales: mención especial al Ecuador

Trabajo fin de estudio presentado por:	Lenin Hurtado Angulo
Tipo de trabajo:	Trabajo fin de máster
Directora:	Elena Davara Fernández de Marcos
Fecha:	02 de marzo del 2022

Resumen

Uno de los más populares servicios de la sociedad de la información, lo constituyen las llamadas redes sociales, estas constituyen un medio de comunicación, forma de entretenimiento, herramienta de estudio y trabajo especialmente en época de pandemia, pero también en manos interesadas, pueden convertirse en mecanismos de vulneración de derechos mediante el mal uso de los datos personales.

Europa lleva un importante camino recorrido en materia de protección de datos, su legislación actual es producto de la evolución normativa desarrollada desde la década de los 70 del siglo pasado. Ecuador, tras haber experimentado una masiva filtración de datos de sus ciudadanos, aprobó la Ley Orgánica de Protección de Datos, publicada en el Suplemento del Registro Oficial # 486 del 26 de mayo del 2021, lo que marca el inicio de, lo que esperamos sea, la era en la que se proteja como norma general el derecho a la protección de datos personales y se torne eficaz la protección de todos los derechos relacionados.

PALABRAS CLAVES: redes sociales, creación de perfiles, menores de edad, control parental.

Abstract

One of the most popular services of the information society are without any doubt, the social networks. These are a way to get people together, to study and work in pandemic situation. However, not everything is good in relation to social networks, through them, many people have severely suffered the violation of theirs rights, such as privacy, intimacy and, finally theirs personal images.

Europe has follow an important road as far as protection of personal data is concern, the legislation is product of a significant evolution developed since the 70’ of the

last century. Ecuador has recently approved the data protection act, which was published in the Official Bulletin No. 486 of May 26th 2021, this is, we hope, the beginning of the era in what the personal data rights are efficiently protected, as well all right related.

KEY WORDS: social networks, profiles making, parental controls.

Índice de contenidos

Abreviaturas

art.	Artículo
CE	Consejo de Europa
COIP	Código Orgánico Integral Penal
CRE	Constitución de la República del Ecuador
LOGJCC	Ley Orgánica de Garantías Jurisdiccionales y Control Constitucional
LOPD	Ley Orgánica de Protección de Datos Personales del Ecuador
LOPDGDD	Ley Orgánica de Protección de Datos y Garantía de Derechos Digitales
RGPD	Reglamento General de Protección de Datos
TIC	Tecnologías de la Información y la Comunicación
TJUE	Tribunal de Justicia de la Unión Europea
UE	Unión Europea
WT29	Grupo de Trabajo del artículo 29

1. Introducción

En las sociedades actuales, que se ha dado en llamarlas sociedades de la información o del conocimiento, es imprescindible el flujo de la información de toda índole, incluso aquella catalogada como información personal, es decir, aquella que identifica a una persona física o la vuelve identificable.

En el contexto indicado, los derechos y libertades de las personas físicas, corren grave riesgo, de no mediar la implementación de mecanismos que protejan los datos personales para conciliar la necesidad de propender al flujo de la información, en las condiciones más seguras para tales derechos, con la protección de los derechos y libertades de sus titulares.

Las tecnologías de la información y la comunicación (en adelante TIC), han promovido el mejoramiento de la calidad de vida del ser humano; la posibilidad de comunicarse de una persona con otra ubicada en cualquier lugar del Mundo, por alejado o remoto que sea su lugar de residencia es, sin duda, una de las ventajas de estas tecnologías.

Con los beneficios anotados en relación a las nuevas tecnologías, llegan también riesgos que están representados por la migración a entornos virtuales de conductas delictivas que se manifiestan en entornos tradicionales. Entre tales conductas podemos mencionar, delitos contra la propiedad, tráfico de narcóticos y de personas, pornografía infantil y, desde luego el uso no autorizado de los datos personales en vulneración de los derechos y libertades de sus titulares.

Las redes sociales, como servicios de la sociedad de la información, han tenido una entusiasta recepción en todos los estratos sociales y son parte esencial en la forma en la que se relacionan las personas, esto tiene una relevancia especial cuando se involucran menores de edad que son, como se los reconoce, nativos digitales.

En Ecuador existen aproximadamente 14 millones de personas con conexión a Internet, de las cuales alrededor del 90% utiliza tal conexión para el intercambio de información mediante redes sociales y la mayoría de esos usuarios son jóvenes (hasta 29 años de edad), y un considerable porcentaje de ellos son menores de edad. Con lo anteriormente expresado como premisa, es evidente que el entorno virtual se vuelve una

amenaza para una población especialmente vulnerable que, en tal virtud, demanda de protección especial.

Mediante la presente investigación, nos proponemos exponer las particularidades que son propias del uso de las TIC, y el marco normativo que ha sido diseñado para precautelar, en la mayor medida posible el derecho a la protección de datos personales, como forma de precautelar los derechos y libertades de los ciudadanos.

Finalmente, debemos indicar que pretendemos abordar la temática del uso de las redes sociales y las condiciones que se deben establecer para hacerlo de manera segura, con particular referencia a la realidad ecuatoriana, que recientemente ha empezado a bosquejar las herramientas para alcanzar dicho objetivo.

2. Marco teórico y desarrollo

2.1. Protección de datos

2.1.1. Datos e información

Dato es todo dígito, letra, color, situación de hecho, que tiene un escaso contenido comunicacional, es decir, no tiene un significado unívoco. Los datos deben ser procesados, de lo contrario no servirían para nada más que para ser parte de la contaminación informativa. Es el proceso que al darle significado a los datos, los convierten en información que teniendo las características de exactitud, dirección y oportunidad, va a servir de base para el proceso de tomar decisiones, fin último de la información.

De lo anterior, inferimos que la información se deriva del procesamiento de los datos; tal procesamiento, que debemos entenderlo como tratamiento y, por tal, de acuerdo a lo establecido en el art. 4.2 del *Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE Reglamento General de Protección de Datos* (en adelante RGPD) y en el art. 4 de la *Ley Orgánica de Protección de Datos del Ecuador* (en adelante LOPD), en relación a los datos personales, debemos concebirlo como:

«Tratamiento: Cualquier operación o conjunto de operaciones realizadas sobre datos personales, ya sea por procedimientos técnicos de carácter automatizado, parcialmente

automatizado o no automatizado, tales como: la recogida, recopilación, obtención, registro, organización, estructuración, conservación, custodia, adaptación, modificación, eliminación, indexación, extracción, consulta, elaboración, utilización, posesión, aprovechamiento, distribución, cesión, comunicación o transferencia, o cualquier otra forma de habilitación de acceso, cotejo, interconexión, limitación, supresión, destrucción y, en general, cualquier uso de datos personales» (ASAMBLEA NACIONAL, 2021).

Una vez que los datos personales hayan sido sometidos a tratamiento y, como consecuencia de tal tratamiento, se ha obtenido información, como parte del cumplimiento de los fines declarados por parte del responsable del tratamiento, se deberá poner a disposición de quien deberá tomar una decisión en virtud de la información obtenida, esto es, se deberá entregar la información resultante al destinatario de la misma.

Es de extrema importancia destacar, que no cualquier resultado del procesamiento de datos deriva en información, para que esta se produzca, el tratamiento de los datos debe tener como resultado un producto que sea concordante con el objetivo general de la información, es decir, la toma de decisiones. Por lo tanto, tal resultado debe ser exacto, estar dirigido a quien debe tomar las decisiones y entregado en el momento en el que se puedan tomarlas; solo así se podrá calificar como información al resultado del procesamiento de datos.

De otro lado, debemos también indicar que el tratamiento de los datos, les da significado, lo que finalmente es lo que convierte en información los datos que originalmente tenían poco contenido comunicacional. Una letra, un dígito, un color, un hecho, color de ojos, número IP, dirección de correo electrónico, etc., tienen poco contenido comunicacional por si solos, pero cuando tras el procesamiento al que se los somete, se les atribuye un significado, eso es lo que convierte a los datos en información, *v.gr.*, el color verde, por si solo, puede tener variados significados, dependiendo de las personas que lo vean, tal ambigüedad es propia de los datos no procesados, pero si a dicho color se lo incorpora a un dispositivo de ordenamiento del tránsito vehicular (semáforo), dicho color adquiere un significado único que permite a los conductores y peatones, tomar decisiones adecuadas.

2.1.2. Datos personales

Dentro del género datos, se encuentran los denominados datos personales, podemos decir que estos están definidos por la posibilidad que, mediante ellos, se identifique a una persona física o que la haga identificable.

El art. 4.1 del RGPD, define los datos personales expresando:

«Toda la información sobre una persona física identificada o identificable y (el interesado); se considerará persona física identificable toda persona cuya identidad pueda determinarse, directa o indirectamente, en particular mediante un identificador, como por ejemplo un nombre, un número de identificación, datos de localización, un identificador en línea o uno o varios elementos propios de la identidad física, fisiológica, genética, psíquica, económica, cultural o social de dicha persona» (PARLAMENTO EUROPEO, CONSEJO DE LA UNIÓN EUROPEA, 2016).

El Grupo de Trabajo del artículo 29 (en adelante WT29) realiza en su dictamen 4/2007 un detallado análisis del concepto de datos personales, a partir de la definición propuesta en el art. 5 de la Directiva 95/46/CE de Protección de Datos, derogada por el RGPD. Entre los elementos que incorpora a partir de la definición que proporciona la Directiva, establece que dato personal es todo aquel relativo a personas físicas, debe entenderse, por lo tanto, que las personas jurídicas están excluidas de la definición, así como las personas fallecidas y las no nacidas. Como consecuencia de lo anterior, la lógica inferencia a la que se llega, es que los datos de las personas jurídicas, las fallecidas y las correspondientes a las no nacidas, no están incluidas en el ámbito de protección de las normas relacionadas a los datos personales, mas sin embargo, eso no implica que no puedan protegerse por otras disposiciones legales, tales como la penal o la civil, por mencionar solo esas. Al respecto, ROMEO (2021, p. 575) expresa:

«La definición de datos personales permite incluir toda la información que se refiere a una persona física individual, cualquiera que sea la naturaleza u origen de aquella, sea íntima o no, incluso aunque afecte a varias personas al mismo tiempo o a un grupo familiar (en este último caso, cada uno de los miembros individuales de la familia), aspecto que puede ser de gran trascendencia para los datos relativos a la intimidad, al honor, a la propia imagen, a la salud, a los datos biométricos y en particular los datos genéticos, que con el RGPD

gozan explícitamente del carácter de datos personales, siempre que la persona de la que provienen esté identificada o sea identificable».

