



Universidad Internacional de La Rioja  
Facultad de Derecho

Máster Universitario en Protección de Datos

**LA PROTECCIÓN DE DATOS EN LAS REDES  
SOCIALES**

Trabajo de fin de estudio presentado por:	<b>Juan Pablo Burbano Balseca</b>
Tipo de trabajo:	Trabajo Final de Máster (TFM)
Director/a:	<b>Antonio Fayos Gardo</b>
Fecha:	09/05/2021

## Resumen

En la actualidad la protección de los datos personales publicados en las redes sociales, se han convertido en un tema de mucho valor e interés para la sociedad en general, por lo que es muy importante realizar un análisis de la problemática legal que se desprende del uso no racionalizado de las redes sociales. Este estudio es importante puesto que abarca un fenómeno que tiene significativos efectos en las personas usuarias de las redes sociales, mediante esta investigación se puede contribuir de manera positiva con alternativas que permitan que las personas puedan dar un verdadero uso de las redes sociales. De tal manera, la relevancia de este estudio recae en el cuidado e importancias que se le debe dar a las publicaciones en las redes sociales. Su objetivo principal consistió en: analizar el uso de tecnología, mediante del análisis documental y de campo, para contribuir en la protección de datos en las redes sociales.

**Palabras clave:** Publicación, Datos personales, Redes sociales, tecnología, protección.

## Abstract

At present, the protection of personal data published on social networks has become a subject of great value and interest for society in general, so it is very important to carry out an analysis of the legal problems that arise from the use not streamlined from social media. This study is important since it covers a phenomenon that has significant effects on people who use social networks, through this research it is possible to contribute in a positive way with alternatives that allow people to make real use of social networks. Thus, the relevance of this study lies in the care and importance that should be given to publications on social networks. Its main objective consisted of: analyzing the use of technology, through documentary and field analysis, to contribute to the protection of data on social networks.

**Keywords:** Publication, Personal data, Social networks, technology, protection.

## Índice de contenidos

### Contenido

Resumen.....	3
Abstract .....	4
Índice de contenidos.....	5
Índice de Anexos.....	7
1. Introducción .....	8
1.1. Justificación del tema elegido .....	8
1.2. Problema y finalidad del trabajo .....	9
1.3. Objetivos .....	10
1.3.1. Objetivo General.....	10
1.3.2. Objetivos Específicos .....	10
2. Marco teórico y desarrollo.....	11
2.1. Protección de Datos.....	11
2.1.1. Origen y Evolución de la protección de datos.....	13
2.1.2. Privacidad como Derecho Humano .....	16
2.1.3. Datos personales en redes sociales .....	18
2.1.4. Legislación Española en la protección de datos personales. ....	20
2.1.5. Legislación Ecuatoriana en la protección de datos .....	21
2.1.6. El Estado en el Ciberespacio.....	22
2.2. Uso de la Tecnología. ....	29
2.2.1. Impacto en la sociedad .....	29
2.2.2. Realidad Virtual .....	30
2.2.3. Redes sociales.....	31

2.2.4.	Riesgos ventajas, desventajas y amenazas de la privacidad en las redes sociales	32
2.2.5.	Lo público y privado en redes sociales .....	34
2.2.6.	La dimensión pública de una persona en redes sociales .....	35
2.2.7.	La dimensión privada e íntima. ....	35
2.2.8.	Estrategias para la privacidad .....	36
2.2.9.	Principio de la autodeterminación informativa. ....	37
3.	Conclusiones.....	55
	Referencias bibliográficas .....	56
	Listado de abreviaturas .....	61
Anexo A.	REGLAMENTO .....	62

## Índice de Anexos

Reglamento General de la Protección de Datos.....	62
Código Orgánico Integral Penal .....	63
Constitución Política del Ecuador .....	64

## 1. Introducción

Las redes sociales tienen su inicio aproximadamente desde el año 2002, las cuales facultan a las personas interactuar con otras personas, es decir que las redes sociales se han ido poco a poco integrando como una herramienta del convivir diario de la sociedad. Es por esto que el presente estudio nace como interés personal de ver como los usuarios hacen publicaciones de muchos datos en las redes sociales sin tomar conciencia de lo perjudicial que sería para ellos el publicar información de validez en su vida personal, no se puede dejar de un lado que hoy en día las redes sociales se han convertido en el medio de información y comunicación de las personas, pero se debe tener en cuenta que es lo que se puede publicar y que es lo que no se puede publicar, con el propósito de prevenir que los datos personales sean mal utilizados. En este sentido se analiza la protección que debe brindarse a los datos personales publicados en las redes sociales e identificar los diferentes riesgos a los cuales se exponen los usuarios al momento de publicar sus datos ya sean estos personales e institucionales y así poder determinar técnicas, estrategias y mecanismos legales que respalden la integridad física y personal de los usuarios. Por consiguiente, la presente investigación se la ejecuta con el fin de hacer tomar conciencia a las personas que hacen uso de las redes sociales en cada uno de los riesgos del mal manejo de las redes sociales,

### 1.1. Justificación del tema elegido

Frente a lo expuesto, se justifica el estudio puesto que, los usuarios de las redes sociales tienen derecho a que sus datos personales sean protegidos, por otro lado, se puede considerar que España mediante la Agencia Española de Protección de Datos es un país que ha evolucionado en lo referente al derecho de la protección de datos. Esta indagación sirve para que las personas que hacen uso de las redes sociales conozcan que, aunque en el Ecuador no se ejecute a plenitud el derecho a la protección de datos, si existen leyes y reglamentos internacionales que lo hacen y que permiten garantizar la seguridad y la privacidad de las personas al publicar sus datos personales en las redes sociales.



Este estudio es importante puesto que abarca un fenómeno que tiene significativos efectos en las personas usuarias de las redes sociales, mediante esta investigación se puede contribuir de manera positiva con alternativas que permitan que las personas hagan un verdadero uso de las redes sociales. De tal manera, la relevancia de este estudio recae en el cuidado e importancias que se le debe dar a las publicaciones en las redes sociales.

Por lo tanto, con la investigación se podrá hacer recapacitar a los usuarios de lo importante que es la no publicación de cada una de sus actividades diarias en las redes sociales por su seguridad, puesto que, al momento de subir un dato personal, se tiene que ser consciente del control que se pierde de la información publicada, la cual es revisada y en muchas ocasiones compartida por otras personas sin autorización del dueño, con lo que se vulneran los derechos de los usuarios de las redes sociales.

## 1.2. Problema y finalidad del trabajo

La protección de los datos personales en diferentes países está respaldada en legislaciones, con los avances de la tecnología es necesario la implementación de leyes internas, en donde cada país marca sus propias tendencias. El auge de la tecnología y el uso frecuente del internet de parte de las personas permiten que el Estado Ecuatoriano se vean en la necesidad de implementar leyes y reglamentos que brinden las garantías necesarias a los usuarios de las redes sociales.

En la actualidad la protección de los datos personales publicados en las redes sociales, se han convertido en un tema de mucho valor e interés para la sociedad en general, por lo que es muy importante realizar un análisis de la problemática legal que se desprende del uso no racionalizado de las redes sociales. La finalidad del estudio consiste en hacer ver a los usuarios de las redes sociales la realidad de la vulneración de sus derechos que se exponen al momento de hacer todo tipo de publicación de su convivir diario, por razones culturales se debe establecer que los usuarios sean más conscientes, y que a pesar de que se tenga una ley y un reglamento si no se cambia esa falta de consciencia de los usuarios de nada servirá tenerla.

### 1.3.Objetivos

#### 1.3.1. Objetivo General

- Analizar a la protección de datos concerniente a redes sociales en la legislación ecuatoriana.

#### 1.3.2. Objetivos Específicos

- Identificar los riesgos más comunes en el Ciberespacio.
- Detallar los mecanismos legales de la protección de datos.
- Establecer una comparativa entre la legislación ecuatoriana y española con relación a la protección de datos en materia de redes sociales.

## 2. Marco teórico y desarrollo

### 2.1. Protección de Datos

Los datos personales se refieren a toda información de carácter personal y/o reservada, relativa a un determinado sujeto y que lo vuelve identificable como individuo. En virtud de lo expuesto dicha información le otorga una identidad, descripción, lugar de procedencia, edad, domicilio, trayectoria profesional y/o académica, entre otros. Además de lo ya mencionado, los datos personales describen aspectos más sensibles o delicados del individuo como lo es, ideología, inclinación política, estado de salud, características físicas, costumbres y tendencias sexuales (Instituto Federal de Acceso a la Información Pública, 2010).

El tratamiento de los datos personales constituye uno de los temas que adquirido mayor relevancia durante los últimos 50 años y ha llamado la atención tanto de los entes reguladores, los operadores privados y demás organizaciones. De forma inicial, fue muy poco reglamentado, pero en el transcurso de la última década y ante el desarrollo inconmensurable de la tecnología y la eclosión mundial de servicios como el internet, las telecomunicaciones, las redes sociales, los servidores y demás que hacen alusión a la sociedad de la información han puesto de manifiesto la indiscutible relevancia social y económica que tiene la información personal y su adecuado tratamiento (Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales., 2015).

En tal sentido, la protección de datos personales está vinculada al uso de la informática y de forma más explícita en la afectación de una serie de datos o conocimientos que hacen alusión a la esfera de la intimidad del sujeto. De esta forma, el tratamiento de datos y la recolección de los mismos, son presupuestos fundamentales para la protección de los datos personales y son objeto de amparo de un ordenamiento jurídico especializado (Mayorga, García, Duret, Carrión, & Yarad, 2019).

De acuerdo con Maqueo, Moreno, y Recio (2017) los datos personales hacen alusión a cualquier información que se refiera a una persona y que de forma más explícita pueden abarcar los siguientes aspectos de un ser humano como:

- Familia.
- Transacciones financieras y solvencia económica
- Creencias religiosas e ideologías políticas
- Procesos judiciales y condenas criminales
- Origen étnico o racial
- Profesión e historial laboral
- Historial académico, títulos y grados obtenidos en los diversos niveles de la educación
- Conductas y comportamientos sexuales
- Trastornos psicológicos
- Pasatiempos
- Historial clínico, salud y presencia de enfermedades, entre otros.

En pocas palabras, los datos personales se constituyen como la información sobre las personas en todos los ámbitos de su propia existencia e independientemente de los medios que se utilizan para captarlos, almacenarlos, utilizarlos, manejarlos, registrarlos o comunicarlos, son objetos de protección por parte del ordenamiento jurídico.

Según la Organización de Cooperación y el Desarrollo Económico (1980) los datos personales se entienden como toda información correspondiente a una persona identificada o identificable y que se encuentra regulada por un controlador de datos, establecido de conformidad con la legislación nacional, cuyas competencias principales radican en el determinar los contenidos y el uso de los datos personales independientemente de su capacidad para recoger, guardar, procesar o divulgar dicha información.

De forma concordante, la Directiva 95-46-ce del Parlamento Europeo y del Consejo (1995) relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales señala que los datos personales son toda información sobre una persona física identificada o identificable; no obstante y a diferencia del concepto aportado por la

Organización de Cooperación y el Desarrollo Económico, la Directiva considera como datos relativos a una persona identificable a toda información que permita determinar de forma directa o indirecta y en particular a través de un número de identificación a uno o varios aspectos o elementos específicos característicos de la identidad física, fisiológica, psíquica cultural, económica o social de la persona.

### 2.1.1. Origen y Evolución de la protección de datos

Actualmente a nivel internacional, nacional y local, lo referente a la protección de datos ha sido un tema que ha ido conociéndose por la comunidad en general, puesto que este permite que cada una de las personas puedan conocer a lo que se exponen al momento de administrar sus datos en los diferentes medios informativos.

De acuerdo con Mayorga, García, Duret, Carrión y Yarad (2019) la protección de datos personales se concibe como un derecho humano de tercera generación producto de la evolución constante de los derechos erigidos desde la Declaración Universal de los Derechos Humanos de 1948. en este contexto la Declaración (Asamblea General de las Naciones Unidas, 1948) en su artículo 12 señala que ninguna persona podrá ser objeto de injerencias arbitrarias en su vida privada, en su vida familiar, a su domicilio o a su correspondencia, además, no podrá ser objeto de ataques tanto en contra de su honra como de su reputación y en función de precautelar y garantizar tales preceptos, todo ser humano tiene derecho a la protección contra tales injerencias o ataques a través del establecimiento de un ordenamiento jurídico.

de esta forma, el catálogo de los derechos humanos a lo largo de la historia se ha mostrado permeable y abierto a la incorporación de nuevos valores sin perjuicio de la aceptación unánime por parte de la doctrina; no obstante y en función de los avances tecnológicos el legislador se ha visto en la necesidad de dar respuestas a las nuevas pretensiones individuales que se derivan de los importantes cambios en la esfera social, económica, política y cultural suscitada a raíz de los fenómenos propios de las nuevas realidades y coyunturas. En síntesis, el progreso social y el desarrollo tecnológico han demandado no sólo la protección más integral y estricta sobre la esfera personal del individuo sino también requieren de garantías

que aseguren la correcta manipulación de la información personal de un individuo en sus relaciones con terceros (Herrán Ortiz, 2003).

Resulta importante destacar que el desarrollo normativo del derecho a la intimidad frente a la información y la protección de los datos privados, tanto en el ámbito constitucional y normativo, se denotó primero en el continente europeo y posteriormente en América Latina. el primer antecedente en Europa con relación al derecho para controlar la información en sistemas de contenido se puede observar en la Constitución alemana de Weimar de 1919, la cual permitía a un funcionario a examinar su expediente personal. Para 1967 el Consejo de Europa efectuó un estudio sobre el avance de las tecnologías de la información y su incidencia en la vulneración del derecho a la intimidad, con ello a mediados de los setenta se aprobaron las resoluciones sobre protección de la intimidad frente a los bancos electrónicos de datos en el sector privado y público (Ojeda, 2015).

Jauregui (2012), expresa que:

La protección de datos de carácter personal, es una de las claves esenciales del respeto a la vida privada dentro de la defensa de los derechos humanos y las libertades fundamentales, por ello es importante que las leyes de transparencia y acceso a la información pública, contemplen como excepción al derecho de acceso, el derecho a la vida privada y la intimidad de las personas (p.32).

