UNIVERSIDAD CATÓLICA DE CUENCA

UNIVERSIDAD CATÓLICA DE CUENCA

Comunidad Educativa al Servicio del Pueblo

UNIDAD ACADÉMICA DE CIENCIAS SOCIALES

CARRERA DE DERECHO

TÍTULO:

Análisis del marco legal de la protección de datos personales frente a las aplicaciones móviles en Ecuador.

TRABAJO DE TITULACIÓN PREVIO A LA OBTENCIÓN DEL TÍTULO DE ABOGADO

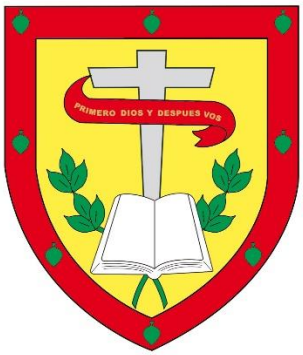
AUTOR: FELIPE JOSUE ANDRADE ARIAS

DIRECTOR: DR. JUAN MARTÍNEZ ALBORNOZ

CUENCA - ECUADOR

2024

DIOS, PATRIA, CULTURA Y DESARROLLO



UNIVERSIDAD CATÓLICA DE CUENCA

Comunidad Educativa al Servicio del Pueblo

UNIDAD ACADÉMICA DE CIENCIAS SOCIALES

CARRERA DE DERECHO

TÍTULO

ANÁLISIS DEL MARCO LEGAL DE LA PROTECCIÓN DE DATOS PERSONALES FRENTE A LAS APLICACIONES MÓVILES EN ECUADOR

TRABAJO DE TITULACIÓN PREVIO A LA OBTENCIÓN DEL TÍTULO DE ABOGADO

AUTOR: FELIPE JOSUE ANDRADE ARIAS

DIRECTOR: DR. JUAN MARTÍNEZ ALBORNOZ

CUENCA - ECUADOR

2024

DIOS, PATRIA, CULTURA Y DESARROLLO

Universidad Católica de Cuenca

DECLARATORIA DE AUTORÍA Y RESPONSABILIDAD

Declaratoria de Autoría y Responsabilidad

Felipe Josue Andrade Arias portador(a) de la cédula de ciudadanía Nº **0150747335**. Declaro ser el autor de la obra: **"Análisis del marco legal de la protección de datos personales frente a las aplicaciones móviles en Ecuador"**, sobre la cual me hago responsable sobre las opiniones, versiones e ideas expresadas. Declaro que la misma ha sido elaborada respetando los derechos de propiedad intelectual de terceros y eximo a la Universidad Católica de Cuenca sobre cualquier reclamación que pudiera existir al respecto. Declaro finalmente que mi obra ha sido realizada cumpliendo con todos los requisitos legales, éticos y bioéticos de investigación, que la misma no incumple con la normativa nacional e internacional en el área específica de investigación, sobre la que también me responsabilizo y eximo a la Universidad Católica de Cuenca de toda reclamación al respecto.

Cuenca, **09 de mayo de 2024**

F: .....

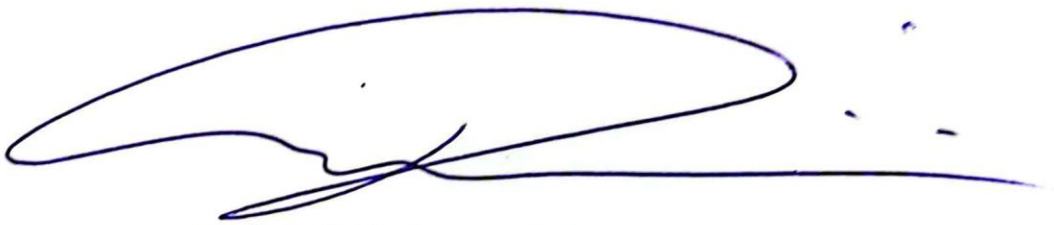
Felipe Josue Andrade Arias

C.I. **0150747335**

Universidad Católica de Cuenca

CERTIFICO

Certifico que el presente Trabajo de Investigación desarrollado por el Estudiante, FELIPE JOSUE ANDRADE ARIAS con numero de cedula, 0150747335, con el tema **"ANÁLISIS DEL MARCO LEGAL DE LA PROTECCIÓN DE DATOS PERSONALES FRENTE A LAS APLICACIONES MÓVILES EN ECUADOR"**, bajo mi supervisión.