Es importante destacar la adjetivación que realiza la definición en relación a la personas físicas, cuyos datos personales son objeto de protección normativa; según el art. 4.1 del RGPD, tales personas deben ser identificadas o identificables. En el primer caso, una persona es identificada, cuando mediante características físicas, fisiológicas, biométricas, genéticas o de otras de similar naturaleza, se pueda determinar su identidad, esto es, se refiere de manera general a los datos personales identificativos (nombre, apellido, número de documento de identidad, etc.); mientras que será identificable, cuando los datos antes indicados, se hallen disociados de cualquier persona, es decir, de sus datos identificativos y, mediante el empleo de mecanismos técnicos, se puede establecer la relación entre esos datos y las personas a las que pertenecen, sin que ello involucre esfuerzos desproporcionados, desde el punto de visto técnico y económico.

A parte de lo expresado, nos parece trascendente que se exprese nuestra disidencia con la sinonimia que se sugiere alrededor de los conceptos de datos frente a la información. A nuestro entender, no se puede establecer la pretendida sinonimia, pues información solo tendremos luego que se hayan sometido a tratamiento los datos, con lo que adquirirían significado o ha permitido la identificación de una persona, si se trata de datos relativos a personas físicas, en cuyo caso tendremos datos personales.

2.1.3. Derecho a la protección de datos personales

El actual reconocimiento de la protección de datos personales, como un derecho fundamental, es relativamente reciente, como recientes son las amenazas a los datos personales, que hicieron necesaria la articulación de un medio para protegerlos. La principal de las amenazas a los datos personales, llegan de la mano de la aparición de las TIC; la posibilidad de someter a procesamiento (tratamiento) grandes volúmenes de datos personales, a muy altas velocidades y -a partir de la información resultante- que sirvan para tomar lo que puede considerarse decisiones automatizadas, es lo que constituye la más grande amenaza al derecho a la protección de datos personales y a otros no pocos derechos del mismo rango, tales como: intimidad, privacidad, buen nombre, reputación, entre otros.

Largo es el camino que se ha recorrido desde la aprobación de la Declaración Universal de los Derechos Humanos, el 10 de diciembre de 1948, hasta el RGPD en Europa y la LOPD en Ecuador. En ese camino se ha tenido que establecer la necesidad de protección de los datos personales como mecanismo de asegurar otros derechos relacionados; no hablamos de un derecho instrumental, pues el derecho a la protección de datos es autónomo, sino que son derechos relacionados; la persona humana, cierto es, constituye una unidad, pero se manifiesta en múltiples dimensiones, de ahí que la protección de sus datos personales incida en los derechos y libertades que, como ser humano, estamos habilitados para ejercer.

En el sentido expuesto se pronuncia ÁLVAREZ (2020, p. 57) señalando:

«La evolución hasta el reconocimiento de la protección de datos personales como un derecho fundamental ha pivotado desde la consideración de este como una extensión del derecho a la intimidad o a la vida privada; pasando por su consideración como derecho autónomo hasta llegar a ser incorporado en la generación de derechos humanos desde finales del siglo pasado. Resulta evidente que la extraordinaria evolución tecnológica actual que permite tratar datos de forma masiva y automatizada hace que el derecho a la protección de datos personales adquiera una nueva dimensión muy alejada de las primeras referencias en la materia como, por ejemplo, el Convenio de Roma de 1950».

Inicialmente se consideró la protección de datos como un derecho subjetivo, cuya satisfacción quedaba en manos privadas, es decir, su observancia quedaba como responsabilidad de las personas al evitar involucrarse en información relativa a otra, sin que esta hubiera consentido en ello. Esta es precisamente la tesis sostenida por los abogados bostonianos Samuel Warren y Louis Brandeis, cuando en 1890 escribieran en la Harvard Law Review, su famoso artículo *The Right to Privacy*, en el que propusieron el derecho a ser dejado en paz (*Right to be let alone*), que se entiende como el derecho que tenemos los seres humanos a excluir del conocimiento de la información relacionada a nuestra vida privada a todos aquellos que consideremos que no deben tener acceso a ella, se trata en esencia de un derecho de exclusión.

Desde la consideración de la protección de datos personales, por parte de Warren y Brandeis, como algo que se podría imponer a los particulares, llegamos a la teoría de la

libertad informativa, estructura por el Tribunal Constitucional alemán, donde se estableció, frente a la ley del censo aprobada en el año 1982, que la protección de datos es el derecho de todas las personas a oponerse a las intromisiones que cualquier entidad, pública o privada, física o jurídica, pretenda ejercer y el Estado está llamado a precautelar el pleno ejercicio de tal derecho al ser considerado, desde ese momento, un derecho subjetivo público.

Desde la *Declaración Universal de los Derechos Humanos*, del 10 de diciembre de 1948 en la que se incluyó, en su art. 12, la directa mención a la prohibición dirigida a todos los que no cuenten con la anuencia del titular de los datos personales, a entrometerse en la vida privada de otros, pasando por la Convención para la Protección de los Derechos Humanos y Libertades Fundamentales, que en su art. 8 reitera que ni aun la autoridad pública puede interferir en el pleno ejercicio del derecho a la vida privada y familiar, sin la habilitación legal respectiva, lo que también está incluido en el Pacto Internacional de los Derechos Civiles y Políticos del 19 de diciembre de 1996.

Tras el recorrido convencional indicado, fue Suecia el país que aprobó la primera ley nacional de protección de datos en 1973, lo que fue seguido, en los años siguientes, por Alemania, Francia, Países Bajos y Reino Unido.

Debemos reiterar que la principal amenaza al derecho a la protección de datos, llegó con el advenimiento de las TIC. La posibilidad de procesar grandes volúmenes de datos y gran velocidad, supuso una vulneración sin precedentes a los derechos y libertades de las personas físicas como nunca antes se había visto. Por tal motivo, ya en la Constitución española de 1978, se incluyó en su art. 18.4 el derecho a la autodeterminación informativa: «4. La ley limitará el uso de la informática para garantizar el honor y la intimidad personal y familiar de los ciudadanos y el pleno ejercicio de sus derechos» (CORTES GENERALES, 1978). La visión del constituyente español fue pionera en relación a identificar, a nivel constitucional, el peligro que entraña para los derechos y libertades de los interesados, la aplicación de las nuevas tecnologías en el tratamiento de los datos personales.

La amenaza del tratamiento automatizado de los datos personales a los derechos y libertades de las personas físicas, fue el impulso que llevó a la aprobación, el 28 de enero

de 1981[1], del Convenio # 108 del Consejo de Europa para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal. ÁLVAREZ (2020, p. 59) expresa sobre este Convenio:

«El Convenio 108, en su origen, definía el marco de protección de la privacidad en relación con las tecnologías de la información y la comunicación. Dicho convenio surgió para desarrollar la protección de los derechos fundamentales de las personas en relación con el uso de la Informática, y fijar las bases para una legislación internacional que permitirá compatibilizar el flujo internacional de datos con la privacidad del individuo. En su artículo 2 aporta las definiciones básicas de «datos de carácter personal», «fichero automatizado», «tratamiento automatizado» y «autoridad controladora del fichero» (lo que hoy conocemos como «responsable del fichero»)».

El 24 de octubre de 1995, el Parlamento Europeo y el Consejo, aprobaron la Directiva 95/46/CE relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de los datos. Esta Directiva significó un punto de equilibrio entre la protección de los derechos y libertades de los titulares de los datos personales y la necesidad de generar la circulación de dichos datos en el marco del libre comercio, que el esfuerzo de integración que supone la Unión Europea demanda; mas sin embargo, al requerir de legislaciones nacionales de transposición de dicha Directiva[2], provocó la aparición de visiones distintas en materia de protección de datos, que lejos de facilitar y garantizar tal protección, supuso el impedimento de unificación de las políticas regionales de protección de datos.

Precisamente, como consecuencia de la disparidad de visiones sobre la aplicación la protección de datos personales establecidos en las leyes nacionales de transposición de la Directiva 95/46/CE del 24 de octubre del Parlamento Europeo y el Consejo, se hizo necesaria la aprobación de una norma que supusiese la unificación de los mecanismos de

[1] Precisamente por ser ese día en el que se aprobó este Convenio, en Europa se celebra en esa fecha el día internacional de la protección de datos personales.
[2] La transposición de la Directiva 95/46/CE en los Estados miembros ocurrió el 24 de octubre de 1998, en España se aprobó la Ley Orgánica 15/1999, de 13 de diciembre de Protección de Datos de Carácter Personal y su Reglamento de desarrollo.

protección y que fuera de directa aplicación en los países de la Comunidad Europea. Con tales antecedentes se aprobó el RGPD.

Debemos mencionar en este breve análisis del derecho a la protección de datos y de la legislación que inicialmente la posibilitó, el criterio emitido por el Tribunal Constitucional español, en su sentencia 292/2000 de 30 de noviembre de 2000, cuando al referirse a este derecho, adjetivándolo como fundamental, lo define expresando:

«(…) resulta que el contenido del derecho fundamental a la protección de datos consiste en un poder de disposición y de control sobre los datos personales que faculta a la persona para decidir cuáles de esos datos proporciona a un tercero, sea el Estado o un particular, o cuáles puede este tercero recabar, y que también permite al individuo saber quién posee sus datos personales y para qué, pudiendo oponerse a esa posesión o uso» (TRIBUNAL CONSTITUCIONAL, 2000).

En relación al Ecuador, en la CRE, se incluyó entre los derechos de libertad, el derecho a la protección de datos personales, lo hace en el art. 66.19, que analizaremos *infra*. Tras trece años de aprobada la Constitución que rige en el país, se aprobó la LOPD, la que se encuentra vigente desde su promulgación en el Suplemento del Registro Oficial # 459 del 26 de mayo del 2021.

Finalmente, en relación al derecho a la protección de datos personales, debemos distinguir elementos objetivos y subjetivos.