En otras palabras, se llama datos personales a cualquier información que determine nombres, cedula de identidad, localización o identificador en línea, así mismo el uso de varios elementos que generen identidad ya sea física, genética, económica, cultural, educativa o social de las personas.

En algunos países se han creado marcos regulatorios, los cuales cuentan con ciertos componentes y prohibiciones sobre el uso de la información garantizando el derecho de las personas. En el caso de España la jurisprudencia del Tribunal Constitucional, es quien ha dado

la carta de naturaleza para la formulación del derecho a la protección de datos la cual tiene su soporte en la Constitución Española desde 1978. A nivel mundial sería una buena alternativa que todos los países cuenten con marcos regulatorios en donde se limite a los usuarios de hacer todo tipo de publicaciones en las redes sociales.

Por lo tanto, se puede considerar que se reconoce a los usuarios los diferentes derechos en referencia a los datos personales que las empresas tienen que respetar, así mismo se imponen muchas obligaciones ya sean formales o sustantivas, las cuales se deben de cumplir.

Es de gran importancia el respaldo que se le brinda al usuario al momento que hace uso de las redes sociales para publicar datos personales, pero sería bueno que la ciudadanía tome consciencia en la forma que hace publicaciones, ya que esto les puede generar complicaciones tanto personal como familiar, no todo lo que hacemos es lo que debemos publicar, debemos de tener límites y saber que debemos y que no debemos publicar.

Se puede considerar que hoy en día el uso del internet proporciona la facilidad para poder obtener información de las personas quienes son parte de las diferentes redes sociales, lo que ha forjado el desarrollo de algunas reglas orientadas a la limitación del uso de datos personales son el fin de aseverar la dignidad de las personas.

Por otro lado, los datos personales son entendidos como aquellos en donde se afecta lo íntimo de las personas, los mismos que al momento de ser mal utilizados originan discriminación causando graves riesgo en las personas, cabe recalcar que esta información está sustentada en principios relativos, referentes a los datos personales, que pueden ser de calidad, legitimización del tratamiento de datos, seguridad, cesión a terceros y ciertos datos, los mismos que tienen que ser protegidos por su contenido.

Además, en la protección de datos se debe aludir que son de autonomía convivencial, es decir que en caso de existir alguna vulneración es deber del Estado ecuatoriano brindar las garantías necesarias a la protección de los datos personales. Una persona que haga uso de las redes sociales y que realmente sea consciente de sus actos tomará los respectivos correctivos y evitará hacer publicaciones que en lo posterior pueden causales afectaciones negativas y

perjudiciales en el aspecto personal, familiar, social y porque no laboral, es por eso que los usuarios tienen que ser más cautelosos a momento de hacer publicaciones, sea que existan o no existen leyes que sancionen este tipo de activos, las personas tenemos que evitar en lo posible publicar datos personales en las redes sociales.

### 2.1.2. Privacidad como Derecho Humano

El concepto el derecho a la intimidad en el ámbito jurídico se sustenta en el principio de la dignidad humana y en la tutela de la personalidad individual. Es decir, el derecho a la intimidad se constituye como una manifestación y una de las varias esferas que componen al derecho a la dignidad humana; pero de forma más específica, el concepto de intimidad se liga al derecho a la libertad individual ya sea en los ámbitos de la reserva de la persona, así como en el control de la información personal, de esta forma, la intimidad como manifestación de la libertad individual le permite a cada persona decidir la medida en la que desea mantener la esfera privada de su información personal, familiar y ser dejado en paz respecto de terceros (Herrán Ortiz, 2003).

Según el Tribunal Constitucional de España (SENTENCIA 53/1985, de 11 de abril, 1985) la dignidad es un valor espiritual y moral inherente a toda persona que se manifiesta de forma singular en la autodeterminación consciente y responsable de su propia vida y que lleva consigo la pretensión al respeto por parte de la sociedad y de los otros individuos que la conforman.

De esta forma se puede decir que el derecho a la intimidad es un derecho de la personalidad en virtud de que constituye un bien instrumental tendiente en garantizar la libertad individual de la persona necesaria para el desarrollo de su propia vida. En consecuencia, el derecho a la dignidad humana se establece como un presupuesto fundamental para el desarrollo de la personalidad y además se manifiesta como una parte esencial tanto del derecho a la libertad individual como a la dignidad humana (Pérez-Luño, 1986).



Empero lo mencionado, los derechos de la personalidad también pueden definirse como bienes que garantizan el disfrute a favor de cada persona de sus propias facultades intelectuales, físicas y morales y sin los cuales el individuo quedaría exento del goce de las principales garantías para asegurar su íntegro y efectivo desarrollo (Herrán Ortiz, 2003).

La privacidad es un derecho fundamental consagrado a nivel constitucional en los ordenamientos jurídicos. Todos tenemos derecho a la privacidad, pero también debemos ser responsables de nuestros actos, ya que somos los que tomamos decisiones. En tal sentido que hoy en día se puede considerar que la evolución del derecho a la privacidad se da con el fin de proteger la libertad de las personas para que puedan realizar acciones determinadas.

La privacidad es un derecho que atribuye facultades de control sobre la información personal comporta como correlato la atribución de un importante grado de autonomía personal, es por eso que como ciudadanos tenemos derecho a la privacidad y se debe exigir el cumplimiento de ese derecho, pero así mismo se debe de cumplir con los reglamentos fijados en las redes sociales al momento de hacer publicaciones.

La seguridad de los datos hace referencia a la forma en la cual las redes sociales ayudan a garantizar la confidencialidad, integridad y disponibilidad de los datos personales, la privacidad de los datos es la administración que se le da a los datos personales.

Ranciére (2004) sostiene que “últimamente, esos derechos, los derechos humanos aparecen verdaderamente vacíos, parece que no están en uso, y cuando no están en uso, se hace lo mismo que las personas caritativas hacen con las ropas viejas, son donados a los pobres” (p.306), esto quiere decir que pese a tener derechos no están siendo aplicado como corresponde, solo están tipificados en leyes, pero no se ejecutan como corresponde.

Por otro lado, se puede considerar que las TIC han generado un espacio tan rígido en todos sus niveles, por el contacto constante que se tiene con otras personas, creándose con esto la necesidad de publicar nuestra vida, se ha formado en las personas una costumbre de que se

tiene que hacer publicaciones de lo que se hace diariamente, puesto que sientan la sensación de que alguien está observando sus publicaciones.

El uso de datos sin permiso del dueño se ha convertido en una práctica cotidiana en el medio, cabe indicar que esto se puede estar dando debido al descuido de vigilar la privacidad, ya que no se han generado límites legales para las personas encargadas de manejar los datos personales. La privacidad de la información está amenazada por la curiosidad de las personas, hasta que no se tomen las respectivas medidas en el ámbito jurídico, en establecer leyes apegadas a la realidad informática en relación al uso de la tecnología, creando sistemas de seguridad en donde realmente se pueda sentir protegido el usuario cuando haga una publicación de sus datos personales, el mal uso de la información no tenga un fin y se seguirán vulnerando los derechos humanos de cada uno de las personas, puesto que no existirán leyes que lo respalde y haga valer sus derechos como persona.

Se suele decir que se tiene seguridad sin privacidad, pero no se puede tener privacidad sin seguridad, se debe de pensar en los datos que se consideren que están protegidos, es por eso que hoy en día se tienen que ser cauteloso en el uso de las redes sociales ya que estas no brindan la seguridad y privacidad que deben de tener los datos personales de los usuarios.

Los legisladores en la actualidad buscan la debida protección ante la vulneración de los datos y la intimidad de las personas, cuando se habla de vulneración de los datos personales se hace mención a que el ser humano como tal ha sufrido violación de sus datos. Gracias a la falta de conocimiento de parte de las personas, toca enfrentar a múltiples situaciones un poco complejas de superar, las cuales tienen estrecha vinculación directa con los medios tecnológicos.

### 2.1.3. Datos personales en redes sociales

La Directiva de la Unión Europea en su artículo 26 expresa que los datos personales son:

Toda aquella información sobre una persona identificada o identificable se considera identificable toda persona, directa o indirectamente, en particular mediante un

número de identificación o uno o varios elementos específicos, característicos de su identidad física, fisiológica, psíquica, económica, cultural o social (p.14)

El derecho a la protección de datos personales es un derecho de reciente consagración, el cual ha recibido varias denominaciones, derecho a la autodeterminación informativa, informática, intimidad informática, libertad, habeas data, data protección estos términos se utilizan de manera continua en la legislación, jurisprudencia o doctrina, su campo se sitúa en los derechos fundamentales, un derecho pasivo de primera generación donde proclama la no injerencia de terceras personas en la vida privada del individuo, derecho a la intimidad.

Hoy en día se puede considerar que en las redes sociales existe mucha información personal de usuarios que con facilidad pueden ser difundidas sin consentimiento, mediante los cuales se puede conocer datos privados de una persona, sin necesidad que este se de cuenta que su información está siendo manipulada, generándose con esto arbitrariedad en las redes sociales digitales, cabe manifestar que el uso de las diferentes redes sociales es básicamente compartir información, es del usuario tener las debidas precauciones de la cantidad de datos de la vida privada que se comparte en las redes, sin considerar lo perjudicial que esto puede ser, los datos personales son una expresión de privacidad e intimidad de cada persona, de tal manera que deben ser objeto de tutela.

Por otro lado, Cendejas, (2019) expresa que *“la protección de datos personales es un Derecho que consiste en ofrecer a los individuos los medios para controlar el uso ajeno de la información personal que les concierne”* (p.30). Se debe considerar al uso de las redes sociales como un espacio público, en donde no existe regulación forman, obteniéndose con esto una de las complicaciones en lo referente a medidas que se quieran tomar que permitieran la protección de datos personales, con lo cual se lograría la privacidad en los ciberespacios.

La legislación ecuatoriana está orientada a salvaguarda datos personales que se encuentren en personas que no son los dueños, es decir exige que se tenga cuidado con los datos personales que se recopilen, así mismo las leyes obligan cuidar y hacer posible la disposición de los datos por parte del titular en caso que este lo requiera. Las redes sociales digitales pese a tener su lógica de recopilación de datos, no cuentan con reglamentos específicos, es decir la

protección de los datos personales en las redes sociales digitales no tiene restricciones y obligaciones. Las personas deben hacer un buen uso de las redes sociales, lo más recomendable es que este uso sea restringido para las personas que hacen todo tipo de publicaciones sin medir las consecuencias.

Al hablar de protección de datos personales se hace referencia a la protección jurídica que se otorga a las personas respecto de la recogida, almacenamiento, utilización, transmisión y cualquier otra operación realizada sobre sus respectivos datos, destinada a que su tratamiento se realice con lealtad y licitud, de manera que no se vea afectado de manera indebida sus derechos constitucionales u otros de cualquier clase, que hagan que la persona se sienta desprotegida legalmente al momento de hacer publicaciones de sus datos personales.

#### 2.1.4. Legislación Española en la protección de datos personales.

La Legislación europea es un ejemplo para la mayoría de los Estados en lo relativo al marco europeo, mediante el Reglamento General de la Protección de Datos (RGPD) de la Unión Europea, considerada como una normativa sólida, la cual responde a las acciones tradiciones del entorno público o privado de la población o ciudadanos, el Reglamento General de la Protección de Datos de la Unión Europea tiene su contorno de ejecución en los aspectos materiales y territoriales.

En el aspecto material el reglamento debe ser aprovechado en el momento en que en la base de datos se administre de forma parcial o en su totalidad la información, esto significa que se tiene que descifrar mediante el reglamento el instante en que el titular de la información transfiera la administración de sus datos personales. El ámbito territorial se relaciona a la administración territorial de los datos personales, es necesario que el reglamento se lo aplique una vez que los datos personales sean objeto de una actividad de una institución responsable o encargada de la Unión Europea.

El RGPD dispone de un perímetro de aplicación, directamente para quienes viven o forman parte de la UE, así mismo en aquellos elementos en donde se actúe como donantes, ya sean estos de servicios o bienes, sin considerar que la obligación del pago se ejecute en territorio

perteneciente a la UE o en otro territorio que no sea parte de la UE, es decir que en la UE existen normativas que son aplicadas a la comunidad mediante tratados internacionales, con los cuales se puede exigir el desempeño de la medida presentada.

El RGPD de la UE, el mismo que es un referente significativo en lo referente a la protección de datos, teniendo en cuenta que su alcance aplica para los interventores o procesadores de datos cuyas sedes se localizan dentro de algunos de los países que son miembros de la UE y para organizaciones que se hallan por fuera de la UE, pero que procesan datos sus habitantes.

El Ecuador debe de tomar como modelo referente al RGPD de la UE, para crear un marco legal en donde se puedan crear medidas que permitan garantizar los derechos de los ciudadanos que hacen uso de las redes sociales.

El Reglamento General de Protección de Datos mas creciente de la Unión Europea es aún mas amplio y define una violación de la privacidad como la recuperación o divulgación ilegal de cualquier información relacionada con una persona, esa información puede incluir publicaciones en las redes sociales, direcciones de correo electrónico, datos bancarios, fotografías entre otros aspectos que pueden ser de interés personal. En dicho reglamento se ha estipulado que el incumplimiento del mismo puede generar una multa de hasta un 4% de los ingresos.

Es por eso que cada identidad define su propia política de privacidad de datos en donde por lo general se incluyen que datos pueden ser recopilados y cual será su utilidad, y quienes serán las personas que tendrán acceso a esos datos, de la misma manera se estipula si los datos podrán ser compartidos con terceros, o si se los puede almacenar y por qué tiempo.

#### 2.1.5. Legislación Ecuatoriana en la protección de datos

El derecho a la intimidad ciudadana está reconocida en los diferentes cuerpos legales de la legislación ecuatoriana, los mismos que se encuentran reglamentados, en tal sentido la Constitución de la República del Ecuador 2008 en su artículo 66, numeral 18, 19 20 y 21 reconoce y garantiza a las personas el derechos al honor y al buen nombre, a la protección de

datos de carácter personal, a la intimidad personal y familiar, y a la inviolabilidad y al secreto de la correspondencia física y virtual.