Dr. Juan Pablo Martínez Albornoz

Tutor

Dedicatoria

Las acciones inefables que contiene el aprendizaje dentro de nuestra mente, la forma en la que llevamos el conocimiento y la impartimos a las demás personas es lo mejor que puede existir en cada uno de nosotros demostrando que el conocimiento es una fuente de sabiduría tanto para nosotros como para quien se la enseñamos e impartimos construyendo pensamientos mucho más críticos en nuestro entorno sin dejarnos llevar por trivialidades que afecten nuestros objetivos principales y enfocados por lo cual, dedico esta tesis a quienes fomentaron mi crecimiento académico y personal para poder cumplir un objetivo más y lograr mucho más a partir de culminar este periodo tan efímero.

No obstante, agradezco y dedico a Nathaly Arévalo y a cada lector o lectora con la finalidad de, impartir el conocimiento adquirido por mi persona e ilustrar una nueva perspectiva del Derecho para ilustrar nuevas ideas en su análisis y demostrar un cambio inter-personal como interpersonal.

Agradecimiento

Mi vida y conocimientos adquiridos están agradecidos pues, he conocido y e transformado en base a la experiencia adquirida el conocimiento y lo que me falta por descubrir que, e entablado conexiones con todo aquello que me rodea, mi convicción es tal que marcó un antes y un después de mi estadía como estudiante es por la cual que, agradezco a todos aquellos que forman y formaron parte de mi etapa y por las nuevas etapas que se encaminaran una vez culminado mi formación como estudiante.

Resumen

En la presente investigación de analiza la vulneración de los datos personales frente al uso de aplicaciones móviles en Ecuador específicamente Facebook, Instagram y WhatsApp debido a que los usuarios y administradores de estas aplicaciones móviles se han envuelto en controversias afectado y vulnerando derechos fundamentales reconocidos en la Constitución de la república como en el análisis del Marco Legal de la Protección de Datos Personales.

Los resultados de esta investigación se evidencian que los titulares de su información desconocen por completo el tratamiento indebido que genera terceras personas y administradores ante la adquisición de datos sensibles y su mala utilización en la sociedad actual determinado que no existen sanciones leves ante el mal uso de los datos y su tratamiento inequívoco sé que estima existen en los parámetros de seguridad de las aplicaciones mencionadas, la divulgación de esta información de carácter personal el adquirir dichos datos sensibles genera en terceras personas atracciones positivas como negativas para el tratamiento al que destine la persona que accedió a la información.

En el presente trabajo se sustentó, entre otras técnicas de investigación, mediante las cuales tenemos la documentación bibliográfica, encuestas, exploración sobre la protección de datos personales en Ecuador frente aplicaciones móviles generando así un énfasis en lo cualitativo y cuantitativo frente a la violación de este derecho fundamental que garantiza y protege el Estado.

***Palabras clave**: datos sensibles, Facebook, Instagram, WhatsApp, datos personales.*

Abstract

This research analyzes the violation of personal data in Ecuador concerning using mobile applications, specifically Facebook, Instagram, and WhatsApp. Users and administrators of these mobile apps have been involved in controversies that affect and violate fundamental rights recognized in the country's Constitution and in the analysis of the Legal Framework for Personal Data Protection.

The results of this research show that data owners are completely unaware of the improper handling by third parties and administrators when acquiring sensitive data and its misuse in current society. It is determined that there are no mild sanctions for the misuse of data and its unequivocal treatment, which are estimated to exist in the security parameters of the mentioned applications. The disclosure of this personal information when acquiring such sensitive data generates positive and negative reactions in third parties for the treatment intended by the person who accessed the information.

This study used various research techniques, including bibliographic documentation, surveys, and exploration of protecting personal data in Ecuador regarding mobile applications. This approach emphasizes qualitative and quantitative aspects concerning violating this fundamental right that the State ensures and protects.

***Keywords**: Sensitive data, Facebook, Instagram, WhatsApp, personal information.*

Índice

Introducción.

Viendo la necesidad de demostrar la vulneración de los datos personales frente a las aplicaciones móviles en Ecuador con el objetivo de mejorar el marco legal de la Ley de Protección de datos Personales en base a un análisis exhaustivo sobre la violación de los derechos relacionados con la persona y su información en las redes sociales por tal razón existen tres aplicaciones móviles esenciales las cuales son: Facebook; Instagram; WhatsApp; pioneras en la adquisición de la información las cuales facilitan el acceso de las publicaciones y mensajes en que terceras personas realizan acciones incorrectas al tratar los datos personales.