2.1.3.1. Elementos objetivos en la protección de datos

Son elementos objetivos en la protección de datos personales, tal como lo hemos expresado anteriormente, los datos relativos a personas físicas, desde su nacimiento hasta su muerte. También lo indicamos previamente, que podrían considerarse datos personales, aquellos relacionados a personas fallecidas, pero como también sabemos, las personas que son sujetos de derechos, es decir, con personalidad jurídica, son solo aquellas personas que han nacido y hasta su fallecimiento. Si bien es cierto, que las personas jurídicas tienen personalidad jurídica, no se les reconoce el derecho a la privacidad o a la intimidad, base fundamental de la protección de los datos personales.

También indicamos *supra*, que son datos personales aquellos aptos para identificar a una personas, tales como sus datos identificativos, esto es, su nombre, apellido, DNI; también son datos personales, aquellos que permiten la identificación de una persona, es decir, datos que inicialmente, de forma aislada no permiten tal identificación, pero que asociados a otros, la posibilitan. Entre los datos que permiten la identificación de una persona física, podemos mencionar: dirección domiciliaria, número IP, huella dactilar, ADN, etc.

2.1.3.2. Elementos subjetivos en la protección de datos personales

Entre los elementos subjetivos en la protección de datos personales, podemos identificar los siguientes:

a) **Interesado**: Esta es la persona física identificada mediante los datos o a quién se puede identificar con ellos. Es el titular del derecho fundamental a la protección de datos, a la que se pretende proteger en sus derechos y libertades, cuyos datos son sometidos a tratamiento.

b) **Responsable del tratamiento:** Esta es la persona física o jurídica quien establece los fines del tratamiento y los medios que han de emplearse para cumplir con los mismos. Si existen varias personas que tienen esa potestad, se los ha de reconocer como corresponsables. Sea cual fuere el caso, asume las consecuencias del incumplimiento de las obligaciones que se le atribuyen, así como también deben garantizar el ejercicio de los derechos de los interesados.

c) **Encargado del tratamiento:** Es la persona física o jurídica que asume, por cuenta del responsable, el tratamiento de los datos personales. El tratamiento que asume, debe ser realizado siguiendo las disposiciones del responsable y, entre ellos, debe existir una relación jurídica evidenciada en un contrato que cumpla con las exigencias que la normativa establezca.

d) **Tercero:** Si en el tratamiento de los datos personales, una persona física o jurídica, no decide sobre los fines del tratamiento y los medios que han de emplearse en el mismo, ni realiza el tratamiento por cuenta de quien resuelve sobre fines y medios del tratamiento, se puede calificar a esa persona como tercero. El tercero puede intervenir

en el tratamiento, pero sin establecer fines y medios del tratamiento, puede hacerlo por delegación del encargado (en tanto el primero haya recibido habilitación por parte del responsable para tal delegación).

e) **Destinatario:** Es la persona física o jurídica quien puede tomar decisiones basadas en la información resultante del tratamiento de los datos. El art. 4.9 del RGPD define al destinatario como: «la persona física o jurídica, autoridad pública, servicio u otro organismo al que se comunique datos personales, se trata o no de un tercero (…)». Debemos entender que la comunicación a la que se refiere la definición del RGPD, debe haber sido hecho de manera lícita, es decir, en función del tratamiento a la que se sometieron los datos personales, se debían entregar o comunicar el resultado del tratamiento a esa persona física o jurídica para que pueda hacer uso de la información resultante.

2.1.3.3. Principios en la protección de datos personales

Para que el responsable pueda realizar el tratamiento de los datos personales, luego de haber establecido los fines y los medios para dicho tratamiento, debe realizar el tratamiento cumpliendo con los principios que, por tales, se tornan en obligaciones a observar en todo el tiempo que requiere su realización. Tales principios son:

a) **Licitud, lealtad y transaparencia:** Para que el tratamiento de datos personales sea lícito, debe estar basado en una de las bases legitimadoras establecidas en los arts. 6 y 9 del RGPD. Será leal en la medida que dicho tratamiento cumpla con los fines establecidos previamente al tratamiento y, transparente, cuando se cumpla con informar al interesado sobre dichos fines y, a más de informarle sobre los fines, debe informarle los derechos que puede ejercer y la forma de ejercerlos.

b) **Limitación a la finalidad** El responsable del tratamiento de los datos personales, debe atenerse a la finalidad declarada, para establecer la base legitimadora y durante todo el tiempo que dura el tratamiento. Podrá sin embargo, haber otra finalidad distinta de la inicialmente declarada, en la medida que tenga relación con la primera.

c) **Minimización de datos personales:** Establecidos los fines del tratamiento, el responsable solo recabará los datos personales que sean estrictamente necesarios para dichos fines.

d) **Limitación al plazo de conservación:** Los datos personales, se deberán conservar, por parte del responsable del tratamiento, únicamente durante el tiempo que se requiera para cumplir con la finalidad declarada, al cumplirse el tiempo que el tratamiento demande, se deberán eliminar los datos o, por lo menos, disociarlos (anonimizarlos), de manera que se desconecten los datos identificativos del interesado del resto de los datos, de suerte que se haga imposible, desde el punto de vista técnico, revertir la anonimización.

e) **Calidad de datos personales:** El responsable del tratamiento debe ser capaz de asegurar la calidad de los datos personales, lo cual implica que se realice la actualización o corrección respectivas, todo en la medida de sus posibilidades, de forma que no se afecten los derechos y libertades de los interesados.

f) **Integridad y confidencialidad:** El responsable del tratamiento debe asegurar que los datos no sean alterados accidental o intencionalmente durante todo el tiempo que dure el tratamiento. De igual manera, debe asegurar que nadie ajeno al tratamiento tenga acceso a los datos personales. El responsable debe implementar medidas técnicas y organizativas, para el cumplimiento de las obligaciones indicadas. Las medidas que implemente, deben ser producto del análisis de riesgo que, previamente al tratamiento de los datos personales, se haya realizado, donde se identifiquen las amenazas, la probabilidad de ocurrencia de las mismas, así como el impacto sobre los derechos y libertades de los interesados en caso de ocurrencia. Una vez establecido el riesgo inherente, si este resulta elevando, se deberá realizada una evaluación de impacto sobre los datos e implementar las salvaguardas o medidas de seguridad en función del riesgo identificado hasta reducirlo al mínimo, es decir, hasta alcanzar un nivel de riesgo que se pueda calificar de tolerable o residual.

g) **Responsabilidad proactiva:** El responsable del tratamiento debe implementar todas las medidas técnicas y organizativas para garantizar los derechos y libertades de los interesados en el tratamiento de sus datos personales. Para tal efecto debe ser capaz

de justificar ante la autoridad de control, el cumplimiento de sus obligaciones. Este principio es conocido en la doctrina de protección de datos como *accountabilty*, que permitió pasar de una actitud reactiva, de parte de los responsables, a una preventiva, donde se anticipe las amenazas a las que puedan estar expuestos los datos personales y establezca las medidas de seguridad adecuadas al riesgo.

2.1.3.4. Bases legitimadoras para el tratamiento de los datos personales.

El tratamiento de datos personales, solo será posible a partir de su fundamentación en una de las bases legitimadoras, lo que además sustenta el principio de licitud, previamente mencionado. Tales bases legitimadoras son:

a) **El consentimiento:** Podemos afirmar que el consentimiento es una manifestación de la voluntad mediante la cual se acepta un acto jurídico determinado. En relación a la protección de datos, el interesado debe asentir que sus datos sean sometidos a tratamiento, de manera que el responsable sea habilitado para hacerlo directamente o mediante el concurso del encargado. El consentimiento para que sea válido, debe ser informado, esto es, el responsable debe transparentar los fines del tratamiento, la categoría de datos que serán sometidos al mismo, el tiempo que se conservarán, incluso se deberá informar, si estos serán objeto de transferencia internacional. El consentimiento debe ser específico, es decir, relacionado a la o las finalidades declaradas por el responsable; debe ser inequívoco, vale decir, que no quepa la menor duda de su otorgamiento, se excluye en consecuencia el consentimiento tácito, el interesado debe realizar, por lo menos, una acción afirmativa que no deje dudas de su anuencia en relación al tratamiento pretendido de sus datos; el consentimiento debe ser revocable, con la misma facilidad con la que se haya otorgado el consentimiento, se lo debe poder revocar. Debemos también expresar que, como los menores edad, no están habilitados legalmente para expresar válidamente su consentimiento[3], lo deberán hacer sus padres o tutores legales por ellos.

[3] En el RGPD se establece como edad mínima para expresar el consentimiento 16 años, pero habilita para que los países miembros de la Unión Europea, puedan establecer una edad inferior para tales efectos, España

b) **El tratamiento es necesario para la ejecución de un contrato**: El responsable puede proceder con el tratamiento de los datos personales, aun cuando el interesado no haya prestado su consentimiento, cuando dicho tratamiento sea necesario para la ejecución de un contrato en el que el interesado esté involucrado o cuando él haya dado orientaciones expresas en discusiones realizadas en fase pre contractual. Tal caso podría presentarse, por ejemplo, cuando el interesado sea parte en la firma de un contrato de compra venta y, para su celebración, se requiere incorporar información económica que esté relacionada con él.

c) **El tratamiento es necesario para el cumplimiento de una obligación legal:** Tal caso podría ocurrir en un centro educativo, esto es, se estaría cumpliendo con la satisfacción del derecho a la educación que, como sabemos es una obligación en la mayoría de los países en beneficio de sus nacionales. No solo el Estado, cumpliendo con sus obligaciones constitucionales, estaría habilitado para el tratamiento fundamentado en esta base legitimadora, piénsese en un empleador que debe entregar información de los ingresos de sus trabajadores a la administración tributaria, en cumplimiento de sus obligaciones como agente de retención en el pago de tributos sobre la renta.

d) **El tratamiento es necesario para proteger intereses vitales del interesado:** Esta base legitimadora, se hizo evidente en la presente época de pandemia, cuando la información relativa a la salud de la población, era captada en lugares públicos, con el objetivo de realizar labores de control epidemiológico, en tal caso se protege los intereses vitales (salud y la vida) no solo del titular de los datos, sino de quienes tienen o hayan tenido contacto con él.

e) **El tratamiento es necesario para el cumplimiento de una misión en interés público:** Siendo el interés público un concepto jurídico indeterminado, solo puede entenderse esta base legitimadora para el tratamiento de los datos personales, aceptando que todo acto realizado por el Estado, en cualquiera de sus niveles, es

lo ha hecho, incorporado en su ley 3/2018 LOPDGDD una edad mínima de 14 años. En Ecuador, la LOPD establece en su art. 21 que los menores de edad, desde los 15 años, podrán otorgar, en calidad de titulares, su consentimiento explícito para el tratamiento de sus datos personales, siempre que se les especifique con claridad sus fines.

de interés público (o debe serlo) y, por lo tanto, el tratamiento de los datos es inoponible con relación a las entidades públicas.

f) **Interés legítimo:** Para que el responsable pueda fundamentar el tratamiento de los datos personales en esta base legitimadora, sus intereses deben prevalecer sobre los derechos de los interesados. Tal prevalencia debe ser derivada de un juicio de proporcionalidad o ponderación, en el que se determine que el nivel de afectación de los derechos y libertades de los interesados, se justifican en el nivel de satisfacción de los intereses del responsable o de terceros. Es importante destacar, que basados en el RGPD, ninguna entidad pública, puede invocar esta base legitimadora para el tratamiento de datos personales. Relievamos que en Ecuador, no existe impedimento alguno para que una entidad pública emplee esta base legitimadora en el tratamiento de los datos personales.