Mediante estos artículos se da aval y firmeza los derechos individuales y colectivos de cada uno de los seres humanos, dándole mayor énfasis al derecho de la intimidad, protección de información y la inviolabilidad, los cuales se testifican en las garantías expuesta en el cuerpo legal mencionado.

Por otro lado, el Código Orgánico Integral Penal del Ecuador en el artículo 178 estipula la violación a la intimidad en donde se establece que quienes hagan uso de la información sin consentimiento o la autorización legal del dueño, será sancionado con pena privativa de libertad de uno a tres años. Cabe señalar que estas normativas no son aplicables para aquellas personas que divulguen videos o grabaciones de audio en donde intervengan por si mismo, ni cuando la información sea de carácter publico según lo estipulado por la ley.

En COIP salvaguardar la intimidad y todo tipo de violación que deteriore a la persona o colectividad, por el hecho de haberse usado información personal, la misma que fue tomada sin aprobación del dueño de acuerdo a las excepciones previstas en la ley.

En tal sentido se puede expresar que hace falta que cada uno de los artículos estipulados en las diferentes normativas legales, sean ejecutados de manera permanente, lo cual permitirá que las personas u usuarios de las redes sociales que acostumbran hacer publicaciones de su vida personal y familiar, puedan sentirse respaldados por las leyes y normativas existentes, se debe de garantizar la seguridad privada de las personas, para que no se vulnere el derecho a la privacidad.

#### 2.1.6. El Estado en el Ciberespacio.

El ciberespacio es concebido como un lugar intangible caracterizado por grandes flujos de información que circula en la red de interconexión mundial, mediante el cual se accede de manera no física, solo en esencia. Es decir que es un espacio virtual creado por una red interconectada electrónicamente.

Sterling (2000) considera que el Ciberespacio “no es algo de nuestros días y tiene ya un cierto tiempo, que habría nacido concretamente cuando se inventó el teléfono” (p. 1), por lo tanto, el uso de las TIC no es nada nuevo, más bien en años anteriores se lo usaba, pero no como en la actualidad que las personas lo han tomado como una tradición de publicar todo lo que hacen.

El Estado Ecuatoriano debe establecer mecanismos legales que respalden a los usuarios de las redes sociales, para que sus datos no sean mal utilizados, la ciudadanía está siendo violentada sistemáticamente, sin que los organismos de defensa y seguridad tengan una repuesta ante esta situación que perjudica a cada uno de las personas que hace de forma permanente uso de las redes sociales.

Los sistemas de información están estrechamente conectados a algún tipo de red, lo que permite que los datos de las personas puedan ser vulnerados, debido a las diferentes aplicaciones que se tienen, imposibilitando el control de la información de los usuarios, el auge de la conectividad ha provocado desventajas en los usuarios, por lo que es necesario la implementación de políticas restrictivas de conectividad a la red, en donde las personas se sientan restringidos para hacer todo tipo de publicación.

Todas las personas tienen derecho de proteger sus datos personales al momento de hacer uso de los sistemas informáticos, pero cabe manifestar que estos sistemas en nuestro país no son seguros ni privados, por consiguiente, es necesario que el Estado garantice a la ciudadanía la seguridad en el Ciberespacio.

Se puede considerar que existe un vacío legal en la protección de datos en las redes sociales, puesto que el Ecuador no cuenta con una agencia de protección de datos la cual ponga en descubierto los casos de privacidad de diferentes tecnologías usadas para la seguridad personal de quienes hacen uso de las redes sociales, se debe destacar que la información de las personas en el internet debe aplicar los criterios de seguridad es decir confidencialidad, integridad, disponibilidad y no repudio.

Por consiguiente, es de mucha importancia que se brinde las garantías necesarias que las personas deben tener al momento de hacer publicaciones de sus datos personales en las redes sociales, los ecuatorianos como tal hacen un llamado al Estado para que se brinde las garantías fundamentales en el instante que los datos personales de un usuario de las redes sociales se han mal utilizados por terceras personas sin la respectiva autorización del dueño.

#### 2.1.7. Los dilemas y riesgos de la protección de datos en el ciberespacio.

El desarrollo tecnológico originado a raíz de la popularización y universalización del internet, así como de las aplicaciones digitales en los diversos sistemas operativos, han creado todo un nuevo esquema de posibilidades, alcances y desafíos. La actual generación esta inherentemente vinculada con las actitudes y aptitudes vinculadas a las nuevas tecnologías por lo que inevitablemente su información personal de una u otra manera se encuentra dentro del incalculable contenido de la red (García A. , 2011)

De acuerdo con el Club de Roma (Casique, 2017), entidad no gubernamental fundada en Roma que se ha encargado efectuar estudios multisistémicos e interdisciplinarios relativos a problemas suscitados a causa del crecimiento de la población y sus nuevas dinámicas. Las nuevas tecnologías de la información tan acelerado el cambio en todas las sociedades del mundo y han forzado a la humanidad para adaptarse a nuevas relaciones espacio temporales.

En consecuencia, un cambio radical y de carácter global requiere de un inteligente e intuitivo uso de los nuevos medios e instrumentos de la denominada sociedad de la información por lo tanto será necesario para años venideros la implementación de principios y derechos derivados de la transparencia y el acceso global a la información a fin de fomentar la solidaridad humana la comunicación global el acceso al conocimiento y la información y la creatividad interactiva (Casique, 2017),

El internet y uno de sus servicios más populares, las redes sociales, se han transformado con el transcurso del tiempo y en especial en la última década, llegándose a constituir en la base sustancial de una nueva economía, comercio, comunicación, educación y conocimiento



además han llegado a ser influyentes en las relaciones suscitadas en servicios financieros, instituciones y administraciones públicas e inclusive servicios de salud (Minguet, 2003).

De acuerdo con el Instituto Nacional de Estadísticas y Censos, en Ecuador el porcentaje de hogares con acceso a internet llegó al 45,5 por ciento en el año 2019 mientras que el porcentaje de personas que ingresan al internet al menos una vez al día aumento 2 puntos respecto al año 2018 llegando a ubicarse en el 86 por ciento. También resulta particularmente inquietante señalar que el porcentaje de personas que más utilizan el servicio de internet en función de su edad resultan ser menores de edad, para el año 2019 se estimó que más 60 por ciento de menores entre los 16 y 18 años usan el internet frecuentemente (Dávalos, 2020).

El innegable crecimiento de usuarios de internet a nivel tanto global, regional como local necesariamente implica una gran debilidad que se suscita en función de la creciente complejidad e interconexión de los sistemas que se encargan de transmitir la información. De esta forma, aparecen vulnerabilidades referentes principalmente a la seguridad de la información y justificadas en dos factores primordiales: el posible número de manejadoras responsables o atacantes y los medios disponibles (Singh, 2000).

El desarrollo de la tecnología permite a su vez el diseño de un sistema de protección que constantemente sigue evolucionando acorde a las nuevas exigencias y desafíos; sin embargo y en función del origen tecnológico del sistema de protección también se debe considerar al desarrollo del sistema de vulneración y/o ataque. Las vulneraciones al sistema informático son tópicos comunes en la actual sociedad de la información en la que vivimos y son originadas a causa de un ataque informático motivado por diversas circunstancias cómo puede ser: la intromisión en la intimidad de una persona, el ataque al buen nombre y reputación de un individuo, o la obtención de créditos y beneficios económicos (Davara, 2010).

Además de lo mencionado, resulta preciso resaltar que un ataque informático tendiente a sustraer ilícitamente información personal por lo general se dirige a: información delicada como identidad e ideología política social y religiosa; historial laboral, historial crediticio; usuarios y contraseñas necesarios para el acceso a diversos programas y plataformas digitales

de índole social, financiera, económica, académica, religiosa, laboral, entre otras; información sobre inclinación u orientación sexual, información referente al historial clínico; e, información de menores de edad incluyendo direcciones fotos y videos (Minguet, 2003).

Los cambios suscitados a raíz de la revolución tecnológica y la era de las tecnologías de la información y la comunicación han tenido un real impacto en el campo del derecho en virtud a los nuevos paradigmas, necesidades y desafíos derivados del uso de la tecnología, por lo cual han influido en todas sus ramas. De esta forma se puede observar diversas aplicaciones como: la incorporación del comercio electrónico que ha originado nuevos contratos y dinámicas en el derecho mercantil; la posibilidad de controlar en la red inmensos flujos de dinero de los que en muchas ocasiones resulta imposible rastrear su origen y licitud, creado verdaderos paraísos virtuales que se constituyen en desafíos para el derecho fiscal y penal (Del Peso Navarro, 2010).

Sin embargo, las problemáticas más graves y relativas al uso de las tecnologías se evidencian en el campo penal y de forma más específica en los delitos contra la integridad de las personas. Así y con el apareamiento de nuevas tipologías penales como el terrorismo a través del uso de la red, el tráfico de pornografía infantil, entre otros, merecen especial atención debido a que en muchos casos implican el uso de información personal (Del Peso Navarro, 2010).

En este contexto, la nueva realidad devenida con el desarrollo el ciberespacio tiene que ver con el delito informático y la aparición de los hackers o piratas informáticos, quienes son conocedores y expertos de los sistemas informáticos y de comunicaciones. La finalidad de los hackers radica en la comisión de delitos informáticos con el fin de obtener datos informaciones y conseguir de ellas un rédito económico. En este sentido, el delito también ha sabido mutar y adaptarse a las nuevas realidades en función del apareamiento de nuevas instituciones criminales y complejas redes delictivas especializadas en el ataque a sistemas informáticos, la defraudación a través de medios de comercio electrónico, la venta de información personal contenida en repositorios y bases de datos, entre otros (Ministerio de Defensa España, 2010).

De acuerdo con Marqués Graells (2005) los riesgos del internet se relacionan con: la información, la comunicación interpersonal, las actividades económicas, el funcionamiento del sistema informático y las adicciones.

<b>RIESGOS</b>	<b>CONSECUENCIAS</b>
Riesgos relacionados con la información	<ul style="list-style-type: none"> <li>● Acceso a información poco fiable y falsa</li> <li>● Pérdida de tiempo</li> <li>● Acceso de menores a información inapropiada y nociva</li> <li>● Acceso a información alusiva a conductas peligrosas o que hagan apología al delito</li> </ul>
Riesgos relacionados con la comunicación interpersonal	<ul style="list-style-type: none"> <li>● Bloqueo de servicio de correo electrónico</li> <li>● Recepción de spam</li> <li>● Recepción de mensajes ofensivos</li> <li>● Otorgamiento inconsciente o involuntario de información personal</li> <li>● Uso ilícito de información personal de terceros</li> <li>● Contacto con personas con malas intenciones</li> </ul>
Riesgos relacionados con actividades con repercusión económica	<ul style="list-style-type: none"> <li>● Estafas en servicios virtuales</li> <li>● Publicidad abusiva y malintencionada orientada a la compra</li> <li>● Uso de servicios mercantiles y comerciales de internet por parte de menores</li> <li>● Robo de información personal y especialmente información relativa a cuentas bancarias</li> <li>● Violación de propiedad intelectual (pirateo)</li> <li>● Negocios ilegales</li> <li>● Gastos desorbitados en páginas de internet</li> </ul>
Riesgos relacionados con el funcionamiento de la red Internet	<ul style="list-style-type: none"> <li>● Contagio de virus, malware u otros programas maliciosos</li> <li>● Espionaje cibernético a través de cookies o virus</li> <li>● Publicidad no deseada, spam</li> <li>● Robo de contraseñas e identificaciones de servidores de internet</li> </ul>
Riesgos relacionados con las adicciones	<ul style="list-style-type: none"> <li>● Adicción a redes sociales</li> <li>● Juegos con mecánicas enfocadas en la compra (loot boxes)</li> <li>● Adicción a juegos</li> <li>● Compras Compulsivas</li> <li>● Adicción a pornografía</li> </ul>

Actualmente, uno de los temas más discutidos y controversiales respecto a las redes sociales radica en los derechos de la intimidad y la privacidad de sus usuarios, ya que si bien, tanto la intimidad como la privacidad en la vida cotidiana se encuentran delimitadas en función del derecho que tiene toda persona a protegerse de cualquier intromisión. En las redes sociales estos conceptos no pueden ser aplicados con la misma efectividad y contundencia ya que en parte y debido a la naturaleza de las aplicaciones sociales y de interacción, que se basan en perfiles personales generados por sus propios usuarios, su protección resulta muchos más compleja. Este elemento ha dado lugar a un nivel sin precedentes de divulgación de información con carácter personal a manos de terceros que a través de mecanismos ilegítimos e ilegales implementados con el fin de obtener un beneficio económico (Roig, 2009).

Por otra parte, un tema que representa un enorme desafío para la sociedad actual tiene que ver con la ciberseguridad, el uso de las redes sociales y el derecho de los menores de edad para acceder a la sociedad de la información. En este contexto, dicho grupo humano se concibe como una de las principales víctimas y más un atractivo beneficio económico para los ciberdelincuentes debido a su natural relación con la tecnología. Delitos como la pornografía infantil, el acoso, el bullying, son sólo algunos de los peligros que tienen los menores en el ciberespacio, por lo que requieren ser considerados como sujetos especiales de protección por los ordenamientos jurídicos referentes a la protección de datos personales (Moral, 2013).

En este aspecto, el establecimiento de buenas prácticas y costumbres por parte de la familia y la comunidad pueden proteger al menor y a su integridad ante los riesgos que representa el uso del internet y las redes sociales (Astorga & Schmidt, 2019). Dichas prácticas pueden ser:

- la educación sobre las políticas de uso de redes sociales.
- el conocimiento de las medidas de seguridad y privacidad en cuentas o perfiles digitales.
- la delimitación en el contenido al que puede acceder un menor
- el acceso razonable y responsable al internet.

Sin perjuicio de los preceptos antes mencionados, es menester señalar que la tecnología y el internet se han constituido también como herramientas indispensables y necesarias para la educación de los menores y la creación de espacios de conocimiento a su favor, hecho que aún resulta más importante si se toma en cuenta la actual situación social y sanitaria suscitado a raíz de la propagación de la pandemia de COVID-19.

## 2.2. Uso de la Tecnología.

### 2.2.1. Impacto en la sociedad

A nivel mundial se procesa una gran cantidad de información digital mediante redes, el uso del internet para estas acciones es realizado por diversos grupos de personas, desde ciudadanos comunes, empresa privadas e instituciones públicas. La humanidad no había contado con un volumen tan amplio de información de modo tan sencillo de acceder a ella.