El uso de las redes sociales como: Facebook; Instagram y WhatsApp, en la sociedad no se brinda el uso correcto al momento de tratar la información personal como por ejemplo la adquisición ilegitima de datos sensibles en la aplicación de WhatsApp.

La problemática planteada en la presente investigación se describe de qué manera la Ley de Protección de Datos Personales toma el control del uso adecuado de las aplicaciones móviles en Ecuador como por ejemplo, Facebook, Instagram y WhatsApp.

Para finalizar esta investigación se ha logrado determinar la vulneración del derecho a la protección de datos personales y derechos que engloba el mismo permitiendo conocer el uso inadecuado que realizan los usuarios y administradores al momento de publicar datos sensibles en las aplicaciones mencionadas esperando a futuro el uso adecuado de los usuarios al momento de acceder y utilizar las aplicaciones móviles en Ecuador.

Capítulo I

Objetivo de aprendizaje: Como objetivo de aprendizaje es determinar, conocer e identificar las bases generales de la informática, derecho informático y aplicaciones móviles por lo cual, se requiere de toda comprensión para entendimiento del desarrollo de la investigación y determinar las implicaciones de la informática y las aplicaciones móviles en la sociedad.

1. La informática en relación a la sociedad.

La informática en relación con la sociedad requiere de un sin número de técnicas para tratar la información que se recepta y poder diferenciarlas de cada una de ellas de tal forma que la información que proporciona cada una de las personas en sitios tecnológicos como en aplicaciones móviles son tratados según se allá creado para su determinada finalidad en cuanto a la relación que posee esta con la sociedad, toda información que tratamos e interactuamos en la informática como tal se regirá mediante técnicas y estrategias para que sea tratada según su contenido.

"La informática es una ciencia de la computación que se encarga del tratamiento y estudio racional, de la información. Es decir, esta ciencia se encarga de distinguir a un conjunto de conocimientos prácticos y teóricos relacionados con la ciencia y la tecnología que, al relacionarse, hacen posible el tratamiento automático y racional de la información a través de computadoras." (Adrián, 2019)

Conforme lo establece el presente autor en la cita determina que, dicho tratamiento es conformado por su estudio racional y tratada para un correcto funcionamiento de la información proporcionada por cualquier medio sea este por computador u dispositivo móvil al ser una ciencia de la informática requiere de practica y aprendizajes técnicos no obstante, la información se adecuara conforme se haya programado en la aplicación y programa determinado para su entorno, tal como lo expresa

Por lo cual previamente analizado la informática cumple funciones determinadas para la sociedad en cuanto a sus avances tecnológicos versando en diferentes posibilidades en la que puede versar su funcionamiento y su tratamiento esto determina el uso constante de la información o tratamiento del mismo mediante su uso y manipulación por lo cual genera

preocupación ante el tratamiento y la regulación legal por lo cual, utilizar dicha informática mediante computador u dispositivo móvil se engloba en regulaciones legales para su adecuado funcionamiento y finalidad para la cual programas u aplicaciones móviles fueron creadas.

En base a lo expresado referimos a la siguiente pregunta; **¿Cuál es la importancia de la informática en la sociedad?**

Partiendo de la siguiente pregunta es de vital importancia es uso de la informática en nuestro entorno social puesto que, determina una herramienta que puede ser utilizada en dispositivos móviles como en ordenadores optimizando el tiempo que se requiere el realizar actividades cotidianas no obstante, es determinado por los avances tecnológicos que han avanzado de forma drástica en nuestro entorno exigiendo nuevos retos para la rama del derecho informático es el regular este uso de la información en base a la creación normativa, jurisprudencial, políticas públicas y demás técnicas jurídicas que permite el uso y regularización del mismo en cuanto se determinan por el estado de Ecuador.

Partiendo de la informática se debe tomar en cuenta que, el avance tecnológico del mismo ha desarrollado el uso de aplicaciones móviles en la sociedad en la cual cumple con diferentes funciones dependiendo para la cual fue creada desde este punto a finales del siglo XX surgen las primeras aplicaciones de los dispositivos móviles desde su creación han sido mejorados y creados para cumplir con las necesidades que hoy atraviesa la sociedad, tomando relevancia el derecho informático como fuente de regulación legal.