2.1.3.5. Derechos de los interesados

Ha quedado claro, en este punto, que la protección de datos es un derecho fundamental cuyo ejercicio el Estado está llamado a garantizar en beneficio de todos los ciudadanos. Es en ese sentido que al interesado, como titular de los datos personales que se someten a tratamiento, se le reconocen derechos que deben ser observados prolijamente por los responsables y encargados del tratamiento. De más está decir, que ningún derecho es absoluto, por lo que al ejercerlos se deberá fundamentar adecuadamente la petición, de forma que puede ocurrir que atentas las circunstancias, la petición de ejercicio de un derecho no sea atendida por el responsable ni por la autoridad de control pertinente, por falta de dicha fundamentación o por su defectuosa estructura.

a) **Derecho de acceso**: El interesado tiene el derecho de acceder a los datos que se estén procesando, el responsable tiene la obligación de confirmarle el tratamiento al que se están sometiendo los datos personales, las finalidades que persigue, el plazo de conservación, si acaso es posible su determinación o, de lo contrario, el criterio que implementará para la conservación de los datos personales. De igual forma, debe permitirle el acceso a la identificación de los destinatarios de los datos y si estos serán objeto de transferencias internacionales.

b) Derecho de rectificación: Debemos recordar que los responsables del tratamiento de los datos personales, están obligados a asegurar la calidad de los datos, es decir, en la medida de lo posible, tales datos deben reflejar la realidad de los interesados. Si los datos personales no reflejan la realidad del interesado, este puede ejercer su derecho de rectificación, en cuyo caso, el responsable debe realizar todas las acciones técnicas que estén a su alcance para actualizar los datos, todo para garantizar los derechos y libertades de los interesados.

c) Derecho de supresión (eliminación): El tratamiento de los datos, debe estar en todo momento sometido a la finalidad que los responsables declararon al inicio del tratamiento o, si esta es cambiada, debe estar relacionada con la inicial. De igual forma, el tratamiento debe ser realizado respetando el plazo de conservación establecido o el criterio para su determinación. Si no se respetan los parámetros indicados, los interesados pueden ejercer su derecho de supresión o eliminación ante el responsable. Importante es destacar que, no necesariamente deberán eliminarse los datos personales de los interesados cuya finalidad se ha cumplido o el plazo de conservación se haya alcanzado; los datos en tales casos, podrían ser anonimizados, es decir, que los datos identificativos se separen de los demás datos, de suerte que no se pueda identificar a una persona física a partir de esos datos. Para cumplir con una finalidad de estudios estadísticos, científicos o históricos, se pueden conservar los datos personales más allá del cumplimiento de la finalidad declarada o del plazo de conservación establecido, pero deben aplicarse precisamente las técnicas de anonimización antes indicadas, para respetar los derechos de los interesados. Finalmente debemos destacar que este derecho, igual que todos los demás, no es absoluto, pues su ejercicio irrestricto depende de la base legitimadora del tratamiento, si esta se basa en el consentimiento, solo basta con revocarlo para que se convierta en una obligación del responsable, pero si no es el caso, el interesado deberá motivar adecuadamente el ejercicio de su derecho de supresión, sin lo cual el responsable estará habilitado para negarlo.

d) Derecho al olvido: Intimamente relacionado al derecho identificado *supra*, concebido para que el interesado o titular de los datos personales, exija del responsable la supresión de los mecanismos de localización de su información que

se encuentre en Internet. Es por tal razón que se lo considera un refuerzo del derecho de supresión.

e) Derecho de oposición: Los interesados pueden oponerse a todo tratamiento que no esté fundamentado en un base legitimadora o se desvíe de la finalidad declarada al iniciar el tratamiento o haya cumplido el periodo de conservación.

f) Derecho de portabilidad: Este derecho habilita al interesado para solicitar que sus datos sean entregados a otro responsable que asumirá, por su expresa voluntad el tratamiento de sus datos. Al respecto APARICIO, VIDAL (2019, p. 235) sostienen:

«Básicamente, la portabilidad atribuye al interesado el derecho a disponer de la información sometida a tratamiento para su reutilización en otro entorno diferente. De esta forma, el propio interesado o el tercero a quien este facilite los datos, u ordene que se le transfieran directamente, podrán utilizar los datos tratados inicialmente por el responsable para cualquier uso que le interese al dueño de la información, ya sea para recibir un servicio de valor añadido sobre los mismos datos, para su análisis y utilización para cualquier propósito que secunde el interesado, o para sustituir al responsable del tratamiento».

g) **Derecho a no ser objeto de decisiones automatizadas, incluida la elaboración de perfiles**: Cuando en un entorno en el que se producen una enorme cantidad de datos, derivados en gran medida por la implementación de técnicas disruptivas, tales como el Internet de las cosas (*Internet of Things* - IoT), se implementan mecanismos de análisis masivos de datos que permiten tomar decisiones basadas en dichas técnicas, *v,gr*, con el uso del *Big Data*, puede ocurrir que, por masivas e impersonales, afecten los derechos y libertades de los interesados. En consecuencia, si se va a realizar ese tipo de tratamiento[4], en primer lugar se debe informar a los interesados y, en segundo lugar, se deben implementar medidas de seguridad suficientes y adecuadas al riesgo que llevan implícitas esas técnicas, de

[4] En ocasiones, el perfilado de los interesados, es inoponible frente al interés legitimo que puede argüirse por parte de los responsables del tratamiento de datos personales, como cuando se trata de mercadotecnia directa, en la medida que tal interés legitimo haya sido precedido del respectivo juicio de proporcionalidad, que establezca que, para el caso concreto, se justifica el perfilado de los interesados y que el nivel de afectación de sus derechos y libertades, está justificado en función de tal análisis previo.

manera de asegurar, en la mayor medida posible, que el tratamiento de los datos personales, no se realizará en vulneración de los derechos de los interesados.

2.1.3.6. Perspectivas de la protección de datos en Ecuador

En la Constitución aprobada por la Asamblea Constituyente en el 2008 y que actualmente rige en Ecuador, se estableció como un derecho fundamental, la protección de datos personales, se lo hizo en el art. 66.19:

«Se reconoce y garantizará a las personas: (…) 19. El derecho a la protección de datos de carácter personal, que incluye el acceso y la decisión sobre información y datos de este carácter, así como su correspondiente protección. La recolección, archivo, procesamiento, distribución o difusión de estos datos o información requerirán la autorización del titular o el mandato de la ley» (ASAMBLEA CONSTITUYENTE, 2008).

La norma constitucional ecuatoriana describe el contenido del derecho a la protección de datos, establece en definitiva que el tratamiento, es decir, la recolección, archivo, procesamiento, distribución o difusión de los datos, requieren una base legitimadora, menciona concretamente, como tales, el consentimiento o el mandato de la ley, lo que justamente podemos reconocer como el contenido del fundamento de la licitud del tratamiento, uno de los pilares del tratamiento de los datos personales, tal como se mencionó en líneas previas.

El art. 11.3 de la propia Carta Fundamental ecuatoriana establece que los derechos y garantías reconocidas en ella, son de directa e inmediata aplicación, esto es, no requieren de legislación secundaria, para su aplicación:

«El ejercicio de los derechos se regirá por los siguientes principios: […] 3. Los derechos y garantías establecidos en la Constitución y en los instrumentos internacionales de derechos humanos serán de directa e inmediata aplicación por y ante cualquier servidora o servidor público, administrativo o judicial, de oficio o a petición de parte» (ASAMBLEA CONSTITUYENTE, 2008).

Pese al expreso reconocimiento en la CRE del derecho fundamental a la protección de datos personales, el país nunca sintió que fuera necesario proteger los datos personales. Se hablaba de la información pública y el derecho a acceder a ella, frente a la que, con

frecuencia se ejerce la garantía jurisdiccional de acceso a la información pública, reconocido en el art. 91 CRE y en el art. 47 de la Ley Orgánica de Garantías Jurisdiccionales y Control Constitucional (en adelante LOGJCC) y del art. 22 de la Ley Orgánica de Transparencia y Acceso a la Información Pública. No fue sino hasta la enorme filtración de datos personales, hecho reconocido por parte de la autoridades nacionales el 16 de septiembre del 2019, que se tomó la iniciativa de proponer una ley al respecto. Los medios de comunicación nacionales, dieron cuenta del hecho y, como era lógico esperar, se produjo una enorme preocupación sobre el manejo de los datos personales en el país.

«La firma VPN Mentor reveló una de las peores noticias en cuanto privacidad se refiere en Ecuador. Halló una masiva filtración de datos de más de 20 millones de personas en un servidor no seguro ubicado en Miami, en Florida, de las cuales 6,7 millones corresponden a menores de edad. Un equipo dirigido por los investigadores Noam Rotem y Ran Locar descubrió la vulneración que puede incluir datos además de personas fallecidas. Según su reporte, la violación de datos involucra una gran cantidad de información sensible de identificación personal a nivel individual. La mayoría de las personas afectadas parecen estar ubicadas en Ecuador» (PLANV, 2019).