El internet es una de las herramientas digitales utilizadas por toda la sociedad, estableciéndose como un factor necesario en el desarrollo de diversas actividades del convivir diario en todos los aspectos de la vida de una persona, en otras palabras, se puede expresar que mediante el uso del internet se recopila, almacena y envía mucha información en tiempo real, permitiendo la intercomunicación con otras personas, es por esto que se ha convertido en un medio que facilita la información.

Castellls, (2016) expresa que:

Internet se está convirtiendo rápidamente en un medio de comunicación interactivo que va más allá del uso divertido pero superficial de los chats, el valor añadido del Internet en relación con otros medios es su capacidad para recombinar productos y procesos de información y comunicación en tiempo real o en un tiempo determinado (p. 36).

El uso de la tecnología ha ganado su espacio, especialmente las redes sociales, en donde como usuarios se ha interpretado mal su uso pensando que todo lo que hacemos debemos de publicar, exponiendo la intimidad personal y familiar, la cual en ocasiones se ve afectada. Se debe tener claro como cuando, donde y para qué se deben utilizar las redes sociales, la sociedad esta errada en el uso que se le esta dando a las redes sociales hoy en día.

Es herramienta tecnológica como son las redes sociales debe ser utilizada de manera adecuada, sin que la vida personal o familiar sea afectada, los datos personales no deben ser publicados, ya que no se puede saber cuál es la intención que tienen las demás personas que revisan las publicaciones que uno hace, cada persona es dueña de sus actos y se encuentra en libertad de hacer lo que a ella le parezca, pero se debe ser consciente que mucha de la información personal y familiar no se deben de hacer públicas.

La aparición de la tecnología trajo consigo problemas y afectaciones sociales puesto que no se han visto contemplados los derechos propios del ser humanos, como la privacidad, seguridad, autorías. En otras épocas para poder el Gobierno conocer la vida de un ciudadano debían ejecutar planes o mecanismos lentos para acceso a la información, enviando agentes policiales e investigando documentaciones del individuo, pues ahora toda la información que el gobierno debe conocer de un ciudadano se encuentra expuesta en una plataforma virtual a la cual se puede acceder facilitando así el trabajo de investigación, convirtiendo esto en un factor negativo que permite la vulneración del derecho a la privacidad de las personas, puesto que todos sus datos personales se encuentran expuestos para que terceras personas hagan uso de forma indebida sin la autorización del dueño

### 2.2.2. Realidad Virtual

Los seres humanos piensan que el uso de las redes sociales es para dar a conocer a todos cada una de las actividades que se realiza ya sean de índole personal, familiar, social, deportiva, económica, es decir todo y cada uno de los movimientos de la vida cotidiana son expuestos sin medir las consecuencias a las cuales se puede llegar por hacer el mal uso de las redes sociales con publicaciones de la vida personal.

La tecnología es un riesgo para la privacidad, puesto que al momento de hacer publicaciones de los datos personales se expone al público aspecto que solo son de importancia para el dueño, pero son estos errores los que han generado la vulneración de derechos de los usuarios de las redes sociales puesto que se limitan hacer publicaciones innecesarias en las redes sociales.

### 2.2.3. Redes sociales

Las redes sociales son medios que permiten la intercomunicación con otras personas a nivel internacional, nacional y local, en tal sentido Gómez & Otero (2016) expresan que:

Socioculturalmente las redes sociales son herramientas transformadoras de los hábitos ya que otorgan al ciudadano de a pie posibilidades de difundir ampliamente mensajes personales con objetivos profesionales, lúdicos organizativos, promocional o incluso político, aquí el concepto difusión conforma el hecho diferencial, ya que formas de relaciones anteriores, como el correo electrónico o la mensajería instantánea estaban fuertemente orientados a la comunicación uno a uno, en las redes sociales, en cambio quien emite el mensaje lo hace ante un público amplio (p.190).

La falta de protección jurídica o la limitación de una sola garantía jurisdiccional, son las causantes directas que exista la vulneración del derecho a la privacidad, puesto que no se brinda las garantías necesarias al usuario al momento de hacer publicaciones en las redes sociales, es necesario que se establezcan obligaciones y responsabilidades a los prestadores de los servicios de las redes sociales respecto a la protección de datos y privacidad que deben tener los usuarios.

En la actualidad se puede expresar que existe un vacío legal para la protección de datos y la intimidad en las redes sociales, ya que no se cuenta con una agencia de protección de datos, la misma que ponga en descubierto los casos de privacidad y diferentes tecnologías usadas para la seguridad de las personas. Cabe destacar que la información de las personas en el internet debe aplicar los criterios de seguridad, es decir, confidencialidad, integridad, disponibilidad, y no repudio, se debe brindar las garantías y seguridad necesaria a los usuarios

al momento de hacer publicaciones en las redes sociales, el Estado Ecuatoriano debe establecer leyes que permitan sancionar a aquellas personas que sin autorización obtienen información de otra y la hacen pública, afectando a la persona y a su respectiva familia.

Es de mucha importancia proteger la información confidencial y que esta no solo se limita a esa acción sino más bien a recoger y almacenar los datos que estén vinculados en la esfera de la intimidad para salvaguardar la privacidad de los usuarios, puesto que muchas personas son afectadas por el mal manejo de las redes sociales generando daños, los mismos que no están garantizados por la falta de protección jurídica o la limitación de una sola garantía jurisdiccional para aquello.

Algunas redes sociales se han visto en la obligación de adaptar políticas de privacidad en donde los usuarios deben de decidir quienes pueden ver sus publicaciones, es por eso que hoy en día muchas personas al momento de hacer publicaciones realizan sus ajustes en las publicaciones y otras por lo contrario publican sin tomar en cuenta las respectivas medidas que las redes sociales han realizado a favor de los usuarios para evitar la vulneración del derecho a la privacidad.

Los usuarios creen que las redes sociales son tableros de anuncios, álbum de fotos, publican lo mínimo que realizan diariamente convirtiéndose como algo habitual en los usuarios, pero no se toman las correcciones o cuidados necesarios al momento de hacer las publicaciones. Las redes sociales deben generar un marco regulatorio para la privacidad el cual debe estar basado en principios generales de protección de los datos personales, de tal manera que se debe de incluir el modelo europeo de protección de datos el cual está legalmente regularizado y brinda las garantías necesarias en relación a la protección de los datos personales.

Si los usuarios hacen consciencia del uso de las redes sociales, los casos de vulneración de derecho de privacidad, mermarían, así mismo la implementación de reglamentos aportaría de forma positiva en la protección de los datos personales de los usuarios de las redes sociales.

#### 2.2.4. Riesgos ventajas, desventajas y amenazas de la privacidad en las redes sociales



Una de las principales preocupaciones de los usuarios en el uso de las redes sociales es la privacidad que deben tener sus datos, la publicación de datos personales en las redes sociales ha sido causante de fenómenos como el “*spam o el phishing*” en donde se pone en riesgo la información personal, generándose con esto múltiples inconvenientes ya sean estos personales o familiares.

#### 2.2.4.1. Ventajas de las redes sociales

Entre las ventajas de las redes sociales se puede considerar que mediante esta se llega a conocer a diferentes personas ya sea internacional, nacional o local, sin trasladarse hasta ese lugar, es decir que las fronteras no son impedimento para conseguir la existencia de comunicación entre personas de todo el mundo. Por otro lado, la utilización de las redes sociales es el ahorro de tiempo y recursos para conseguir los mismos o mejores objetivos que los que se pueden lograr mediante los tipos de comunicación tradicional como el correo o el teléfono.

#### 2.2.4.2. Desventajas y amenazas de la privacidad en las redes sociales

Los usuarios de las redes sociales se ven expuesto a las amenazas y peligros del mundo de la tecnología, siendo una amenaza todo lo que invade el sistema operativo o software, lo que daña los programas del equipo, filtrándose la información de uso personal generándose afectaciones hasta graves al usuario.

Mediante el uso de las redes sociales pueden existe otros tipos de vulnerabilidad, puesto que el simple hecho de etiquetar a alguien en una imagen podría ser aprovechada por otras personas con el fin de sacar provecho o dañar la reputación de la persona etiquetada. El reconocimiento facial es otra amenaza, el cual se lleva a cabo a través del etiquetado de las imágenes el cual puede ser localizado.

Cabe mencionar que en el momento de cancelar las cuentas es falso que toda la información se elimina puesto que quedan los comentarios publicados en los perfiles, por lo que es

necesario que el usuario debe ser conocedor de estos escuetos mecanismos de seguridad que tienen estas plataformas.

Existen conductas asociadas a robos de identidad virtual en las redes sociales, y lo realizan creando perfiles distintos que en ocasiones son falsos y usados en las plataformas de la red falsa, asimismo han llegado a la suplantación de identidad virtual de otro usuario, dando como resultado una vulneración flagrante a la privacidad, teniendo como resultado la pérdida de la reputación, la existencia de suplantación o robo de identidad en redes sociales pueden provocar lo que se llama fuga de información ya que podría acceder a grupos privados o exclusivos.

#### 2.2.5. Lo público y privado en redes sociales

Las redes sociales generan que la mayor parte de los usuarios realicen publicaciones en donde se revelan datos personales o familiares los cuales pueden llegar a manos de personas que no tienen nada que ver con el círculo de familiares o de amigos. Al momento de ingresar a las redes sociales en ocasiones los usuarios lo hacen en sus hogares o en los Ciber lugares en donde se pueden exponer al robo de sus cuentas o clases, las cuales son utilizadas para sacar la información o hacer publicaciones que dañan la imagen del dueño de la cuenta.

Duaso (2011), considera:

Lo que es privado o público se difumina en ocasiones y lo que creemos que es compartido por un número muy reducido de amigos puede ser difundido a un número incalculable de personas durante un tiempo indefinido y de forma peligrosamente descontextualizada (196).

El mantener aspecto de la vida de forma privada en las redes sociales, puede ser importante que conservar la intimidad en la vida real, las diversas publicaciones que se hacen en las redes sociales son las expresiones de nuestra personalidad de manera virtual. Con el uso de redes sociales la privacidad pareciera estar constante en conflicto, la utilización de terceros de la

información publicada genera que las personas puedan ser de manera muy fácil identificadas generándose con esto mucho riesgo.

#### 2.2.6. La dimensión pública de una persona en redes sociales

El carácter público de una persona se establece con aquellas acciones que por voluntad propia y por razones de convivencia social e interés colectivo, se realizan con los demás miembros de la comunidad, pero dentro de ciertos límites que pueden ser además de las impuestas por el Estado, normas de convivencia que se basan en valores sociales y morales.

Para Garzón lo público es: *“la esfera de libre accesibilidad de los comportamientos y decisiones de las personas en sociedad, las cosas que pueden y deben ser vistas por cualquiera”* (2018, p. 6).

En este sentido se puede considerar que las redes sociales son extensiones del espacio público, en donde se puede tener una charla, ideas, opiniones, criterios, expresiones y discusiones, se comparte información de diversas temáticas, teniendo en cuenta los mecanismos y criterios digitales, mostrando el usuario de manera libre comportamientos y decisiones que pueden ser vistos por todas las personas que son sus seguidores y en ocasiones por aquellas que no son seguidores.

#### 2.2.7. La dimensión privada e íntima.

Los aspectos jurídicos permiten tener cierta claridad sobre lo que es privado en la vida de una persona, aunque las conceptualizaciones tomadas desde lo jurídico no son exhaustivas ni permanentes, pero proporcionan un piso mínimo para saber qué es la privacidad y la razón por la cual debe ser protegida y que esas razones se materialicen de manera formal en la constitución en forma de Derechos.

Para Escalante (2017) lo privado “no quiere decir secreto, público no quiere decir abierto de modo inmediato e indiscriminado, para cualquiera” (p.6-7), la diferencia entre lo público y lo

privados de las personas terminas siendo en cierto sentido relativa, puesto que cada persona decide a quienes hace partícipe de su espacio publico y que tipo de información personal comparte en lo público.

Por otro lado, las personas poseen espacios de privacidad e intimidad, ámbitos de completa autonomía, fuera de la vista de todo el público, donde se tiene la capacidad de autodeterminación sobre las decisiones que aquí se toman, sobre lo que se hace y se piensa sin dar cuentas a nadie, no hay nada que por su naturaleza pueda ser completamente privado, por decir los sueños pensamientos y emociones que tiene una persona, lo cual es algo completamente privado.

Para la existencia del Derecho a la privacidad, debe de asegurarse la autonomía de los individuos para decidir los alcances de su vida privada, a quién y de qué manera comparten voluntariamente información, para ello se debe limitar el alcance del Estado, a fin de no cometer intromisiones ilegales en la esfera de lo privado, esto se lo puede lograr mediante la creación de normativas legales, haciendo respetar el derecho que cada uno de las personas tienen, de lo contrario no se podrá gozar de un verdadero derecho a la privacidad.

Si como ciudadanos se hace publicaciones de datos personales, somos los encargados de realizar la respectiva seguridad para que la información no pueda ser manipulada por terceras personas.

#### 2.2.8. Estrategias para la privacidad

Para lograr obtener una protección a la privacidad en las redes sociales es necesarios que los usuarios:

- Piensen que la publicación de fotos en tiempo real puede perjudicar su visa personal y laboral.
- Por seguridad, sino por salud mental no se puede vivir al día en redes sociales.
- Mantener mucho cuidado al momento de dar una información por redes sociales.

- Proteger los datos personales
- Evaluar las actitudes y condiciones de privacidad de los contactos.
- Mantener en privado números de teléfono, dirección, correo.
- Revisar los ajustes de privacidad de las redes sociales.
- No utilizar almacenamiento público para compartir información privada.
- Utilizar aplicaciones de mensajería con cifrado o extremo a extremo.
- No hacer publicaciones innecesarias con información que son de interés personal.

#### 2.2.9. Principio de la autodeterminación informativa.

El Derecho a la Autodeterminación Informativa pertenece a la tercera generación de derechos, tiene su origen en la solidaridad y en la necesidad de cuidar derechos que se puedan vulnerar, varios autores sostienen que el Derecho a la Autodeterminación Informativa se encuentra supeditado a los derechos de primera generación, al derivarse del derecho político a la libertad de informarse.