"En sentido general, podemos decir que la informática jurídica es el conjunto de aplicaciones de la informática en el ámbito del derecho. Nacida propiamente en 1959 en Estados Unidos, la informática jurídica ha sufrido cambios afines a la evolución general de la misma informática" (Valdés, 2008)

"En 1959, el centro colocó los ordenamientos legales de Pensilvania en cintas magnéticas. El sistema fue posteriormente demostrado, en 1960, ante la American Bar Asociación (ABA) (Asociación Americana de la Barra de Abogados) en la reunión anual celebrada en Washington, D.C. Ésta fue la primera demostración de un sistema legal automatizado de búsqueda de información." (Valdés, 2008)

Se posee conocimiento que la informática jurídica en un sentido general es la rama del derecho que va a regular la información en sistemas informáticos siendo esta impuesta bajo diferentes ámbitos u aplicaciones del derecho para su regulación por lo cual, las primeras regularizaciones parten en el año de 1959 en Pensilvania con el uso de denominados "cintas magnéticas", para la protección de la información y a su vez sea una herramienta de búsqueda de información dentro de un sistema informático puesto que, se tenía como concepción el uso de sistemas informáticos para cálculos matemáticos por regla general no obstante partiendo que la informática posee otra dimensión en la conservación de información y búsqueda del mismo empíricamente cambia los entornos sociales a los que se tenía comúnmente ante el uso para aspectos matemáticos.

1.1.Antecedentes de las aplicaciones móviles.

"La evolución de los teléfonos móviles y la aparición de aplicaciones para diferentes áreas han aumentado en los últimos años, según investigaciones realizadas no existe una fecha exacta del momento exacto que fue desarrollada la primera aplicación, pero, se decir que estas empezaron a surgir a finales de los años 90. Según Alfaro (2017) las primeras aplicaciones aparecieron en dispositivos telefónicos con pantallas pequeñas las cuales no eran táctiles, estas primeras aplicaciones con las cuales contaban los dispositivos son videojuegos, ring tones, agenda y calendario las cuales efectuaban funciones muy sencillas." (Moreno, 2022)

Las aplicaciones móviles poseen determinadas evoluciones siendo estas que anteceden a finales del siglo "XX", desde el año de 1990 con la aparición del primer dispositivo móvil, encontramos aplicaciones como, *"teléfono", "Agenda", "Contactos",* entre otros cumpliendo con funciones básicas entre esos años su utilización contaba con dispositivos no táctiles como lo encontramos hoy en día sino más bien dichos dispositivos pioneros de la aplicación móvil contaba con dispositivos no táctiles como el uso de diferentes botones para cada una de las funciones que corresponda ante el surgimiento de aplicaciones móviles en los primeros dispositivos inteligentes genera un cambio trascendental en la sociedad por el hecho que permite a los usuarios de los mismos acceder a diferentes tipos de aplicaciones con sus respectivas funciones este surgimiento comienza a mediados del año 2007 con las primeras

empresas tecnológicas pioneras de dicho cambio estructural en la sociedad siendo, “Apple”, con su creador, “Steve Jobs” y “Android”, con su creador, Reich Minera.

“En un primer momento las aplicaciones móviles fueron diseñadas para facilitar optimizar el tiempo de trabajo de directivos y profesiones de altos cargos. No obstante, en la evolución de las aplicaciones móviles, el sector del ocio y el entretenimiento empezó a coger protagonismo.” (Baena, 2019)

Las aplicaciones móviles es un avance tecnológico que facilita el trabajo cotidiano que se realizaba de forma manual como el escribir en agendas u otras actividades que se desarrollan de forma escrita (con acción del hombre), hoy en día estas acciones se han visto desapareciendo con el paso del tiempo ya que, el dispositivo móvil en cada una de la aplicación que requiera pormenoriza el tiempo de su uso en segundos se puede determinar acciones como agenda guardar contactos entre otras actividades, dichas actividades refieren tanto a un uso profesional en diferentes disciplinas profesionales no obstante, refiere de igual forma que su uso no profesional estas contribuyen en la formación de capacidades cognitivas para cualquier persona como otro medio de aprendizaje de diferentes actividades como para divertirse sea solo o con amigos entre sí no obstante, las aplicaciones móviles ha contribuido a la sociedad por lo cual requiere de un correcto esta debe enfocarse en distintas regulaciones legales por las cuales someterse.

1.2.Antecedente del Derecho informático.