Tan solo días después de revelada la filtración masiva de los datos personales, esto es, el 19 de septiembre del 2019, el gobierno envió a la Asamblea Nacional, el Proyecto de LOPD, que finalmente fue aprobado el 26 de mayo del 2021, fecha en la que entró en vigencia tras su publicación en su Suplemento del Registro Oficial # 459 de dicha fecha, con lo que empezamos en firme la implementación de un sistema de protección de datos personales. Desde luego, tomará un tiempo hasta que la población tome conciencia sobre la necesidad de protección de sus datos personales y que se cree la institucionalidad necesaria para hacer realidad un sistema de protección de dichos datos. En la ley aprobada se prevé, en su primera disposición transitoria, una suerte de *vacatio legis*:

«Las disposiciones relacionadas con las medidas correctivas y el régimen sancionatorio entrarán en vigencia [sic] en dos años contados a partir de la publicación de esta ley en el Registro Oficial, en el transcurso de este tiempo los responsables y encargados del tratamiento de datos personales se adecuarán a los preceptos establecidos dentro de esas disposiciones, su reglamento de aplicación y demás normativa emitida por la Autoridad de

Protección de Datos Personales. El resto de disposiciones [sic] establecidas en esta ley entrarán en vigencia conforme se establece en la Disposición Final de esta Ley» (ASAMBLEA NACIONAL, 2021).

Hemos empezado tarde a sistematizar la protección de datos personales[5], pero lo hemos hecho al fin, de seguro no será un camino fácil de recorrer, desde el propio desconocimiento de los instrumentos de protección de parte de las autoridades nacionales, pero sin duda la aprobación de la ley es un importante paso en ese camino. Esperamos que durante la *vacatio legis*, se instrumenten mecanismos de difusión del contenido de la LOPD, muy en particular los derechos y las formas de ejercerlos.

2.2. Las redes sociales.

2.2.1. La Sociedad de la información

El efecto transformador que las TIC tienen en las sociedades actuales es innegable y se amplía a pasos agigantados. Podríamos afirmar sin ambages, que no existe un área en la que no incidan sobre la forma en la que los miembros de la comunidad global se comportan; no solo nos referimos a los nativos digitales[6], sino a todas las personas independientemente de su edad o condición económica.

La Sociedad de la información, es el término que reconoce la omnipresencia de las tecnologías disruptivas derivas de la aplicación de las TIC, en todos los ámbitos del desarrollo actual, RICO (2007, P. 72) expresa sobre la realidad inherente a la sociedad de la información el siguiente criterio:

«En este reciente y dinámico contexto conocido como sociedad de la información, localizamos como caracteres esenciales la bidireccionalidad de la información y la generalizada expansión de las tecnologías que permiten su tratamiento. De este modo, nos enfrentamos a un mundo donde todo interactúa y se retroalimenta, en el que la información cada vez emana de un número mayor de fuentes y se dirige a un público más

[5] Antes de aprobación de la LOPD, con lo que se pretende eliminar la dispersión normativa en materia de protección de datos, existían en el país más de doscientos normas jurídicas de distinto rango que se referían a los datos personales, sin contar entre ellas el *habeas data* como garantía jurisdiccional que, como tal reconoce el Art. 92 de la CRE.

[6] Es la denominación que se les atribuyen a quienes las tecnologías de la información y la comunicación, son naturales a su realidad, normalmente son los jóvenes a quienes se les reconoce tal actitud.

amplio y diverso. Naturalmente, la difusión de la información contenida en este caudaloso flujo va a provocar innumerables consecuencias en el ámbito de los derechos, libertades, actitudes y relaciones sociales. En concreto, y dado que le afecta de manera directa, no es de extrañar que las tecnologías informacionales y la sociedad que han creado afecten el alcance y contenido del derecho a la información».

De acuerdo al criterio doctrinal propuesto, la idea implícita en el concepto sociedad de la información, incluye el que aquellos que la integran, no se limiten a obtener información de forma pasiva, sino que sean actores de primera linea en su producción, esto es, no solo obtienen información, sino que también la generan. Una consecuencia de esta nueva realidad que constituye la sociedad de la información, es que los derechos y libertades de las personas, estén expuestos a riesgos sin precedentes y, en consecuencia, reclaman formas de protección que estén en condiciones de enfrentar los retos propios de la nueva realidad que impone su implementación.

En muchas ocasiones se establece una sinonimia entre sociedad de la información con sociedad del conocimiento. A nuestro entender, no existe tal sinonimia, podemos afirmar que el concepto de información se queda en la forma de interactuar con las tecnologías de la información y la comunicación, mientras que la sociedad del conocimiento, engloba el uso de las TIC en la generación del conocimiento, que pase necesariamente del procesamiento de los datos, a muy altas velocidades, que deriva en la obtención de información, a la producción de conocimiento, que lo entendemos como la información que una sociedad acumula sobre un determinado asunto. FLORES, SEGURA, SANCHEZ (2007), sobre el tema afirman:

«La diferencia entre sociedad de la información y sociedad del conocimiento no ha sido esclarecida por la mayor parte de los estudiosos del tema. Desde nuestra perspectiva la diferencia radica en la posibilidad de modificar el uso que se hace de las tecnologías de la información para que puedan impulsar la producción de conocimientos de investigación y vinculados a la producción».

Queda claramente establecido, a nuestro entender, que cuando nos referimos a la sociedad de la información, lo hacemos relacionando la intensa utilización de las tecnologías de la información y la comunicación; mientras que al hablar de la sociedad del

conocimiento, es una referencia a la consecuencia de la existencia de la primera en la producción de conocimiento.

2.2.2. Las redes sociales: definición

La transición de las tecnologías 1.0 a las 2.0 implicó el cambio en la conducta de los internautas, desde ser unos meros consumidores de información, a producirla; en palabras de TOMEO (2014, p. 4)

«El usuario intercambia contenidos, opina, forma grupos de referencia, ejerce amplio poder de influencia en los demás y genera nuevas relaciones interpersonales por medio de los vehículos y aplicaciones que facilita la propia web 2.0, o -como algunos prefieren llamarla- «la Web social». Una de las formas en las que se refleja esta nueva forma [sic] de interacción de los usuarios de Internet, lo constituyen las redes sociales».

Las redes sociales son un servicio de la llamada sociedad de la información; la Directiva 98/34/CE define en el art. 1.2 lo que debe entenderse por tal:

«A efectos de la presente Directiva, se entenderá por: […] 2) «servicio», todo servicio de la sociedad de la información, es decir, todo servicio prestado normalmente a cambio de una remuneración, a distancia, por vía electrónica y a petición individual de un destinatario de servicios».

Las redes sociales, ahora no cabe duda, nacieron para prestar un servicio, esto es, permitir a los usuarios intercambiar información, de la más variada naturaleza, entre quienes comparten intereses comunes, tales como: profesionales, políticos, científicos, lúdicos, deportivos, comerciales, etc. En consecuencia, sin mayor esfuerzo, caben en la definición que la Directiva proporciona sobre servicios de la sociedad de la información.

En la Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico, mediante la cual se incorpora al ordenamiento jurídico español la Directiva 2000/31/CE, del Parlamento Europeo y del Consejo, de 8 de junio, relativa a determinados aspectos de los servicios de la sociedad de la información, en particular, el comercio electrónico en el mercado interior (Directiva sobre el comercio electrónico), se establece en el apartado 2 de la exposición de motivos el siguiente criterio:

«Se acoge, en la Ley, un concepto amplio de servicios de la sociedad de la información, que engloba, además de la contratación de bienes y servicios por vía electrónica, el suministro de información por dicho medio (como el que efectúan los periódicos o revistas que pueden encontrarse en la red), las actividades de intermediación relativas a la provisión de acceso a la red, a la transmisión de datos por redes de telecomunicaciones, a la realización de copia temporal de las páginas de Internet solicitadas por los usuarios, al alojamiento en los propios servidores de información, servicios o aplicaciones facilitados por otros o a la provisión de instrumentos de búsqueda o de enlaces a otros sitios de Internet, así como cualquier otro servicio que se preste a petición individual de los usuarios (descarga de archivos de vídeo o audio...), siempre que represente una actividad económica para el prestador. Estos servicios son ofrecidos por los operadores de telecomunicaciones, los proveedores de acceso a Internet, los portales, los motores de búsqueda o cualquier otro sujeto que disponga de un sitio en Internet a través del que realice alguna de las actividades indicadas, incluido el comercio electrónico» (CONSEJO DE EUROPA, 2000).

Con la reiteración en la disposición legal española de transposición de la Directiva 2000/31/CE, queda claramente establecido que las redes sociales pueden y deben ser consideradas como un servicio de la sociedad de la información. ORTIZ (2010, p. 24) propone una definición de redes sociales, desde sus orígenes y objetivos, indicando:

«Podemos definir de manera amplia las redes sociales *on line* [sic] como aquellos servicios de la sociedad de la información que ofrecen a los usuarios una plataforma de comunicación a través de Internet para que estos generen un perfil con sus datos personales, facilitando la creación de redes en base a criterios comunes y permitiendo la conexión con otros usuarios y su interacción. De esta manera se crea el fenómeno viral cuya clave es la vinculación entre usuarios».

De los elementos reconocidos en la definición que se propone, podemos inferir que las redes sociales son inicialmente, un mecanismo de comunicación entre personas que comparten intereses o aficiones comunes, dicho elemento unificador se determina mediante el perfil o descripción que el usuario hace de si mismo al crear su cuenta en la red social.

En Ecuador, las redes sociales tienen una enorme penetración en todos los estratos sociales, uno de los ejes en el desarrollo del gobierno digital, lo constituye precisamente, el avance hacia la transformación digital y la implementación de herramientas digitales, entre las que se cuentan, sin lugar a dudas, las redes sociales. Es el Ministerio de Telecomunicaciones y Sociedad de la Información, el que resalta este hecho que se ha evidenciado aún más en época de pandemia, MINISTERIO DE TELECOMUNICACIONES (2021)

«Facebook, Twitter o Instagram son algunas de las redes sociales más reconocidas en el planeta y que une a millones de usuarios. En Ecuador, para muchas personas, su uso es algo normal como un mecanismo de informar e informarse. Como parte del acceso a las Tecnologías de la Información y Comunicación (TIC), el Ministerio de Telecomunicaciones y de la Sociedad de la Información, como ente rector del sector, implementa políticas públicas que permiten la masificación de estos servicios».