Se debe tener en cuenta que los derechos de tercera generación gozan de nuevas condiciones para su ejercicio, diferentes a las contempladas por los de primera generación. Tanto han evolucionado, y tal es la importancia que han adquirido, que poseen instituciones exclusivas para su correcto desarrollo, la garantía constitucional asegura el control y acceso a la información: el Hábeas Data. Y no sólo se limita a garantías, sino que también origina leyes de protección de datos personales, e instituciones o agencias de protección de la información.

El reconocimiento a la protección de datos personales estipulado en el artículo 66, numeral 19 de la Constitución de la República del Ecuador (2008), estaría a su vez protegiendo al Derecho a la Autodeterminación Informativa, el sistema de protección de datos es la parte instrumental, mientras que la Autodeterminación Informativa es el derecho a tutelar en sí, sin embargo, no otorga un reconocimiento expreso a este derecho como elemento de la protección de datos personales.

En algunas jurisprudencias libertad informativa o autodeterminación informativa, es aquella facultad soberana que posee una persona a ser solo ella quien da a conocer la información, determinando que información suya puede estar en conocimiento de terceros, así mismo el titular es quien autoriza que información poder se anulada rectifica, actualizada, eliminada, pues el titular es quien sabe que información necesita estar en algún registro o banco de datos, dicha información tiene que ser fiscalizada por el titular, dando a conocer que tipi de información quiere que se conozca.

La Constitución de la Republica del Ecuador 2008, art. 92 Habeas data estipula: *“la persona titular de los datos podrá solicitar al responsable el acceso sin costo al archivo, así como la actualización de los datos, su rectificación, eliminación o anulación”*.

Uno de los fines de la autodeterminación es que el titular es aquella persona quien autoriza que datos pueden ser los necesarios que se encentren en un registro o banco de datos, esto implica que el individuo no solo puede conocer cuando él así lo deseen sus datos, también a tener acceso de su información. La autodeterminación se lo aplica aquellos datos que encontramos en ficheros automatizados cuyos datos afecten su intimidad, su honor constitucionalmente protegido, también constituye una parte importante del ámbito constitucional de la intimidad.

La responsabilidad tiene que ver con asumir las consecuencias de actos que se realizan conscientemente y intencionalmente, es la capacidad humana que permite poder escoger entre distintas opciones y actuar por medio de la libre voluntad, es decir es un valor que está en la conciencia de la persona que le permite reflexionar, administrar, orientar y valorar las consecuencias de sus actos siempre en el plano de lo moral.

En el proceso de autodeterminación se pueden identificar cinco aspectos que las personas deben seguir para regir sus vidas los cuales se enmaran en el respeto, poder de elección, autodirección y la oportunidad, cada uno de estos aspectos cumplen un rol especifico en le ser humano, es por ello que se les debe brindar la atención debida, puesto que lo contrario se podrá fracasar como persona.

Cabe recalcar que los únicos responsables de cada una de las acciones que se realizan diariamente son las personas, si ya se conoce o se sabe las consecuencias negativas que pueden generarse por publicaciones de datos personales en las redes sociales, entonces se debe de tener mucho cuidado en subir información que de pronto los demás no necesitan saber, pero ya queda en la responsabilidad de cada persona conservar su derecho a la privacidad.

### 3. Metodología

#### 3.1. TIPO DE INVESTIGACIÓN

En forma de premisa es menester efectuar algunas puntualizaciones sobre la ciencia y el conocimiento científico, preceptos íntimamente ligados ya que avanzan conjuntamente en medida en que se plantean y se resuelven los problemas, en otras palabras, la ciencia y el conocimiento adquieren nuevos matices y evolucionan gracias al apareamiento y entendimiento de nuevas dificultades. En la presente investigación relativa a la protección en las redes sociales, se pretende abarcar la problemática y paradigma de la protección de datos y su aplicabilidad en la realidad jurídica ecuatoriana, se debe tomar en cuenta que dicha premisa resulta en un tema relativamente novedoso en la legislación nacional ya que a la fecha actual Ecuador no posee una normativa específica y delimitada sobre esta temática (Unzain & Lazarte, 2018).

Para la investigación se utilizó el método científico intuitivo que consiste en la acción y efecto de intuir o percibir una idea o verdad de forma instantánea y directa, a través de este método se puede tener una primera respuesta, con carácter más espontáneo y original ante las problemáticas planteadas y al tratarse de la observación de fenómenos socio jurídicos y sus problemas derivados se puede utilizar dicho método de forma recíproca y complementaria con el método científico a fin de dar respuestas inmediatas. Construir hipótesis y/o respuestas que sean revisables y comprobables a través de teorías científicas (Ponce de León, 1996).

La investigación se desarrolla en base al denominado método analógico o comparativo, en este sentido Sartori considera que el método comparativo tiene como finalidad establecer una serie de similitudes y diferencias sobre un objeto, teoría o

problemática estudiada, debido a que la comparación está íntimamente ligada a la homogeneidad, es decir se compara a variables, hipótesis, conceptos o problemas que pertenecen al mismo género o especie. Por su parte al establecerse diferencias de igual forma se requiere de un trabajo sistémico y riguroso que permita visualizar, determinar las propiedades y los atributos de los preceptos a ser comparados (Gómez Díaz de León & León de la Garza, 2014).

De acuerdo con Sotomarino (2018) el Derecho Comparado indudablemente conlleva al análisis comparativo entre los diversos ordenamientos jurídicos e instituciones que conforman al derecho público y privado, en la medida en que cada rama, materia o institución establece los lineamientos o premisas que serán el sustento del análisis comparativo, de esta forma, el método comparativo aplicado en el derecho pone en evidencia y permite comprender las similitudes y diferencias, en el desarrollo de los ordenamientos jurídicos que se comparan considerando elementos como sus antecedentes, el contexto político, social y/o económico de su promulgación y demás elementos que los unen y separan. Con el análisis comparativo también se puede tomar en cuenta a elementos como la interpretación, aplicación de la norma, influencia ideológica, política o religiosa y la determinación de circunstancias específicas anexas a un determinado momento histórico para su elaboración, debate y promulgación.

En la presente investigación se pretende hacer una comparación jurídica- normativa basada en las siguientes premisas (Mancera Cota, 2008).

1. Sistema jurídico.
2. Sujeto-materia de comparación.
3. Delimitación Del nivel de comparación
4. Identificación de las similitudes y diferencias
5. Prueba de funcionalidad

En este sentido, la comparación se efectuó entre las legislaciones ecuatoriana y española, la materia de comparación comprende a todos los derechos y principios en torno a la protección de datos, el nivel de comparación se delimita en la protección de datos relativa la información personal encontrada en las redes sociales.



Para viabilizar la técnica del derecho comparado, la presente investigación se sustenta en la técnica de investigación documental que, a diferencia de la investigación de campo, se realiza a través del contacto directo con los documentos y el estudio de su contenido. En consecuencia, el método documental se sirve, de los libros y documentos como su principal fuente de información y resulta más viable en investigaciones relacionadas con el Derecho, debido a la complejidad y dificultad que representa el empleo de metodologías de campo para el estudio de esta rama de la ciencia (García, 2015).

La investigación desde el método de análisis documental, permite la recolección de información a través de fuentes documentales y bibliográficas como lo son: libros, periódicos, manuales, tratados, folletos, revistas, enciclopedias, artículos científicos, conferencias, entre otros. En el ámbito jurídico esta técnica reviste de una particular importancia puesto que permite el análisis de normas jurídicas tales como constituciones, leyes, tratados internacionales, ordenanzas, resoluciones, acuerdos, además permite el análisis de otras fuentes del derecho como es el caso de jurisprudencia de tribunales y pronunciamientos doctrinarios (Botero, 2003).

### 3.2. DESCRIPCIÓN DE LOS INSTRUMENTOS UTILIZADOS

Para la presente investigación se ha utilizado el instrumento de ficha de contenido que en la investigación resulta en una herramienta para concretar el método de análisis documental y viabilizar el estudio de derecho comparado. A través de la ficha de contenido el investigador puede recolectar los datos y obtener la información necesaria, además la ficha de contenido permite resumir la toda la información referente a un objeto de estudio determinado y provista de distintas fuentes bibliográficas (Villabella, 2020).

### 3.3. PRESENTACIÓN Y ANÁLISIS DE DATOS

En la presente investigación a fin de desarrollar el estudio de legislación comparada, se ha planteado dividirlo en dos grandes apartados. En primer lugar, se efectuó un análisis sobre el derecho humano a la protección de datos tanto en el sistema regional interamericano como europeo, y posteriormente se ha efectuado un análisis del derecho a la protección de datos en la Constitución ecuatoriana y española respectivamente. En segundo lugar, se elaboró un análisis más enfocado y más especificado en la protección de datos concerniente

a las redes sociales, tomando como comparativa a la legislación española y ecuatoriana, así como, los contextos en los que estos ordenamientos jurídicos se han desarrollado.

### 3.3.1. La protección de datos en el marco jurídico regional europeo e interamericano

<b>Sistema interamericano</b>	<b>Sistema Europeo</b>
<b>CONVENCIÓN AMERICANA SOBRE DERECHOS HUMANOS (1969)</b>	<b>CARTA DE LOS DERECHOS FUNDAMENTALES DE LA UNIÓN EUROPEA (2000)</b>
<b>Artículo 11. Protección de la Honra y de la Dignidad</b>	<b>Artículo 7. Respeto de la vida privada y familiar</b>
1. Toda persona tiene derecho tanto al respeto de su honra como al reconocimiento de su dignidad. 2. Ninguna persona puede ser objeto de injerencias arbitrarias o abusivas en la esfera de su vida privada, incluyendo a su familia, su domicilio o su correspondencia, tampoco puede ser víctima de ataques ilegales a su honra o reputación. 3. Toda persona tiene derecho a la protección de la ley contra dichas injerencias o ataques.	Todas las personas tienen el derecho al respeto de su vida privada y familiar, así como de su domicilio y de sus comunicaciones.
	<b>Artículo 8. Protección de datos de carácter personal</b>
	1. Toda persona tiene derecho a la protección de sus datos de carácter personal 2. Los datos personales serán tratados tratarán de modo leal, para fines concretos y sobre la base del consentimiento del titular o en virtud del mandato de la ley. Además, toda persona tiene derecho a acceder a sus datos recogidos incluyendo a la rectificación. 3. El respeto de estas normas quedará sujeto al control de una autoridad con carácter independiente.

En el ámbito interamericano como europeo, gran parte del mérito sobre la constitucionalización de los derechos fundamentales lo tienen los diversos instrumentos y declaraciones sobre derechos humanos. Por una parte, la Convención Americana de Derechos

Humanos promulgada por la Organización de Estados Americanos es el máximo referente de derechos humanos en el sistema interamericano y en su artículo 11 habla sobre la protección de los datos personales de forma indirecta y asociada con derechos como la intimidad personal y familiar, la honra y el buen nombre.

En contraposición el sistema europeo y específicamente el sistema jurídico de la Unión Europea contempla un mayor desarrollo con relación al derecho a la autodeterminación informativa y a la protección de datos. De acuerdo con autores como Murillo de la Cueva (2011) esto se debe a que la comunidad europea ha afianzado a la tutela de estos derechos a partir de un diálogo entre los legisladores internacionales, comunitarias, estatales y además se ha establecido una doctrina y una jurisprudencia en común. Finalmente es menester resaltar que, en el sistema europeo, el derecho a la protección de datos es autónomo respecto del derecho a la intimidad personal y familiar.

### 3.3.2. La protección de datos en la Constitución ecuatoriana y española

<b>Constitución ecuatoriana (2008).</b>	<b>Constitución española (1978)</b>
<p>Art. 66.- Se reconoce y garantizará a las personas:</p> <p>19. El derecho a la protección de datos personales, que incluye el acceso y la decisión sobre información y datos de este tipo, así como su correspondiente protección. La recolección, archivo, procesamiento, distribución o difusión de estos datos o información que requerirán de la autorización del titular o del mandato de la ley.</p>	<p>Artículo 18. 1.- Se garantiza el derecho al honor, a la intimidad personal y familiar y a la propia imagen. 2. Inviolabilidad de domicilio. Ninguna persona podrá entrar o registrarse sin consentimiento del titular o resolución judicial, salvo en caso de un delito flagrante. 3. Se garantiza el secreto de las comunicaciones y, en especial, de las aquellas relacionadas a servicios postales, telegráficos y telefónicos, salvo resolución judicial. 4. La ley limitará el uso de la informática e información con el fin de garantizar el honor, la intimidad personal y familiar de los ciudadanos y su pleno ejercicio de sus derechos.</p>

En Ecuador, en virtud de la promulgación de la Constitución de 2008, se ha efectuado un importante avance en el reconocimiento del derecho a la protección de datos personales. En la sección denominada derechos de libertad que hacen alusión a un conjunto de derechos fundamentales de primera, segunda e inclusive tercera generación constantes el artículo 66, específicamente en el numeral 19, se hace el reconocimiento al derecho a la protección de datos de carácter personal, que incluye a la garantía de su protección, el acceso a la información de carácter personal, privado y/o reservado exclusivamente bajo el consentimiento del titular, y otros elementos de suma importancia como su recolección, procesamiento, distribución, difusión o archivo que de igual manera opera bajo el consentimiento previo de su titular o ante el mandato expreso de la ley.

Si bien, comúnmente se asocia al derecho de la protección de datos con la libertad de expresión o el derecho al honor, la honra y la intimidad, el constitucionalismo ecuatoriano lo establece como un derecho autónomo que si bien es su parte de los derechos de libertad inherentes a toda persona no se desprende de los derechos fundamentales antes mencionados. Razón por la cual, en el texto de la Carta Magna ecuatoriana la protección de datos tiene su propio numeral, además si se toma en cuenta al artículo 40 ibidem este derecho se concatena como otros como por ejemplo la movilidad y la migración.