“El nacimiento del Derecho Informático, según Téllez [1], se remonta a 1949 con la obra de Norbert Wiener, en cuyo capítulo 4 es dedicado al derecho y las comunicaciones, expresa la influencia que ejerce la cibernética respecto a uno de los fenómenos sociales más significativos: el jurídico.” (Aguilar P. A., 2015)

"El desarrollo de la humanidad se ha visto influenciado por avances tecnológicos que siempre traen consigo aspectos novedosos, tanto positivos como negativos, por tal motivo la sociedad se ha visto en la necesidad de adaptarse a esos cambios y sacar el mejor provecho de estas situaciones, que a fin de cuenta son a las que el ser humano debe adaptarse para seguir escalando peldaños en su desarrollo." (Hernández', 2012)

Como antecedente fundamental parte desde su nacimiento como tal del Derecho Informático, tomando énfasis al uso de los sistemas informáticos y cibernéticos como un aspecto más importante se tomando en consideración la expresión clásica del derecho desde su teoría general a ser remplazado por un sistema informático u cibernético para que aquello concurra se requiere de un sinnúmero de avances tecnológicos para que suceda como tal la transición de hombre a máquina en el sistema judicial, en relación al uso de aplicaciones móviles este permite el uso adecuado de las herramientas judiciales que son adaptadas conforme las necesidades que se requiera.

"Cuando surgió el Derecho informático, en la década de 1960, para dar respuesta a la aparición de las computadoras y, por lo tanto, al procesamiento automatizado de la información, los primeros temas que se plantearon fueron los siguientes: regulación de bienes informáticos (protección de bienes inmateriales, separación del software *y del* hardware*); protección de datos personales (los datos ya no se guardan en soporte de papel, la información se procesa en forma automática, el perfilamiento se vuelve mucho más fácil de realizar); flujo transfronterizo de datos (el envío de datos fuera de las fronteras de un Estado); delitos informáticos (actos ilícitos en que se tiene a las computadoras como instrumento o fin); contratos informáticos (cuyo objeto sea un bien o un servicio informático) y valor probatorio de los soportes informáticos (valor jurídico probatorio del documento electrónico y de la firma electrónica)."* (Díaz, 2022)

Con el surgimiento de la informática es por siguiente que su uso debe estar regulado por la rama del derecho informático es la rama adecuada para controlar y regular este uso de sistemas informáticos garantizando que los datos no sea de acceso público sino más bien este acceso lo posea personas a quien va a ser destinado dichos datos, la protección de datos personales es lo que engloba por regla general el derecho informático ya que esta información es de carácter confidencial permitiendo únicamente al titular de la información, el Estado garantiza la protección de los mismos en coordinación al uso adecuado que es brindado por el titular de su información y el tratamiento que este dé.

Partiendo de la protección de datos personales surge la necesidad de creación de su regulación para garantizar que el tratamiento de la información sea de carácter personal y no de carácter público la regulación es de vital importancia tanto como en las diferentes ramas de derecho por lo cual esta se concatena estableciendo una estrecha relación para considerar el uso adecuado y sancionatorio en caso de existir algún tipo de vulneración de estos datos personales tomando en consideración que esta regulación no es únicamente para los datos personales como tal no obstante, esta regulación recae en las aplicaciones móviles para determinar el tratamiento que esta ampliación brinda a la información proporcionada por los usuarios para acceder a las diferentes funciones de las diferentes aplicaciones en la que considere acceder para que dicho tratamiento no vulnere derechos reconocidos en la constitución, tratados internaciones y normativa legal vigente en el Estado de Ecuador se debe tomar en cuenta que el Estado es quien posee la información de cada persona según se estima en su uso y regulación para determinar la protección del mismo.

"El derecho de la informática, como instrumento regulador del fenómeno informático en la sociedad, no ha sido estudiado del mismo modo que la informática jurídica, porque se ha dado más importancia a los beneficios que a los eventuales perjuicios que puedan traer consigo las computadoras respecto al derecho y la sociedad en general." (Valdés, 2008)

Toma relevancia la regulación del derecho informático en relación con la informática jurídica no determina una base sólida ya que el avance tecnológico y desarrollo de sistemas informáticos u aplicaciones móviles a gran medida en relación con la sociedad expresa su uso por el cual recae únicamente en un sentido positivo ignorando por lo general la protección de los datos personales de las aplicaciones móviles, actualmente son mucho más exigentes en la privacidad para su uso al momento de aceptar los términos de condiciones no determina una garantía de que la aplicación cumple con el tratamiento de la información.

1.3.Definición de Derecho informático.