2.2.3. Clases de redes sociales.

El criterio de clasificación generalmente aceptado de las redes sociales, parte del elemento que convoca a sus usuarios al crear una cuenta en ellas. Así podemos reconocer tres tipos de redes sociales: Comunicacionales, especializadas y profesionales.

2.2.3.1 Redes sociales de comunicación.

Estas redes sociales están orientadas a establecer comunicación entre sus usuarios; por lo general, quienes usan este tipo de redes, en algún momento tuvieron algún tipo de relación y perdieron contacto, podemos citar a manera de ejemplo: compañeros de estudios, amigos de la infancia, compañeros de trabajo, etc. Entre las redes de este tipo más conocidas, podemos citar Facebook, Myspace, Wechat, Weibo[7].

2.2.3.2. Redes sociales especializadas.

Este tipo de redes se desarrollan a partir de temas puntuales, *v.gr.*, opiniones cortas sobre temas concretos de diversa índole, esto es, *microblogging*, tales como Twitter o

[7] WeChat y Weibo, son dos de las más populares redes sociales en China que, por el número de usuarios locales rivaliza con las muy famosas Facebook y Myspace.

Mastodon; a para encontrar parejas sentimentales: Meetic o Tinder; para compartir fotografías o videos, tales como Instagram o Tik Tok, etc.

2.2.3.3. Redes sociales profesionales.

Este tipo de redes sociales están orientadas a la búsqueda de empleo o para la realización de *networking*, es decir, el establecimiento de relaciones profesionales entre personas con perfil laboral similar. Entre las redes sociales de este tipo más utilizadas podemos citar a LinkedIn, Viadeo, Womenalia, entre otras.

2.2.4. Teoría de los seis grados separación.

Esta teoría sociológica, plantea que una persona puede contactar con cualquier otra en cualquier parte del Mundo, sobre todo si comparten intereses, contactando a sus conocidos, estos a su tiempo, a los suyos, los que constituirían un segundo nivel, los que a su vez, contactarían a sus conocidos, en otro nivel; de tal manera que alcanzando un sexto nivel se habría contactado con cualquier persona en el lugar en el que se encuentre.

Esta teoría fue propuesta por el escritor húngaro Frigyes Karinthy en 1930, en un cuento llamado *Chains* y, posteriormente recogida por el sociólogo Duncan Watts, en su libro "*Six degrees: The Science of Connected Ages*". Al respecto, LONDOÑO (2017) indica:

«Según Watts si cada persona conoce en promedio, entre amigos, familiares y compañeros de trabajo o escuela, a unas cien personas, y estos a su vez se relacionan con otros 100 (de segundo nivel), tenemos un network potencial de 10.000 que multiplicado por los 100 adicionales que conocen estos 10.000 llega a un millón (que ya están en tercer nivel) que por 100 más son 100.000.000 en un cuarto nivel, a 10.000.000.000 en un quinto nivel y a 1.000.000.000.000 en un sexto nivel. En seis pasos, y con las tecnologías disponibles, se podría enviar un mensaje a cualquier individuo del planeta».

Esta teoría tiene una gran incidencia en lo que respecta a las redes sociales, teniendo en mente que, el objetivo central de estos servicios de la sociedad de la información, es contactar a personas que manifiesten intereses comunes, tal como se expuso *supra.* De allí podemos entender el fenómeno de la viralización que provocan las publicaciones que realizan los usuarios de estas redes y sus efectos en quienes son mencionados en ellas.

Finalmente, si consideramos que la teoría de los seis grados de separación, fue propuesta en 1930, cuando las tecnologías de la información y la comunicación, no se habían desarrollado como lo están ahora, podemos concluir que en la actualidad, no se requieren seis niveles para contactar a una persona en el lugar en el que se encuentre, de seguro tal objetivo sería alcanzado con muchos menos «saltos». LONDOÑO (2017) lo reitera:

«Nuestros «grados de separación» colectivos se han reducido en los últimos cinco años. En 2011, los investigadores de Cornell, la Università degli Studi di Milano, y Facebook calcularon el promedio de los 721 millones de personas que usaban el sitio entonces, y encontraron que era 3,74. Ahora, con el doble de gente que usa el sitio, la distancia entre dos personas en el mundo se ha acortado a 3,46 grados».

2.2.5. La cultura de la cancelación.

La vigencia de la teoría de los seis grados de separación y el extendido uso de las redes sociales, ha sido el punto de partida de conductas que pueden resultar lesivas para los derechos y libertades de muchas personas. Si bien las redes sociales y la forma en que la información circula en ellas, fueron de gran ayuda en circunstancias en las que se requirió convocar a la población en la denominada primavera árabe[8], pero en otras circunstancias, se ha convertido en fuente de vulneración de derechos, en lo que se ha denomina cultura de la cancelación.

Podemos definir a la cultura de la cancelación, como las consecuencias perniciosas derivadas de la circulación de información en redes sociales, que implican valoraciones de las conductas de determinadas personas, sin que necesariamente quien las publica conozca las circunstancias en las que los hechos se produjeron, haciendo juicios de valor

[8] El derrocamiento del régimen de Mubarak de Egipto se remonta a la publicación de un solo video en línea por un residente de 28 años de Alejandría, Egipto, llamado Khaled Said. El 6 de Junio de 2010, bajo el pretexto de que había sido tráfico de drogas, dos detectives lo sacaron de un cibercafé y lo golpearon hasta la muerte. A los dos días, un hombre Egipcio Wael Ghonim (tiene 30 años y ejecutivo de marketing de Google), creó una pagina de Facebook titulada Todos somos Khaled Said, que atrajo a 300 seguidores en los primeros dos minutos y se expandió a cientos de miles de personas. A finales de Enero de 2011, el grupo se había convertido en un clamor público que se reunieron en una manifestación masiva en la plaza Tahrir de El Cairo Square. Ver: Hal Licino. Cómo las redes crearon la primavera árabe en: https://www.benchmarkemail.com/es/blog/como-las-redes-sociales-crearon-la-primavera-arabe/

que son aceptados sin permitir a los involucrados emitir réplica alguna. Todo lo anterior produce en el afectado efectos negativos en lo profesional, laboral e incluso familiar.

Este fenómeno se ha puesto más en evidencia con la pandemia del COVID 19, en el marco de la cual, el uso de las redes sociales se ha elevado exponencialmente, así como las derivaciones de su uso. DELGADO (2020) ensaya una definición de la cultura de la cancelación:

«Recientemente ha surgido la cultura de la «cancelación» o *cancel culture*, un concepto que consiste en retirar el apoyo o «cancelar» a una persona que dijo o hizo algo ofensivo o cuestionable. Es un tipo de *bullying* grupal ya que son muchas personas que se ponen de acuerdo para atacar o descalificar los puntos de vista de otra persona o de alguna empresa. Esto se ha vuelto aún más popular al delatar actitudes racistas, homofóbicas y machistas. Es un movimiento tan grande que varias personas han perdido sus trabajos por ser canceladas, sin la posibilidad de enmendar o arreglar sus acciones, quedando para siempre encerradas en un charco de odio público».

Los efectos de la cancelación, se tornan mucho mas perniciosos, cuando se suma a fenómenos tales como el eWOM, esto es, el boca oído virtual, entendido como el criterio de una persona, a la que se califica como *influencer*, sobre otra; un producto, un servicio, una situación de cualquier naturaleza, que replicado por todos aquellos con los que comparte intereses, llega a extremos de volverse viral y posicionarse como una verdad incuestionable, sin que puede ejercer derecho a replicar las afirmaciones dichas en su contra, o a ejercer algún tipo de defensa contra su fiscal virtual.

2.2.6. Los datos personales en las redes sociales.

No cabe la menor duda que, cuando alguien se da de alta en una red social (cuando abre una cuenta), entrega de manera voluntaria datos relacionados tanto al titular de la cuenta, así como de terceros (amigos, familiares, compañeros de trabajo o estudios). Como esos datos, de manera general, son aptos para identificar a una persona física o la hacen identificable, lo que se ingresa a la red social, son datos personales. Es en ese momento en que se nos pide ingresar datos identificativos, con escaso nivel de confidencialidad, tales como nombre, profesión, número de documento de identidad, dirección de correo electrónico, etc., pero también se nos pide ingresar, con frecuencia, la filiación política,

confesión religiosa, condición de salud, e información relacionada a nuestros hijos (normalmente, menores de edad). Todos esos datos, pertenecen a los denominados datos sensibles o de categorías especiales, es decir, con un alto nivel de confidencialidad, normalmente incluidos en la esfera de la intimidad del titular de los datos y, en consecuencia, sometidos a un régimen reforzado de protección.

En el momento del alta de la cuenta en la red social, se debe configurar el nivel de seguridad en la circulación de la información, es decir, quién tendrá acceso a la información que se publique. Se deberá establecer si solo las personas que específicamente se autorice, como primera opción; a los autorizados por quien nosotros hayamos autorizado o, si la información podrá ser accesada libremente por cualquier interesado en ella. Tal configuración es trascendente debido a que, en función de ella, será de aplicación la llamada excepción doméstica, si se permite el acceso solo a quienes sean autorizados expresamente a ello y en número reducido, como circunstancia excluyente en la aplicación de la legislación en materia de protección de datos.

Como el ingreso de información en una red social, se adecua a la definición de tratamiento, establecido en el art. 4.2 del RGPD, por lo tanto, se debe aplicar las disposiciones relacionadas a la protección de datos personales y el responsable del tratamiento, estará sometido a las obligaciones y al interesado se le deberán reconocer los derechos como tal.

Si los datos personales ingresados a una red social, deben considerarse o no un tratamiento sujeto a la aplicación de la normativa de protección de datos personales, no es una discusión superada. Fue concretamente a partir del caso de la catequista sueca Bodil Lindqvist que el Tribunal de Justicia de la Unión Europea (en adelante TJUE), en sentencia de 6 de noviembre del 2003, asunto C-101/01[9] que se establecieron criterios para la determinación de tratamientos sometidos a la legislación de protección de datos personales.