Además de lo señalado, el sistema jurídico ecuatoriano para defender y garantizar el derecho a la protección de datos, prevé dentro de la propia Constitución a las denominadas garantías jurisdiccionales específicamente a la garantía del Habeas Data que se encuentra amparada en el artículo 92 ibidem y que permite a toda persona por sus propios derechos o a través de un representante legitimado para tal efecto, tener el derecho a conocer y acceder a los documentos, bancos de datos, datos genéticos, informes, archivos u otro tipo de información que contenga sus datos personales y se encuentran en entidades públicas como privadas, incluyendo información personal, patrimonial. Conjuntamente, esta garantía le permite al ciudadano conocer el uso destinado para sus datos personales, así como su finalidad, origen y tiempo de vigencia, entre otros.

Por su parte, el constitucionalismo español reconoce el derecho a la protección de datos partiendo del reconocimiento del derecho a la intimidad que sirve como una protección del individuo y sus derechos ante el intervencionismo y arbitrariedad de los poderes públicos.

En otras palabras, la Constitución española en su artículo 18 acoge de forma amplia al contenido referente al derecho a la intimidad reconociendo algunas facetas de la misma como lo son: la intimidad domiciliaria, la libertad y confidencialidad de las comunicaciones privadas o también conocidas como secretos de comunicaciones, el propio honor y la limitación en el uso de la información a favor del honor, la intimidad a nivel personal y familiar y el ejercicio de otros derechos de toda persona.

Otra diferencia plausible entre el sistema constitucional ecuatoriano y español en cuanto al tratamiento y garantía del derecho a la protección de datos, radica en la existencia de una garantía jurisdiccional propiamente dicha que a diferencia del caso ecuatoriano. En España, la tutela de las libertades y derechos reconocidos por la Constitución se podrán sustanciar ante el Tribunal Constitucional a través del recurso de amparo.

Si se toma en cuenta a la Sentencia 254-1993 del 20 de julio (1993), todos los derechos y libertades fundamentales vinculan a los diversos poderes del Estado, razón por la cual, si bien no existe un recurso exclusivo para el garantizar el acceso a la información a manos de su titular, los derechos consagrados por la Constitución española incluyendo por supuesto a los establecidos en el artículo 18 deben ser protegidos por todos los poderes públicos y en última instancia por el Tribunal Constitucional a través del Recurso de Amparo.

Adicionalmente y a fin de relacionar de mejor manera al derecho a la protección de datos con el derecho a la intimidad, en la sentencia antes mencionada el Tribunal señala que el uso de la informática se encuentra limitada con respecto al honor y la intimidad personal, en virtud de ello y tomando en cuenta a los diversos convenios internacionales suscritos por España, en especial el Convenio de Protección de Datos Personales de 1981, la protección de la intimidad de los ciudadanos requiere que estos puedan conocer la existencia y los rasgos de aquellos archivos, ficheros o ubicaciones en donde la administración pública conserve los datos con carácter personal que les concierne (Sentencia 254/1993, de 20 de julio (BOE núm. 197), 1993)

Aunque existen otras normativas concernientes al tema como lo es la Ley de Comercio Electrónico, Ley Orgánica de Telecomunicaciones, Ley Orgánica de Comunicación y Ley del Sistema Nacional de Registro de Datos Públicos (Ordóñez, 2017) se hace necesario una ley con carácter general que otorgue un tratamiento al amparo de información personal que sea

restringida y/o reservada y garantice de manera efectiva el cumplimiento de los derechos digitales.

3.3.3. Directrices normativas referentes a la protección de datos en el marco regional interamericano y europeo.

<b>Sistema Interamericano</b>	<b>Sistema europeo</b>
<p data-bbox="229 539 842 584"><b>Comité Jurídico Interamericano (2012)</b></p> <p data-bbox="229 607 842 775"><b>Propuesta de declaración de principios de privacidad y protección de datos personales en las América</b></p> <p data-bbox="229 797 842 1671">Doce principios: 1) propósitos legítimos y justos de datos recolectados 2) claridad y consentimiento en los fines de la recopilación 3) pertinencia y necesidad de la información 4) uso limitado y apegado a sus fines 5) deber de confidencialidad o prohibición de divulgación 6) protección y seguridad contra accesos no autorizados 7) fidelidad de la información 8) acceso y corrección de la información 9) protección acorde con información sensible 10) responsabilidad las del encargado de la información 11) flujo transfronterizo de información 12) publicidad de las excepciones a los principios</p>	<p data-bbox="849 539 1447 640"><b>Parlamento Europeo, Consejo de la Unión Europea (2016)</b></p> <p data-bbox="849 663 1447 775"><b>Reglamento (Ue) 2016/679 Del Parlamento Europeo Y Del Consejo</b></p> <p data-bbox="849 797 1447 1895">CAPÍTULO I. disposiciones generales; CAPÍTULO II. principios; CAPÍTULO III. derechos del interesado (transparencia, información, acceso, rectificación, supresión o derecho al olvido, limitación del tratamiento, portabilidad de datos y oposición); CAPÍTULO IV. responsable del tratamiento y encargado del tratamiento; CAPÍTULO V. transferencias de datos personales a terceros países u organizaciones internacionales; capítulo vi. autoridades de control independientes; CAPÍTULO VII. cooperación y coherencia; CAPÍTULO VIII. recursos, responsabilidad y sanciones; CAPÍTULO IX. disposiciones relativas a situaciones específicas de tratamiento; capítulo x. actos delegados y actos de ejecución; CAPÍTULO XI. disposiciones finales.</p>

La Propuesta de Declaración de Principios de Privacidad y Protección de Datos Personales en las Américas se constituye como el mayor esfuerzo efectuado por la Organización de Estados Americanos y específicamente por el Comité Jurídico Interamericano para lograr una legislación regional uniforme y especializada en la protección y tratamiento de la información personal.

De acuerdo Recio (2015) el informe que fundamenta a la Propuesta, se fundamenta en el derecho a la privacidad y se basa en definiciones como el honor personal, la dignidad, la libertad de expresión y la protección de datos personales. No obstante, el sistema interamericano al no tener que tratar con directivas ni reglamentos en materia de protección de datos, tampoco prevé el establecimiento de un ordenamiento jurídico que sea de obligatoria observancia para los Estados parte, esto en virtud de que el informe únicamente sirve como referente para que cada país miembro de la Organización de Estados Americanos en medida de lo posible y siguiendo su propia experiencia y necesidades adecue un ordenamiento jurídico interno que permita la protección y privacidad de los datos personales.

Los Principios no se constituyen como un contenido exhaustivo y extenso ya que únicamente sirven de orientación para futuras propuestas legislativas o inclusive para la aplicación normativa y regulatoria a nivel local. En otras palabras, la Propuesta de Declaración de Principios de Privacidad y Protección de Datos Personales en las Américas únicamente es una guía para la elaboración, adopción e implementación de medidas que permitan adecuar un alto nivel de protección y garantía en la privacidad y en el derecho a la protección de datos personales.

Por otro lado, el Reglamento de la Unión Europea 2016/679 principalmente se refiere a la protección de los datos personales y a su libre circulación, este instrumento ha permitido unificar y modernizar la normativa de los países adscritos a la Unión Europea en materia de protección de datos. El objeto de este Reglamento radica en permitirle a los ciudadanos un mejor control de sus datos personales, así como regular a las empresas para aprovechar de forma más eficiente las oportunidades que brinda el mercado digital basado en la información personal, bajo parámetros como la reducción de la burocracia y una mayor confiabilidad hacia el consumidor (Redacción Noticias jurídicas, 2016).

Es necesario señalar que en el ámbito europeo también existe otra normativa referente exclusivamente a la protección de datos en ámbitos judiciales y penales, con el fin

de asegurar que la información de víctimas y delincuentes o sospechosos se encuentre protegida mente protegida en dentro del contexto de una investigación criminal.

La diferencia más clara que se observa entre las Propuestas elaboradas por el Comité Jurídico Interamericano y el Reglamento de la Unión Europea radican en su obligatoriedad y vigencia para los Estados partes, en este contexto el Reglamento en su artículo 99 señala que, al entrar en vigor posterior a los 20 días de su publicación en el Diario Oficial de la Unión Europea, será obligatorio en todo su contenido para cada uno de los Estados miembros. Además de lo señalado, el Reglamento se constituye como un verdadero ordenamiento jurídico ya que presenta artículos que hacen alusión a principios rectores, garantías hacia derechos fundamentales, derechos, deberes y obligaciones y un contenido regulatorio con respecto a los derechos salvaguardados. El reglamento al ser obligatorio en su aplicación en todos los países de la Unión Europea, por consecuencia demanda que cada uno de estos implemente y promulgue un ordenamiento jurídico interno especializado en la protección de datos y armónico en su contenido con el mencionado Reglamento.

#### 3.3.4. La protección de datos en el ordenamiento jurídico interno de Ecuador y España

Ecuador	España
<p><b>Ley Orgánica de Protección de Datos Personales (2021)</b></p> <p><b>Contenido principal:</b> información personal consiste en: datos biométricos personales y únicos, datos genéticos, datos personales, datos personales crediticios; datos referentes a género, etnia, cultura, religión, ideología política, antecedentes judiciales, condición migratoria, inclinación sexual; datos sobre salud; establecimiento de un sistema de protección de datos personales; Categorización especial de datos personales; obligaciones del responsable frente a la seguridad de datos personales; transferencia</p>	<p><b>Ley Orgánica 3/2018 Protección de Datos de Carácter Personal y Garantía de Derechos Digitales (2018)</b></p> <p><b>Contenido principal:</b> control de datos de las personas fallecidas a manos de sus familiares; consentimiento de los menores de edad (14- en adelante) en el tratamiento de sus datos personales; tratamiento de información por mandato de la ley, interés público o ejercicio de poderes públicos; protección de los menores en el ciberespacio; categorización de los datos; bloqueo de los datos en caso de supresión o error; designación y obligaciones de los</p>



<p>o comunicación internacional de datos personales; garantía de los derechos digitales entre los que se destaca: <i>derechos en entornos digitales; derecho a la educación digital; derechos de acceso; derecho a la rectificación, derecho a la cancelación, derecho a la oposición; derecho de eliminación; derecho a la información</i></p>	<p>delegados de protección de datos; régimen sancionador; garantía de los derechos digitales entre los que se destaca: <i>derecho a la actualización de informaciones en medios de comunicación digitales; derecho a la intimidad y uso de dispositivos digitales en el ámbito laboral; derecho a la seguridad digital; derecho a la educación digital; derecho a la desconexión digital laboral; derecho a la intimidad ante la utilización de dispositivos de videovigilancia, geolocalización y/o grabación en el trabajo; derecho al olvido y portabilidad en servicios de redes sociales.</i></p>
-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

En Ecuador recientemente se aprobó la Ley Orgánica de Datos Personales, cuyo objetivo radica en el garantizar el ejercicio del derecho a la protección de datos personales a través de un ordenamiento jurídico especializado en el que se incluyen novedades como: el derecho al acceso y decisión sobre la información de los datos de carácter personal, el derecho al olvido, la clasificación de la información contenida en repositorios archivos y referente a datos personales de una persona, entre otros. Además, con la normativa se ha planteado la creación de un ente de control que se denomina Superintendencia de Protección De Datos Personales y cuya función principal será el implementar un Registro Nacional de datos para su protección.

Sin dudas la Ley de Protección de Datos Personales se ha constituido como un importante avance efectuado por el gobierno ecuatoriano en el desarrollo del derecho a la protección de datos y a los derechos digitales como es el caso de la educación. Esta normativa cumple cabalidad con los 12 principios emanados desde la Propuesta de Declaración de Principios de Privacidad y Protección de Datos Personales de las Américas efectuada por el Comité Jurídico Interamericano; sin embargo, dicha ley se encuentra enfocada en la protección de información de datos personales y su regulación, en virtud de lo cual temas

como los derechos digitales, derechos en el ciberespacio o internet y específicamente los derechos en redes sociales, aún no han sido tomados en cuenta para su tratamiento.

En contraparte la Ley Orgánica 3/2018 referente a la Protección de Datos de Carácter Personal y Garantía de Derechos Digitales de España, se visualiza como una adaptación del Reglamento de la Unión Europea 2016/679 en el ordenamiento jurídico interno de España, al igual que la normativa ecuatoriana su finalidad radica en la garantía de la protección de datos personales; no obstante, esta norma jurídica presenta un mayor desarrollo en lo referente a la garantía de los derechos digitales y entre sus principales innovaciones y diferencias frente a la norma ecuatoriana están: el derecho a la seguridad digital, la protección de menores de edad en internet, el derecho a la rectificación en internet, el derecho a la actualización de información en medios digitales de comunicación, el derecho a la intimidad y uso de dispositivos digitales en el ámbito laboral, así como, el derecho a la intimidad frente al uso de dispositivos de grabación y geolocalización en el ámbito del trabajo, el derecho al olvido en las búsquedas de internet y sobre todo, el derecho al olvido y la portabilidad en los servicios de redes sociales o análogos.

### 3.3.5. Protección de datos y redes sociales

<b>Ecuador</b>	<b>España</b>
<b>Ley Orgánica de Protección de Datos Personales (2021)</b>	<b>Ley Orgánica 3/2018 Protección de Datos de Carácter Personal y Garantía de Derechos Digitales (2018)</b>
<b>Art. 24.- Ejercicio de derechos.</b> - los proveedores de servicios de la sociedad de la información y el conocimiento, entre otros y dentro del ámbito de sus relaciones, están obligados a proveer información y capacitación relacionadas con el uso y tratamiento responsable, adecuado y seguro de datos personales de niñas, niños y adolescentes.	<b>Menores y redes sociales. - Artículo 84.</b> los representantes procurarán que los menores de edad hagan un uso equilibrado y responsable los servicios de la sociedad de la información; la utilización o difusión de información personal de menores en las redes sociales puede implicar un delito. <b>Artículo 92.-</b> cualquier persona natural o

jurídicas que desarrolle actividades donde participen menores debe garantizar su intimidad, en publicaciones o difusiones de sus datos personales a través de servicios de la sociedad de la información. **Artículo 97.**- se impulsarán políticas para que los menores hagan un uso equilibrado y responsable de los dispositivos digitales, redes sociales y los servicios de la sociedad de la información.

**Rectificación en Internet. - Artículo 84.** los responsables de redes sociales y servicios deben adoptar mecanismos para posibilitar el ejercicio del derecho de rectificación ante contenidos que vulneren derechos derivados del honor y la intimidad incluyendo a los medios de comunicación digitales.