"De acuerdo con Téllez [1] es una rama de las ciencias jurídicas que contempla a la informática como instrumento (informática jurídica) y como objeto de estudio (derecho de la informática)." (Aguilar P. A., 2015)

"Asnito [2] lo define como el conjunto de principios y normas que regulan los efectos jurídicos nacidos de la interrelación de sujetos en el ámbito de la informática y sus derivaciones, especialmente en el área denominada tecnología de la información. El concepto engloba la sociedad de la información, por lo que define una ecuación cuya resultante es el Derecho Informático: derecho + informática + sociedad de la información = derecho informático" (Aguilar P. A., 2015)

"Siguiendo a Altar [3] es el conjunto de normas, principios e instituciones que regulan las relaciones jurídicas emergentes de la actividad informática" (Aguilar P. A., 2015)

"Pérez [5] establece que está conformada por el sector normativo de los sistemas jurídicos contemporáneos integrado por el conjunto de disposiciones dirigido a la regulación de las nuevas tecnologías de la información y comunicación, es decir, la informática y telemática." (Aguilar P. A., 2015)

"Para Del Pozo [6] el Derecho Informático abarca la universalidad de problemas, métodos y prospectivas que entrelazan a las dos disciplinas que forman su nombre, o sea, el derecho y la informática." (Aguilar P. A., 2015)

"Se conceptualiza el Derecho informático como la rama del Derecho que regula los fenómenos provocados por la informática. Según el profesor Julio Téllez Valdés (2004: 21), es el conjunto de leyes, normas y principios aplicables a los hechos y a los actos derivados de la informática. Si bien son escasos, existen varios ordenamientos jurídicos nacionales e internacionales con alusión específica al fenómeno informático." (Díaz, 2022)

Se determina que, el derecho informático es un instrumento y objeto en conjunto de principios y normas que regulan efectos jurídicos y sus instituciones concatenando los diferentes tipos de disciplinas jurídicas para un correcto funcionamiento de su marco legal garantizando el cumplimiento y protección de los datos que se encuentran en los dispositivos móviles garantizando el derecho a la intimidad y privacidad por regla general.

Los principios constitucionales y garantías jurisdiccionales posee la calidad de proteger y regular la información de cada persona con el propósito de que la información proporcionada sea regulado desde el uso de sus nuevas tecnologías y en coordinación con las aplicaciones móviles la información proporcionada sea tratada de la mejor forma y adecuada en base a políticas públicas de las cuales se someta las aplicaciones por regla general las más utilizadas en Ecuador permitiera que el acceso sea regulado con la finalidad de que, la aplicación móvil cumpla con los estándares establecidos por la normativa en general de Ecuador, como se entiende que todo acto u omisión del mismo será juzgado bajo jurisdicción del Estado únicamente mas no por cualquier otro órgano que no sea competente.

1.4.¿Qué es la seguridad informática en aplicaciones móviles?

"La seguridad de las aplicaciones se refiere a las medidas de seguridad, a nivel de aplicación, cuyo propósito es impedir el robo o el secuestro de datos o códigos dentro de la aplicación. Abarca las consideraciones de seguridad que se deben tener en cuenta al desarrollar y diseñar aplicaciones, además de los sistemas y los enfoques para proteger las aplicaciones después de distribuirlas." (Broadcom, 2022)

"Con el objetivo de establecer un marco unificado de requisitos de seguridad para diseñar, desarrollar y probar aplicaciones móviles seguras en las plataformas iOS y Android, en 2016, el proyecto OWASP publica la primera versión del Estándar de Verificación de Seguridad de Aplicaciones Móviles, o MASVS." (Sanchez, 2019)

La protección de datos personales en las aplicaciones móviles requiere de uso de técnicas adecuadas para evitar la adquisición de datos personales de forma ilegal en las aplicaciones móviles aplicando diferentes métodos de protección en los sistemas operativos de los dispositivos móviles no obstante, no es un medio eficaz para la adquisición ilegal de datos personales aquí interviniendo el derecho informático en cuanto a su marco legal adaptándose a las disposiciones del Estado para su correcto funcionamiento.

"Indicador detección de vulnerabilidades: Las vulnerabilidades más frecuentes encontradas en las aplicaciones fueron las relacionadas con la Calidad del código (66,7%), Almacenamiento de datos inseguro (50%) y Comunicación Insegura (50%). Además, se identificó que ninguna de las aplicaciones revisadas poseía mecanismos que dificultaran los procesos de manipulación e ingeniería inversa, pero al no ser de estricto cumplimiento, sólo se valoró que debía cumplirlo una sola aplicación (figura 5)." (Hernández, Borrego, & Brito, 2021)

"Indicador establecimiento del nivel de seguridad a partir de las vulnerabilidades encontradas: Las pruebas de seguridad aplicadas permitieron identificar que cuatro aplicaciones (66,7%) tenían un nivel de seguridad muy bajo; en una era bajo (16,7%) y finalmente una (16,7%) poseía un nivel alto de seguridad." (Hernández, Borrego, & Brito, 2021)