Resolvió que que la conducta que consiste en hacer referencia, en una página web, a diversas personas y en identificarlas por su nombre o por otros medios, como su número

[9] Véase: https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:62001CJ0101&from=EN

de teléfono o información relativa a sus condiciones de trabajo y a sus aficiones, constituye un «tratamiento total o parcialmente automatizado de datos personales» en el sentido del art. 3, apartado 1, de la Directiva 95/46. Sin mayor esfuerzo hermenéutico se concluye que lo dicho en relación a la información ingresada a un sitio Web, se aplica a aquella ingresada a las plataformas de las redes sociales.

Debemos reparar, en este punto, que la cantidad de información ingresada en las plataformas de las redes sociales, es extremadamente grande, así como la capacidad de procesamiento, en gran medida como consecuencia del uso de las técnicas de *social big data*, mediante la cual, se puede procesar con enorme rapidez, los datos personales de cientos de millones de personas, logrando con ello, el perfilado de los usuarios de las redes, en beneficio de quienes manejan la información personal de los usuarios. Precisamente es este hecho, lo que deriva en la expresión economía de los datos, pues el perfilado conlleva la posibilidad de conocer los gustos y preferencias que finalmente permitirán a aquellos que ofrecen bienes y servicios, diseñar estrategias publicitarias dirigidas específicamente a los interesados en ellos, volviendo una verdad incuestionable aquello de que en redes sociales, cuando un servicio se presenta como gratuito, el producto comercializado es el usuario.

2.2.6.1. Privacidad desde el diseño o por defecto en las redes sociales.

Como una de las expresiones en la aplicación del principio de responsabilidad proactiva, se establece que los responsables y encargados del tratamiento de los datos personales deben aplicar el criterio de la privacidad desde el diseño o por defecto. El cumplimiento de dicho precepto, en relación a las redes sociales, se torna particularmente importante, considerando que el cumplimiento de la obligación de informar, como parte de la observancia de otra obligación atribuida a los responsables y encargados del tratamiento de los datos personales, esto es, la licitud lealtad y transparencia, es precariamente cumplido, esencialmente debido a lo largo y muchas veces denso contenido jurídico, ininteligibles términos y condiciones de uso de las plataformas, que derivan en una aceptación inconsciente de los mismos, en detrimento de los derechos y libertades de los interesados, usuarios de las redes sociales, realidad que crece exponencialmente cuando se involucran menores de edad.

Por lo expresado *supra*, es imprescindible que los desarrolladores de las aplicaciones de redes sociales, las diseñen teniendo en cuenta la máxima protección posible a los datos personales, lo que debería incluir una configuración inicial, al máximo nivel de dicha protección, con independencia de los conocimientos de seguridad de los interesados. Lo anterior no obsta para esperar de los responsables, el cabal cumplimiento del deber de informar en un lenguaje sencillo y claro, sin ambigüedades, incluso pensando que existe un importante número de usuarios que son menores de edad y, en consecuencia, con poca conciencia del peligro que, para sus derechos y libertades, asumen al compartir información personal propia o de terceros. Es aquí donde se debe emplear un método de informacion por capas o niveles para informar a los usuarios de las redes sociales, en los que en un primer nivel se explique de manera general, las condiciones de uso de las redes y, mediante enlace, dirigir a los usuarios más entendidos (o acuciosos) a la descripción íntegra de los términos y condiciones de uso de las redes sociales.

Sobre la aplicación de este principio en el diseño de las aplicaciones relacionadas a las redes sociales, ORTEGA (2010, p. 320) establece:

«En privacidad en el diseño se parte del hecho que todos los requisitos relacionados con el tratamiento de datos personales y privacidad se deben identificar, analizar e incorporar de forma integrada y sistemática en las especificaciones iniciales del nuevo sistema. Para ello, es necesario evaluar todos los procesos y flujos de información previstos en el sistema, analizando sus implicaciones en privacidad desde un punto de vista holístico, preventivo y con un foco más allá del marco jurídico vigente».

De lo afirmado por el autor citado, debemos concluir que, dependiendo de la categoría de datos que se prevén se van a ingresar a la plaforma de la red social, estas deben establecer inicialmente, entiéndase desde su diseño, el nivel de seguridad adecuado al riesgo que se establezca en el análisis respectivo, protegiendo los derechos y libertades de los interesados aún de si mismos. Es precisamente en aplicación de este principio en el que se deben implementar los controles parentales en la plataforma de las redes sociales, para que los padres y madres de familia o los tutores legales en su ausencia, tengan la posibilidad de determinar la información a la que pueden acceder sus hijos o la que pueden compartir, de suerte de reforzar la protección de quienes, como los menores de edad, de

ordinario no tienen noción de los peligros (o lo menosprecian) que entraña compatir información personal con quienes realmente no conocen.

2.2.6.2. Algunos riesgos para los datos personales en el uso de las redes sociales.

Hemos evidenciado que los usuarios de las redes sociales, en ejercicio de su derecho a producir información, son los encargados de proporcionar datos personales de los que son titulares y de titularidad de terceros. Cuando lo hacen, consciente o inconscientemente, ponen en riesgo sus derechos y libertades, mencionamos algunos de ellos:

a) **Sexting**: Es una inveterada costumbre de los usuarios más jóvenes de las redes sociales, con frecuencia menores de edad, intercambiar con sus parejas sentimentales imágenes o vídeos con connotaciones eróticas e incluso sexualmente explícitas. Tal conducta se la ha denominado como *sexting*, una expresión derivada de las palabras inglesas: *sex* (sexo) y *testing* (mensajear). Si bien es cierto, tal conducta no es contraria a ley alguna, el problema se centra en la posibilidad de brechas de seguridad en los dispositivos usados para intercambiar esos contenidos, que puede afectar la confidencialidad de los datos y, por esa vía, vulnerar los derechos de los interesados, es decir, puede llegar a manos de terceros ajenos al destinatario resultando con ello, una severa afectación a la intimidad y reputación, con las afectaciones, no solo a sus derechos y libertades, sino que con frecuencia a su salud mental e incluso física.
b) **Sextorsión**: Como una consecuencia de una brecha de seguridad en el desarrollo del *sexting*, puede ocurrir que aquellos a cuyas manos hayan llegado las imágenes objeto de intercambio entre dos personas, ejerzan sobre ellas, exigencias de índole económica e incluso sexuales, es decir, exigen tener contacto sexual con su víctima so pena de hacer públicas las imágenes en el caso de negarse a cumplir con sus exigencias. De lo anterior se deriva la denominación que se le ha dado a esta conducta, esto es, la fusión de las palabras: sexo y extorsión. Esta conducta esta ligada a otra, por medio de la cual, se expone a la víctima, con quien el infractor ha tenido una relación sentimental, al escarnio social, cuando hacen públicas, normalmente en sus redes sociales, mensajes, imágenes o videos íntimos, tras la ruptura de sus relaciones sentimentales, como una

suerte de venganza. Esta conducta se la conoce como porno venganza (*revenge porn*), que está tipificada en Ecuador como violación a la intimidad[10].

c) **Pornografía infantil**: Cuando una imagen sexualmente explícita en la que está involucrado un menor de edad, se encuentra en poder de otra que no lo sea, tal conducta configura el delito de pornografía infantil.

El art. 189 del *Código Penal español* sanciona con pena privativa de libertad de uno a cinco años esta infracción, incluyendo los siguientes elementos en el tipo: a) El que captare o utilizare a menores de edad o a personas con discapacidad necesitadas de especial protección con fines o en espectáculos exhibicionistas o pornográficos, tanto públicos como privados, o para elaborar cualquier clase de material pornográfico, cualquiera que sea su soporte, o financiare cualquiera de estas actividades o se lucrare con ellas.

De la revisión de la norma penal española, podemos advertir que las conductas que incrimina son: captar o utilizar material, debe entenderse imágenes o videos, que puedan considerarse erótico, en el que se incluya menores de edad o personas con discapacidad, se subsumen en este delito. Nos parece que, frente a la alarma social que causa la vulneración de los derechos a los menores, merece una sanción más drástica que la establecida. Ecuador sanciona este delito con pena privativa de libertad que puede llegar, atentas las circunstancias, a los veintiséis años[11].

[10] **art. 178 COIP**.- Violación a la intimidad.- La persona que, sin contar con el consentimiento o la autorización legal, acceda, intercepte, examine, retenga, grabe, reproduzca, difunda o publique datos personales, mensajes de datos, voz, audio y vídeo, objetos postales, información contenida en soportes informáticos, comunicaciones privadas o reservadas de otra persona por cualquier medio, será sancionada con pena privativa de libertad de uno a tres años.

[11] art. 103 COIP: Pornografía con utilización de niñas, niños o adolescentes.- La persona que fotografíe, filme, grabe, produzca, transmita o edite materiales visuales, audiovisuales, informáticos, electrónicos o de cualquier otro soporte físico o formato que contenga la representación visual de desnudos o semidesnudos reales o simulados de niñas, niños o adolescentes en actitud sexual; será sancionada con pena privativa de libertad de trece a dieciséis años.
Si la víctima, además, sufre algún tipo de discapacidad o enfermedad grave o incurable, se sancionará con pena privativa de libertad de dieciséis a diecinueve años.
Cuando la persona infractora sea el padre, la madre, pariente hasta el cuarto grado de consanguinidad o segundo de afinidad, tutor, representante legal, curador o pertenezca al entorno íntimo de la familia; ministro de culto, profesor, maestro, o persona que por su profesión o actividad haya abusado de la víctima, será sancionada con pena privativa de libertad de veintidós a veintiséis años.

d) ***Grooming***: La conducta que se adecua a este tipo penal, es aquella que manifiesta un adulto, que se hace pasar por un menor para ganarse la confianza de otra que si lo sea, para lograr de esta, el envío de información personal con la que posteriormente pretenderá tener contacto, mediante amenazas; RAMÍREZ (2020) define esta conducta expresando:

«El significado de *grooming* podría traducirse como una práctica de ciberacoso sexual en la que un adulto engaña a un menor de edad con una finalidad sexual. Esta modalidad es más usada en las redes sociales por pedófilos y pederastas para ganarse la confianza de los menores y establecer vínculos emocionales con ellos con el objetivo de conseguir fotografías o vídeos de contenido sexual protagonizados por los menores, en el caso de los primeros, o incluso llegar a mantener un encuentro sexual, en el caso de los segundos».