**Olvido en búsquedas de Internet. - Artículo 93.** derecho de toda persona para que los motores de búsqueda en Internet eliminen de las listas de sus resultados de búsqueda a información personal cuando fuere inadecuada, inexacta, no pertinente, no actualizada o excesiva. **Artículo 94.** derecho de toda persona previa solicitud para suprimir sus datos personales publicados en redes sociales y servicios de la sociedad de la información equivalentes. En el caso de ser publicados por terceros podrán ser suprimidos por solicitud, siempre y cuando sean inadecuados, inexactos, no pertinentes, no actualizados o excesivos. En el caso de

	<p>menores de edad únicamente se requiere de la solicitud.</p> <p><b>Portabilidad. - Artículo 95.</b> los usuarios de redes sociales y servicios de la sociedad de la información pueden recibir y transmitir los contenidos que hubieran facilitado a los prestadores de esos servicios.</p> <p><b>Derecho de familiares de fallecido. - Artículo 96.</b> Los familiares o personas legitimadas por el fallecido podrán decidir sobre el mantenimiento o eliminación de sus perfiles personales en redes sociales o servicios similares.</p>
--	-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

Tomando como punto de partida la premisa de que la Ley Orgánica de Protección de Datos Personales ecuatoriana es una norma jurídica nueva y recientemente aprobada en mayo de 2021, dicha normativa tiene como objetivo principal la protección de los datos personales, el acceso y decisión sobre esta información y el establecimiento de mecanismos de regulación. Si bien, el artículo 2 de dicha ley señala que su ámbito de aplicación comprende a la protección de datos personales que se encuentran contenidos en cualquier tipo de soporte automatizado o no, dicho ordenamiento jurídico no hace mayor alusión a las redes sociales, a los derechos digitales, al internet entre otros y sólo se limita a mencionar a la sociedad de la información como aquel derecho constitucional que fundamenta la promulgación de la ley mencionada.

En el artículo 24 ibidem, se hace alusión a los proveedores de servicios de la sociedad de la información como uno de los tantos y diversos entes, que, dentro del ámbito de sus relaciones, están obligados a proveer información y capacitación con relación al uso y tratamiento de datos personales de menores de edad. Este elemento se constituye como la única alusión que la ley antes referida hace sobre la protección de datos personales en el ámbito de redes sociales.

A más lo mencionado, también vale la pena resaltar a un proyecto de ley que regula los actos de odio y discriminación en redes sociales e internet que en su tiempo fue promovido por el ex presidente Rafael Correa, dicho proyecto tenía como objetivo regular a las empresas proveedoras de servicios de comunicaciones, telemáticas, plataformas de internet o tecnologías de similar naturaleza, con el fin de dar tratamiento al contenido o información que pudiera llegar a constituirse en actos de discriminación o de odio, para lo cual, estos proveedores debían elaborar informes trimestrales sobre los reclamos efectuados por usuarios y referentes a dicho contenido. No obstante, es necesario señalar que el proyecto también ha sido criticado por considerarse excesivamente regulatorio y restrictivo ya que su contenido incidiría negativamente en las potencialidades y funcionalidades que ofrece el internet y traslada la responsabilidad del control social a terceros que sin tener que ver con estos actos compartirían responsabilidad por el mero hecho de prestar el servicio de internet (Legaltech, 2017).

En el contexto de la legislación española, la Ley Orgánica 3/2018 de Protección de Datos Personales y Garantías de los Derechos Digitales al tener un contenido más especializado en cuanto a los derechos digitales en relación con la legislación ecuatoriana. Si hace referencias claras sobre los derechos relativos a la protección de datos en ámbitos como la redes sociales, el internet y los servicios de la sociedad de la información, esto se debe en parte a la influencia del Reglamento General de Protección de Datos de la Unión Europea de 2016, norma en la que ya se habla sobre ciertas obligaciones que deben prestar los proveedores de servicios relativos a redes sociales como lo son: la aplicación de un diseño que garantice mayor seguridad a los datos personales, la información sobre el destino de los datos personales provistos por el usuario y la solicitud del consentimiento específico y explícito sobre el destino de los datos personales.

En este contexto la Ley Orgánica 3/218 establece una serie de obligaciones y compromisos por parte del proveedor de servicios relativos a las redes sociales en materia de protección de datos como: informar al cliente sobre la finalidad y utilización de sus datos personales, fines legítimos del uso de la información, mismos que deben estar sustentados en una base legal, la identidad del responsable del tratamiento de la información, los derechos de los interesados, entre otros de conformidad como lo señala su artículo 11.

A diferencia de la norma ecuatoriana en dónde no se establece claramente a un responsable y su/s delegado/s para la protección de datos, en la legislación española más concretamente en el artículo 34 se habla de la designación de un delegado por parte de los responsables y encargados del tratamiento de datos personales, que entre otros casos comprende a las entidades que explotan redes y presten servicios de comunicación electrónica y a los prestadores de servicios de la sociedad de la información.

Finalmente, los principales ejes sobre los cuales la normativa española garantiza la protección de datos y la privacidad de las personas en el ámbito de las redes sociales tienen que ver con el derecho al olvido, la protección de menores de edad, el derecho de los familiares de un fallecido con relación a su información en redes sociales, la desconexión digital.

## 4. Conclusiones

### **PRIMERA**

La protección de datos es un derecho que se deriva de la protección a la intimidad, el buen nombre y la honra de toda persona, consecuentemente la protección de datos se concibe como toda información de índole personal y que hace alusión al estado de salud, historial laboral, cuentas bancarias, datos de identificación personal y especialmente la información sensible que incluye la ideología política y/o religiosa, inclinación sexual, entre otras. La protección de dicha información demanda a toda persona natural y/o jurídica que posee información de terceros en archivos, repositorios o bancos de datos, su sigilo, salvo el caso de existir autorización del titular de la información o un requerimiento previsto en la ley.

### **SEGUNDA**

El tratamiento de los datos se refiere a uso que un ente responsable efectuó sobre los datos personales de terceros que posea, y se sustenta en principios como la licitud o su uso bajo el amparo de una norma jurídica; lealtad o el tratamiento ético y legal de la información; transparencia o la rendición de cuentas al titular de la información respecto a su uso, fines, riesgos y consecuencias; minimización o la adecuación, pertinencia y limitación de los datos en función de sus fines; exactitud y actualización de los datos; limitación a su conservación o la necesidad de eliminar los datos o destruirlos una vez hayan alcanzado su finalidad; y, la integridad y confidencialidad en la protección de datos a fin de garantizar su seguridad.

### **TERCERA**

En Ecuador la protección de datos esta normada en la Ley Orgánica de Protección de Datos Personales recientemente aprobada el 26 de mayo de 2021 y cuyo objeto radica en salvaguardar al ejercicio del derecho a la protección de datos personales, que

principalmente incluye elementos como su acceso, decisión referente a información o datos de carácter personal y principalmente su protección. No obstante, el ordenamiento jurídico mencionado en su ámbito de aplicación de forma general habla sobre el tratamiento de datos personales contenidos en cualquier tipo de soporte, sea este automatizado o no.

#### **CUARTA**

El ámbito de aplicación generalizado de la Ley Orgánica de Protección de Datos Personales ecuatoriana se constituye como la principal diferencia entre dicha norma y otros ordenamientos jurídicos más avanzados e integrales como es el caso de la Ley Orgánica 3/2018 de España. Entre los elementos que denotan menor desarrollo entre el ordenamiento jurídico de protección de datos ecuatoriano y español, se enmarcan los derechos digitales, la protección en el ciberespacio y principalmente la protección en redes sociales.

## Referencias bibliográficas

### **Bibliografía básica**

Agencia Española de Protección de Datos e Instituto Nacional de Tecnologías de la Comunicación. Estudio sobre la privacidad de los datos personales y la seguridad de la información en las redes sociales online. [www.inteco.es/Estudios/est\\_red\\_sociales\\_es](http://www.inteco.es/Estudios/est_red_sociales_es) 2009

Bertomeu, A. (2012) Redes sociales: conversaciones multipantalla, riesgos y oportunidades. En Pérez, L., Nuez, C., Pozo, J. del (coords.), Tecnologías de la Comunicación. Jóvenes y promoción de la salud. (pp. 116-150). Logroño: Gobierno de La Rioja. Disponible en [http://drojnet2.eu/f/drojnet2/docs/Tecnologias\\_de\\_la\\_Comunicacion\\_Jovenes\\_y\\_Promocion\\_de\\_la\\_Salud.pdf](http://drojnet2.eu/f/drojnet2/docs/Tecnologias_de_la_Comunicacion_Jovenes_y_Promocion_de_la_Salud.pdf)

Bobbio, Norberto. (2019, p.11). Liberalismo y democracia. (2da Ed). México: Fondo de cultura Económica.



Campuzano Tomé, H. Vida privado y datos personales. Madrid: Tecnos (2015)

Carrillo Salcedo, J. A. El convenio europeo de derechos humanos. Madrid: Tecnos. 2016.

Conde Ortiz, C. (2015). La protección de datos personales: un derecho autónomo con base en los conceptos de intimidad y privacidad. Madrid: Dykinson.

Costas, J. (2010). Seguridad Informática. Madrid, España: RA-MA Editorial.

Dávora Rodríguez, M. A. (2015) Anuario de derecho de las tecnologías de la información y las telecomunicaciones (TIC). España: Dávora & Dávora

Duaso Calés, Rosario. (2011, p.195-210) “Redes sociales y vida privada: una ecuación posible” en Protección de datos personales en las Redes Sociales Digitales: en particular de niños y adolescentes Memorándum de Montevideo, Gregorio, Carlos G. y Ornelas, Lina compiladores. México: IFAI.

Escalante Gonzalbo, Fernando. (2017, p.6-40) El derecho a la privacidad., Serie de cuadrenos de transparencia No.6. México: Instituto Federal de Acceso a la Información y Protección de Datos

Esquinas Valverde, P. (2010). Protección de datos personales en la Policía Europea. Valencia: Universidad de Granada & Tirant lo blanch

Garzón Valdés, Ernesto (2018, p.6-17) Lo íntimo, lo privado y lo público, Serie de cuadrenos de transparencia No.6. México: Instituto Federal de Acceso a la Información y Protección de Datos.

Gregorio C. (2011, p. 42-73) “Impacto y evolución de las redes sociales digitales: libertades y derechos” en Protección de datos personales en las Redes Sociales Digitales: en particular de niños y adolescentes Memorándum de Montevideo, Gregorio, Carlos G. y Ornelas, Lina compiladores, México: IFAI.

Mattelart, A. (2015) Historia de la sociedad de la información. (G. Multigner, Trad.) París: Le Découverte.

Palomar Olmeda, A. (20017, 9-40). Los derechos personales en el ámbito de la protección de datos. *Revista española de protección de datos* (No.2),

Pfeiffer, María Luisa. (2019, p.19). "Derecho a la privacidad. Protección de los datos sensibles". en *Revista Colombiana de Bioética*, enero-Junio, <http://www.redalyc.org/articulo.oa?id=189217248002>

Rancière, J. (2004) "Who is the Subject of the Rights of Man?" en *The South Atlantic Quarterly* 103 (2/3): 297-310.

Ruiz de Querol, R., & Buira, J. (2017) *La sociedad de la información*. Barcelona: UOC.

### **Bibliografía complementaria**

Agencia Española de Protección de Datos. Recomendaciones a usuarios de Internet. Recuperado 8 de marzo de 2012 de [www.agpd.es/guia\\_recomendaciones\\_Internet](http://www.agpd.es/guia_recomendaciones_Internet)

Busquet, J., Ballano, S., Aranda, D., Medina, A., Morón, S. y Ruano, L. (2010). El uso de las TIC y la brecha digital entre adultos y adolescentes. Encuentros y (des)encuentros en la escuela y en el hogar. Web de II Congreso Internacional Asociación española Investigación de la Comunicación (Málaga) (<http://www.aeic2010malaga.org/upload/ok/387.pdf>)

Castells, Manuel. (2016, p.36-38). *La Sociedad Red: una visión global*. (1º.ed.). Madrid, España: Alianza Editoria.

Carpizo Mc-Gregor, J., & Gómez-Robledo Verduzco, (2014, 9-63). A. Los tratados internaciones, el derecho a la información y el respeto a la vida privada. *Boletín mexicano de Derecho Comparado* (Año XXXIII, No. 97),

- Comella, C. Privacy e nuove tecnologie. En P. Cendon,(2016, p. 1241- 1259). Libera circolazione e protezione dei dati personali. Trattati, Tomo II Milano: Giuffrè.
- Del Peso Navarro, E, & Ramos González, M.A. (2014). La seguridad de los datos de carácter personal (2ª ed.). Madrid: Díaz de Santos.
- Del Castillo Vázquez, I.-C. (2017). Protección de datos: cuestiones constitucionales y administrativas. El derecho a saber y la obligación de callar. Madrid: Thomson-Civitas.
- Domínguez González, L. A. (2010). Transparencia de la información pública y protección de datos personales: un balanceo necesario. Madrid: Servicio de Publicaciones de la Facultad de Derecho de la Universidad Complutense de Madrid.
- Duaso Calés, Rosario. (2011, p.195-210). “Redes sociales y vida privada: una ecuación posible” en Protección de datos personales en las Redes Sociales Digitales: en particular de niños y adolescentes Memorándum de Montevideo, Gregorio, Carlos G. y Ornelas, Lina compiladores. México: IFAI.
- Escalante Gonzalbo, Fernando. (2017) El derecho a la privacidad., Serie de cuadrenos de transparencia No.6. México: Instituto Federal de Acceso a la Información y Protección de Datos
- Gómez Navajas, J. (2015) La protección de los datos personales. Un análisis desde la perspectiva del Derecho Penal. Navarra: Thomson-Aranzadi.
- Gregorio, Carlos. & Ornelas,(2011). Lina Compiladores. Protección de datos personales en las Redes Sociales Digitales: en particular de niños y adolescentes Memorándum de Montevideo. México: IFAI.
- Lasagabaster Herrarte, I. (2014). Convenio europeo de derechos humanos. Madrid: Thomson-Civitas.