Imagen 1

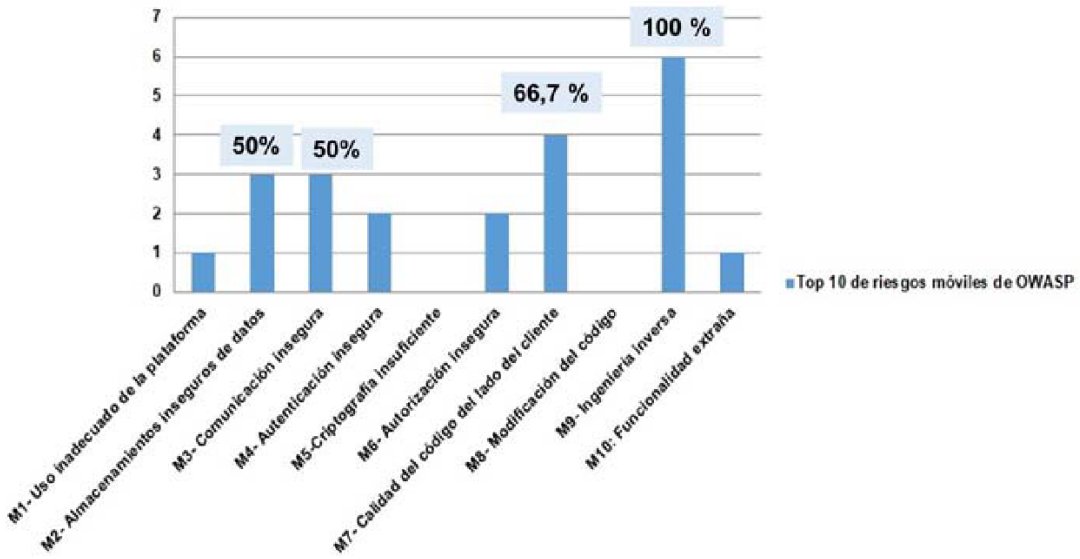


Figura 5. Cantidad de Aplicaciones que presentan vulnerabilidades. Elaboración propia.

Fuente: (Hernández, Borrego, & Brito, 2021)

La imagen 1 presenta los índices de riesgo que existen en el uso de las aplicaciones móviles en la cual se determina que, si existe vulneración de los derechos personales en el uso de aplicaciones móviles como tal, siendo estas reflejadas en un alto índice de porcentaje en la cual los usuarios de dichas aplicaciones son vulnerables a la extracción ilegal de sus datos sin su previo consentimiento toda esta información que se proporciona a las diferentes aplicaciones se encuentran almacenadas en una base de datos cuyo propósito es tratar la información personal de los usuarios.

1.5.¿Qué es base de datos?

"El antecedente cercano de las bases de datos informáticas fueron los sistemas de archivos en los que se podía contener información que luego se procesaba para poder utilizarla en la toma de decisiones." (Creel.)

Como primer antecedente de la base de datos hay que tomar en cuenta que, una vez que se almacenada la información se trataba de determinadas formas para tomar decisiones referentes a la información adquirida de tal forma que los administradores de la base de datos deciden qué hacer con los datos adquiridos y/u otorgados por cada uno de los usuarios, en inicios se puede considerar que la base de datos era de carácter manual en la que el administrador manipulaba la información a los diferentes destinos a los que correspondía en ese entonces con la revolución tecnológica en la que nos encontramos actualmente esta manipulación ya no requiere ser de forma manual pese a que, existe una cantidad masiva de información en las aplicaciones móviles en la cual las bases de datos han ido evolucionando y mejorando sus capacidades y técnicas informáticas de receptar información proporcionada por cada uno de los usuarios una vez se receptada la información los administradores de las aplicaciones móviles en cada una de su base de datos adquieren la información y disponen de la manipulación libre y voluntariamente.

"El sistema de bases de datos es definido por Rob y coronel, como: "la organización de componentes que definen y regulan la recolección, almacenamiento, administración y uso de los datos dentro de un ambiente de base de datos" (Peter Rob y Carlos coronel,2004. P. 18)." (Creel.)

Partiendo del concepto de base de datos se toma en cuenta que, toda la información adquirida se va a ordenar, almacenar y tratar conforme las disposiciones legales resguarde cada administrador dependiendo la aplicación móvil en la que se destine la información.