Esta conducta implica que se asume una identidad falsa, en la que se incluye una edad acorde con la del menor, para hacer creer a la víctima, que existe afinidad con su interlocutor y lograr, de este modo, su confianza al extremo de entablar una amistad y, eventualmente lograr un contacto físico con su víctima. Ecuador ha incluido esta conducta en el catálogo de infracciones, sancionándola con severidad[12], en gran medida teniendo en mente que los menores de edad tienen gran presencia en las redes sociales, ya no solo con fines de contactas amigos, sino en época de pandemia, con fines académicos.

[12] art. 174 COIP.- Oferta de servicios sexuales con menores de dieciocho años por medios electrónicos.- La persona, que utilice o facilite el correo electrónico, chat, mensajería instantánea, redes sociales, blogs, fotoblogs, juegos en red o cualquier otro medio electrónico o telemático para ofrecer servicios sexuales con menores de dieciocho años de edad, será sancionada con pena privativa de libertad de siete a diez años

3. Conclusiones

Tras el desarrollo del análisis realizado sobre la protección de los datos personales y la incidencia que para su ejercicio generan las redes sociales, llegamos a las siguientes conclusiones:

1. **Trascendencia de las redes sociales**: Los datos personales han adquirido una enorme importancia en el desarrollo de la sociedad de la información y esta, a su vez, nos guste o no, es en la actualidad omnipresente.
2. **Beneficios y Riesgos**: Entre los más importantes servicios de la denominada sociedad de la información, se encuentran sin lugar a dudas, las redes sociales. En las actuales circunstancias de pandemia, provocada por el COVID 19, estas han demostrado ser de gran ayuda a la hora de establecer contacto con amigos y familiares, en el desarrollo de actividades laborales, como mecanismo de estudio y entretenimiento. Ciertamente ha sido posible, en gran medida gracias a ellas, sobrellevar el obligado aislamiento, pero también con ellas han surgido nuevas y muy numerosas amenazas, que las sociedades han demostrado no estar del todo preparadas para enfrentar.
3. **Menores de edad**: El manejo de los datos personales, de no mediar un adecuado control, se puede convertir en una forma de vulnerar los derechos y libertades de sus titulares, especialmente cuando están involucrados menores de edad, volviendo caótico su uso y, en consecuencia, convirtiéndose en obstáculo para su normal desarrollo integral.
4. **La situación ecuatoriana**: En relación con Ecuador, si bien es verdad, que se ha legislado para enfrentar, desde la producción normativa penal, conductas que van en contra de bienes tutelados, tales como: la intimidad, la propia imagen, la reputación, los derechos sexuales de los menores y las personas con discapacidad, pero solo recientemente se ha reparado en la necesidad de establecer un sistema de protección alrededor de los datos personales, luego de aprobar la Ley Orgánica de Protección de Datos, cuya difusión y estudio no solo por parte de abogados y funcionarios públicos, sino por el conjunto de la sociedad, es una tarea que se debe asumir con

responsabilidad, para lograr un nivel de aplicación que permita la construcción de un eficiente sistema de protección de los datos personales.

5. **Necesidad de difusión**: Solo en la medida que se entienda, por parte de los ciudadanos, los peligros que se ciernen sobre ellos a través de los accesos no consentidos a sus datos personales, será evidente la necesidad de conocer los derechos que se han reconocido en la novísima legislación y el sistema de protección que propone. Es el camino que ha recorrido Europa desde que en los años setenta del siglo pasado, se empezó a construir el sistema vigente entre los países que componen la Unión Europea y es el que debemos recorrer a partir de ahora en Ecuador.

Referencias bibliográficas

ÁLVAREZ, J. Protección de datos, Practicum, Pamplona:Thomson Reuters, 2020.

APARICIO, J. y VIDAL, M. Estudio sobre la protección de datos. Pamplona:Thomson Reuters, 2019.

BARRIO, M. Manual de Derecho Digital, Valencia: Tirant lo Blanch, 2020.

BERROCAL, A. Derecho de Supresión de datos o derecho al olvido, Madrid:Reus, 2017.

CAZURRO, V. Antecedentes y fundamentos del Derecho a la protección de datos, Logroño: Bosch, 2020.

CEVALLOS, J. «Aspectos generales del derecho a la propia imagen». La Propiedad Inmaterial. Revista del Departamento de la Propiedad Intelectual de la Universidad Externado de Colombia, núm. 15, pp. 61-83, ISSN 1657-1959.

DAVARA, M. Manual de Derecho Informático, Pamplona:Thomson Reuters, 2015.

DELGADO, P. «Estás cancelado. La cultura de la cancelación y sus implicaciones sociales». Observatorio, Instituto para el futuro de la Educación, Tecnológico de Monterrey [consulta: 20 de agosto del 2021]. Disponible en: https://observatorio.tec.mx/edu-news/cultura-de-la-cancelacion.

FERNÁNDEZ, H. Manual de Derecho Informático, Buenos Aires: Abeledoperrot, 2016.

FERNÁNDEZ, M. Derecho Digital: Retos y cuestiones actuales, Madrid: Aranzadi, 2016.

FLORES, A., GALICIA, G., SÁNCHEZ, E. «Una aproximación a la Sociedad de la información y del Conocimiento» Revista Mexicana de Orientación Educativa. 2007, vol. 5, núm. 11, 19-28 [consulta: 24 de agosto de 2021]. ISSN 1665-7527. Disponible en: Una http://pepsic.bvsalud.org/scielo.php? script=sci_arttext&pid=S1665-75272007000100004

GARCíA, P (Director). Principios de Derecho de Internet, Valencia: Tirant lo Blanch, 2005.

HURTADO, L. Manual de Derecho Informático, Guayaquil:Biblioteca Jurídica, 2018.

LONDOÑO, P. «Networking: La teoría de los 6 grados de separación». Semana. 2017 [consulta: 24 de agosto de 2021]. Disponible en: https://www.semana.com/opinion/columnistas/articulo/teoria-de-los-seis-grados-de-separacion-networking-pablo-londono/244890/.

LóPEZ, J. (Director). El Derecho a la intimidad, Nuevos y viejos debates, Madrid: Dykinson, 2017.

MINISTERIO DE TELECOMUNICACIONES Y SOCIEDAD DE LA INFORMACION. [consulta: 7 de septiembre 2021] Disponible en: https://www.telecomunicaciones.gob.ec/wp-content/uploads/2021/05/Agenda-Digital-del-Ecuador-2021-2022-222-comprimido.pdf

Piñar, J. (Director). Reglamento General de Protección de Datos. Hacia un nuevo modelo europea de privacidad, Madrid: Reus, 2016.

PLAN V (redacción). «La peor filtración de datos en la historia del Ecuador al descubierto». [consulta: 25 de agosto del 2021]. Disponible en: https://www.planv.com.ec/historias/sociedad/la-peor-filtracion-datos-la-historia-del-ecuador-al-descubierto.

RALLO, A. (Director). Tratado de protección de datos, Valencia: Tirant lo Blanch, 2019.

RALLO, A y MARTINEZ, R. (Coordinadores). Derecho y redes sociales, Pamplona:Thomson Reuters, 2010.

RAMÍREZ, H. «Grooming: Qué es, cómo detectarlo y prevenirlo». Grupo Ático 34. [consulta: 21 de agosto del 2021]. Disponible en: https://protecciondatos-lopd.com/empresas/grooming/.

RAMOS, X. «Hay 14 millones de usuarios digitales en Ecuador concentrados más en las redes sociales y en videos que en el acceso a noticias e información». El Universo. 23 de mayo de 2021. Disponible en: https://www.eluniverso.com/noticias/informes/hay-14-millones-de-usuarios-digitales-en-ecuador-concentrados-mas-en-las-redes-sociales-y-en-videos-que-en-el-acceso-a-noticias-e-informacion-nota/

REBOLLO, L. y SERRANO, M. Introducción a la Protección de Datos. Madrid: Dykinson, 2006.

RICO, M (Coordinadora). Derecho de las Nuevas Tecnologías, Buenos Aires:La Roca, 2007.

RODRÍGUEZ, J. Figuras y responsabilidades en tratamientos de datos personales. Logroño: Bosch, 2019.

ROMEO, C. «Datos personales (comentario al artículo 4.1 RGPD)», pp. 573-589. En TRONCOSO, A. (coor.) Comentario al Reglamento General de Protección de Datos y a la Ley Orgánica de Protección de Datos Personales y Garantía de Derechos Digitales, Tomo I. 1a ed. Pamplona:Thomson Reuters, 2021.

TELLEZ, A. Nuevas tecnologías. Intimidad y protección de datos, estudio sistemático de la Ley Orgánica 15/1999, Madrid: Edisofer, 2001.

TOMEO, F. Redes sociales y tecnologías 2.0, Buenos Aires: Astrea, 2014.

TOURIñO, A. El Derecho al olvido y a la intimidad en Internet. Madrid: Los Libros de la Catarata, 2014.

Normas Jurídicas

Ecuador. Constitución de la República, 20 de octubre del 2008, Registro Oficial, núm. 449.

Ecuador. Ley Orgánica de Protección de Datos Personales, 26 de mayo del 2021, Registro Oficial, núm. 459.

Ecuador. Código Orgánico Integral Penal, 10 de febrero del 2014, Suplemento del Registro Oficial, núm. 180.

Ecuador. Ley Orgánica de Garantías Jurisdiccionales y Control Constitucional, 22 de octubre del 2009, Suplemento del Registro Oficial, núm. 52.

Ecuador. Ley Orgánica de Transparencia y Acceso a la Información Pública, 18 de mayo del 2004, Suplemento del Registro Oficial, núm. 337.

España. Ley Orgánica 3/2018, de 5 de diciembre, de protección de datos y garantías de los derechos digitales. Boletín Oficial del Estado, 6 de diciembre del 2018, núm. 294, sec. I, pág. 119788.

España. Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y comercio electrónico, Boletín Oficial del Estado, núm. 166, 12 de julio del 2002, pág. 13758.