Sterling (2000, p.1) Ciberespacio <https://www.ciencia-ficcion.com/>

Suñé Llinás, E. (2017). Tratado de Derecho Informático (2ª ed., Vol. I Introducción y protección de datos personales). Madrid: Servicio de Publicaciones de la Facultad de Derecho de la Universidad Complutense de Madrid e Instituto Español de Informática y Derecho.

Real Academia Española (2001), Diccionario de la lengua española. 22.ª ed. Madrid: España

### **Legislación citada**

Asamblea Nacional República del Ecuador. (2014a). Código Orgánico Integral Penal. Año I-No 180. Retrieved from [https://tbinternet.ohchr.org/Treaties/CEDAW/Shared Documents/EQU/INT\\_CEDAW\\_ARL\\_ECU\\_18950\\_S.pdf](https://tbinternet.ohchr.org/Treaties/CEDAW/SharedDocuments/EQU/INT_CEDAW_ARL_ECU_18950_S.pdf)

Constitución de la República del Ecuador. Publicada en el Registro Oficial No. 449, del 20 de octubre de 2008. Ecuador

Declaración Universal de Derechos Humanos

Ley Orgánica No. 5/1992. Ley Orgánica de Regularización del Tratamiento Automatizado de los Datos de Carácter Personal. Publicada en el Boletín Oficial del Estado No. 262, del 31 de octubre de 1992. España.

LO 15/1999, de 13 de diciembre, de Protección de Datos de carácter Personal (LOPD).

## Listado de abreviaturas

COIP	Código Orgánico Integral Penal
LOPD	Ley Orgánica de Protección de Datos
RGPD	Reglamento General de la Protección de Datos
UE	Unión Europea

## Anexo A. REGLAMENTO

# Reglamento General de la Protección de Datos

1

(Actos legislativos)

## REGLAMENTOS

### 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)

(Texto pertinente a efectos del EEE)

EL PARLAMENTO EUROPEO Y EL CONSEJO DE LA UNIÓN EUROPEA,

Visto el Tratado de Funcionamiento de la Unión Europea, y en particular su artículo 16,

Vista la propuesta de la Comisión Europea,

Prevía transmisión del proyecto de texto legislativo a los Parlamentos nacionales,

Visto el dictamen del Comité Económico y Social Europeo <sup>(1)</sup>,

Visto el dictamen del Comité de las Regiones <sup>(2)</sup>,

De conformidad con el procedimiento legislativo ordinario <sup>(3)</sup>,

Considerando lo siguiente:

- (1) La protección de las personas físicas en relación con el tratamiento de datos personales es un derecho fundamental. El artículo 8, apartado 1, de la Carta de los Derechos Fundamentales de la Unión Europea («la Carta») y el artículo 16, apartado 1, del Tratado de Funcionamiento de la Unión Europea (TFUE) establecen que toda persona tiene derecho a la protección de los datos de carácter personal que le conciernan.
- (2) Los principios y normas relativos a la protección de las personas físicas en lo que respecta al tratamiento de sus datos de carácter personal deben, cualquiera que sea su nacionalidad o residencia, respetar sus libertades y derechos fundamentales, en particular el derecho a la protección de los datos de carácter personal. El presente Reglamento pretende contribuir a la plena realización de un espacio de libertad, seguridad y justicia y de una unión económica, al progreso económico y social, al refuerzo y la convergencia de las economías dentro del mercado interior, así como al bienestar de las personas físicas.
- (3) La Directiva 95/46/CE del Parlamento Europeo y del Consejo <sup>(4)</sup> trata de armonizar la protección de los derechos y las libertades fundamentales de las personas físicas en relación con las actividades de tratamiento de datos de carácter personal y garantizar la libre circulación de estos datos entre los Estados miembros.

<sup>(1)</sup> DO C 229 de 31.7.2012, p. 90.

<sup>(2)</sup> DO C 391 de 18.12.2012, p. 127.

<sup>(3)</sup> Posición del Parlamento Europeo de 12 de marzo de 2014 (pendiente de publicación en el Diario Oficial) y posición del Consejo en primera lectura de 8 de abril de 2016 (pendiente de publicación en el Diario Oficial). Posición del Parlamento Europeo de 14 de abril de 2016.

<sup>(4)</sup> Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre de 1995, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos (DO L 281 de 23.11.1995, p. 31).

Anexo B

## Código Orgánico Integral Penal

red%20Documents/ECU/INT\_CEDAW\_ARL\_ECU\_18950\_S.pdf

### 30 -- Suplemento -- Registro Oficial N° 180 -- Lunes 10 de febrero de 2014

exclusión o preferencia en razón de nacionalidad, etnia, lugar de nacimiento, edad, sexo, identidad de género u orientación sexual, identidad cultural, estado civil, idioma, religión, ideología, condición socioeconómica, condición migratoria, discapacidad o estado de salud con el objetivo de anular o menoscabar el reconocimiento, goce o ejercicio de derechos en condiciones de igualdad, será sancionada con pena privativa de libertad de uno a tres años.

Si la infracción puntualizada en este artículo es ordenada o ejecutada por las o los servidores públicos, será sancionada con pena privativa de libertad de tres a cinco años.

#### PARÁGRAFO SEGUNDO Delito de odio

**Artículo 177.- Actos de odio.-** La persona que cometa actos de violencia física o psicológica de odio, contra una o más personas en razón de su nacionalidad, etnia, lugar de nacimiento, edad, sexo, identidad de género u orientación sexual, identidad cultural, estado civil, idioma, religión, ideología, condición socioeconómica, condición migratoria, discapacidad, estado de salud o portar VIH, será sancionada con pena privativa de libertad de uno a tres años.

Si los actos de violencia provocan heridas a la persona, se sancionará con las penas privativas de libertad previstas para el delito de lesiones agravadas en un tercio. Si los actos de violencia producen la muerte de una persona, será sancionada con pena privativa de libertad de veintidós a veintiséis años.

#### SECCIÓN SEXTA Delitos contra el derecho a la intimidad personal y familiar

**Artículo 178.- 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 video, 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.

No son aplicables estas normas para la persona que divulgue grabaciones de audio y video en las que interviene personalmente, ni cuando se trata de información pública de acuerdo con lo previsto en la ley.

**Artículo 179.- Revelación de secreto.-** La persona que teniendo conocimiento por razón de su estado u oficio, empleo, profesión o arte, de un secreto cuya divulgación pueda causar daño a otra persona y lo revele, será sancionada con pena privativa de libertad de seis meses a un año.

**Artículo 180.- Difusión de información de circulación**

Es información de circulación restringida:

1. La información que está protegida expresamente con una cláusula de reserva previamente prevista en la ley.
2. La información producida por la Fiscalía en el marco de una investigación previa.
3. La información acerca de las niñas, niños y adolescentes que viole sus derechos según lo previsto en el Código Orgánico de la Niñez y Adolescencia.

**Artículo 181.- Violación de propiedad privada.-** La persona que, con engaños o de manera clandestina, ingrese o se mantenga en morada, casa, negocio, dependencia o recinto habitado por otra, en contra de la voluntad expresa o presunta de quien tenga derecho a excluirla, será sancionada con pena privativa de libertad de seis meses a un año.

Si el hecho se ejecuta con violencia o intimidación, será sancionada con pena privativa de libertad de uno a tres años.

La persona que, en ejercicio de un servicio público, sin la debida autorización o fuera de los casos contemplados legalmente; o que con una orden falsa de la autoridad pública; o que con el traje o bajo el nombre de uno de sus agentes, viole un domicilio o lugar de trabajo, será sancionada con pena privativa de libertad de tres a cinco años.

En la violación de domicilio se presume que no hay consentimiento del dueño o de la dueña o su encargado cuando no están presentes en el acto que constituya la infracción.

#### SECCIÓN SÉPTIMA Delito contra el derecho al honor y buen nombre

**Artículo 182.- Calumnia.-** La persona que, por cualquier medio, realice una falsa imputación de un delito en contra de otra, será sancionada con pena privativa de libertad de seis meses a dos años.

No constituyen calumnia los pronunciamientos vertidos ante autoridades, jueces y tribunales, cuando las imputaciones se hubieren hecho en razón de la defensa de la causa.

No será responsable de calumnias quien probare la veracidad de las imputaciones. Sin embargo, en ningún caso se admitirá prueba sobre la imputación de un delito que hubiere sido objeto de una sentencia ratificatoria de la inocencia del procesado, de sobreseimiento o archivo.

No habrá lugar a responsabilidad penal si el autor de calumnias, se retractare voluntariamente antes de proferirse sentencia ejecutoriada, siempre que la publicación de la retractación se haga a costa del responsable, se cumpla en el mismo medio y con las

Anexo C

## Constitución Política del Ecuador

ecu\_const.pdf

LEY ORGANICA ELECTORAL, CODIGO DE LA DEMOCRACIA, Arts. 3

Capítulo sexto  
Derechos de libertad

**Art. 66.-** Se reconoce y garantizará a las personas:

1. El derecho a la inviolabilidad de la vida. No habrá pena de muerte.
2. El derecho a una vida digna, que asegure la salud, alimentación y nutrición, agua potable, vivienda, saneamiento ambiental, educación, trabajo, empleo, descanso y ocio, cultura física, vestido, seguridad social y otros servicios sociales necesarios.
3. El derecho a la integridad personal, que incluye:
  - a) La integridad física, psíquica, moral y sexual.
  - b) Una vida libre de violencia en el ámbito público y privado. El Estado adoptará las medidas necesarias para prevenir, eliminar y sancionar toda forma de violencia, en especial la ejercida contra las mujeres, niñas, niños y adolescentes, personas adultas mayores, personas con discapacidad y contra toda persona en situación de desventaja o vulnerabilidad; idénticas medidas se tomarán contra la violencia, la esclavitud y la explotación sexual.
  - c) La prohibición de la tortura, la desaparición forzada y los tratos y penas crueles, inhumanos o degradantes.
  - d) La prohibición del uso de material genético y la experimentación científica que atenten contra los derechos humanos.
4. Derecho a la igualdad formal, igualdad material y no discriminación.
5. El derecho al libre desarrollo de la personalidad, sin más limitaciones que los derechos de los demás.
6. El derecho a opinar y expresar su pensamiento libremente y en todas sus formas y

CONSTITUCION DE LA REPUBLICA DEL ECUADOR 2008 - Página 29  
eSilec Profesional - www.lexis.com.ec



No imprimas este documento a menos que sea absolutamente necesario



manifestaciones.

7. El derecho de toda persona agraviada por informaciones sin pruebas o inexactas, emitidas por medios de comunicación social, a la correspondiente rectificación, réplica o respuesta, en forma inmediata, obligatoria y gratuita, en el mismo espacio u horario.
8. El derecho a practicar, conservar, cambiar, profesar en público o en privado, su religión o sus creencias, y a difundirlas individual o colectivamente, con las restricciones que impone el respeto a los derechos.

El Estado protegerá la práctica religiosa voluntaria, así como la expresión de quienes no profesan religión alguna, y favorecerá un ambiente de pluralidad y tolerancia.

9. El derecho a tomar decisiones libres, informadas, voluntarias y responsables sobre su sexualidad, y su vida y orientación sexual. El Estado promoverá el acceso a los medios necesarios para que estas decisiones se den en condiciones seguras.
10. El derecho a tomar decisiones libres, responsables e informadas sobre su salud y vida reproductiva y a decidir cuándo y cuántas hijas e hijos tener.



luri=CELEX:32018R1725

con independencia del tipo de información transmitida;

- 26) «equipo terminal»: un equipo terminal tal como se define en el artículo 1, punto 1, de la Directiva 2008/63/CE de la Comisión <sup>(18)</sup>.

## CAPÍTULO II PRINCIPIOS GENERALES

### *Artículo 4*

#### **Principios relativos al tratamiento de datos personales**

1. Los datos personales serán:
  - a) tratados de manera lícita, leal y transparente en relación con el interesado («licitud, lealtad y transparencia»);
  - b) recogidos con fines determinados, explícitos y legítimos, y no serán tratados ulteriormente de manera incompatible con dichos fines; de acuerdo con el artículo 13, el tratamiento ulterior de los datos personales con fines de archivo en interés público, fines de investigación científica e histórica o fines estadísticos no se considerará incompatible con los fines iniciales («limitación de la finalidad»);
  - c) adecuados, pertinentes y limitados a lo necesario en relación con los fines para los que son tratados («minimización de datos»);
  - d) exactos y, si fuera necesario, actualizados; se adoptarán todas las medidas razonables para que se supriman o rectifiquen sin dilación los datos personales que sean inexactos con respecto a los fines para los que se tratan («exactitud»);
  - e) mantenidos de forma que se permita la identificación de los interesados durante no más tiempo del necesario para los fines del tratamiento de los datos personales; los datos personales podrán conservarse durante períodos más largos siempre que se traten exclusivamente con fines de archivo en interés público, fines de investigación científica o histórica o fines estadísticos, de conformidad con el artículo 13, sin perjuicio de la aplicación de las medidas técnicas y organizativas apropiadas que impone el presente Reglamento a fin de proteger los derechos y libertades del interesado («limitación del plazo de conservación»);
  - f) tratados de tal manera que se garantice una seguridad adecuada de los datos personales, incluida la protección contra el tratamiento no autorizado o ilícito y contra su pérdida, destrucción o daño accidental, mediante la aplicación de medidas técnicas u organizativas apropiadas («integridad y confidencialidad»).
2. El responsable del tratamiento será responsable del cumplimiento de lo dispuesto en el apartado 1 y capaz de demostrarlo («responsabilidad proactiva»).

### *Artículo 5*

#### **Licitud del tratamiento**

1. El tratamiento solo será lícito si se cumple al menos una de las siguientes condiciones:
  - a) el tratamiento es necesario para el cumplimiento de una función realizada en interés público o en el ejercicio de potestades públicas conferidas a las instituciones y organismos de la Unión;
  - b) el tratamiento es necesario para el cumplimiento de una obligación legal aplicable al responsable del tratamiento;
  - c) el tratamiento es necesario para el cumplimiento de un contrato en el que el interesado es parte o para la aplicación a petición de este de medidas precontractuales;
  - d) el interesado ha prestado su consentimiento para el tratamiento de sus datos personales para uno o varios fines específicos;
  - e) el tratamiento es necesario para proteger intereses vitales del interesado o de otra persona física.