"Base de datos o fichero: Conjunto estructurado de datos cualquiera que fuera la forma, modalidad de creación, almacenamiento, organización, tipo de soporte, tratamiento, procesamiento, localización o acceso, centralizado, descentralizado o repartido de forma funcional o geográfica." (NACIONAL, 2021)

La ley orgánica de protección de datos personales define a la base de datos como una estructura en la que, se va a resguardar la información y va a ser proporcionada y tratada según su zona geográfica según su Gobierno Autónomo Descentralizado (GAD) para su respectivo procesamiento en concordancia a las diferentes técnicas de almacenamiento y tratamiento que otorga los diferentes sistemas informáticos para la toma de decisiones que según se requiera y la requiera el titular de la información.

En el siguiente recuadro detallaremos como se compone una base de datos;

Cuadro 1

Hardware	Los dispositivos físicos del sistema, que comprenden el procesador o computadora, que se controla a través de los dispositivos periféricos, que son de entrada o salida, ya sea que permitan introducir información en la memoria o extraerla de esta.
Software	Son el conjunto de programas utilizados por el procesador en el sistema de base de datos.
Personas	Comprende a los usuarios del sistema de base de datos, se identifican

	cinco tipos de usuarios: Los administradores del sistema, que supervisan el funcionamiento general del sistema. Los administradores de la base de datos. Estos administran la información específica que se contiene en la base de datos. mi. Los diseñadores de la base de datos. Son quienes diseñan el instrumento informático que permite el manejo de la información. Su función es de mayor importancia pues de su trabajo depende la funcionalidad y utilidad de la base de datos. vi. Analistas de sistemas y programadores. Ejecutan los programas de aplicación, mediante los cuales los usuarios finales tienen acceso a los mismos. v. Usuarios finales. Quienes utilizan los programas de aplicación del sistema para las operaciones diarias.
Procedimiento	Son las directrices que se utilizan para el manejo de la base; estos

	variarán de acuerdo a la persona que haga el uso de la base.
Datos	Es el conjunto de hechos guardados en la base de datos; al ser la materia prima que maneja la información, el determinar cuáles deben ingresarse y como deben manejarse es esencial para el correcto funcionamiento de la base de datos.

Cuadro 1; Elaboración propia del recuadro.

FUENTE BIBLIOGRAFICA: (Creel.)

Los sistemas informáticos reflejados en el "*Cuadro 1*", en relación con sus conceptos entendemos qu, las personas son el eje vital del uso de la información, administración de los datos adquiridos por lo cual, facilita la extracción de información con el uso de técnicas informáticas para poder acceder a ello, en base al recuadro encontramos los diferentes tipos de usuarios que pueden adquirir la información siendo estos en primero punto los **administradores de sistemas,** por regla general son aquellos que gestionan los datos adquiridos por las diferentes aplicaciones móviles con la finalidad de tratar la información conforme a lo que requiera la necesidad determinando la manipulación del mismo de los datos obtenidos, en segundo orden encontramos a los **administradores de la base de datos**; quienes se coordinan en acceder a la información específica de cada base de datos que posee en su sistema; en tercer orden a los **diseñadores de la base de datos**, quienes determinan en adquirir datos para realizar funciones como mejoras de la plataforma, como ejemplo encontramos las denominadas cookies u permisos que exige cada aplicación a cada usuario accediendo a información personal; cuarto orden encontramos a los **analistas de sistemas y programadores,** son aquellos que se encargan de dar ejecución a la aplicación u sistema para su correcto

funcionamiento y en un último orden encontramos a los **usuarios,** es conformado por cada persona que es titular de su información siendo la parte importante del funcionamiento de las aplicaciones móviles.

Cada uno de los usuarios otorga el acceso de la información personal desconociendo por completo que, dichos accesos otorgados es el permitir el acceso a la información personal de cada usuario u persona que utiliza la aplicación móvil por lo cual, en escala de cada uno de los administradores poseen dicho acceso a datos que son otorgados antes de dar uso de la aplicación no obstante, otorgar el acceso a los administradores desconociendo sus consecuencias incurre a graves vulneraciones de derecho a la privacidad además que, terceras personas pueden acceder a la información otorgada las aplicaciones móviles de tal forma que, al ser de acceso público entre usuarios recae a consecuencias como en la filtración de datos considerados sensibles dentro de un entorno social en la cual se encuentre la persona, por lo cual el riesgo es inminente para las personas que divulgan datos sensibles en aplicaciones móviles con la finalidad de utilizarlo como un medio de ocio u entrenamiento como tal.

1.6. Datos personales

En relación con los datos personales el uso propio y adecuación de la información de cada persona como titular de sus datos personales son únicamente quienes pueden modificar, eliminar o agregar información personal en sus aplicaciones móviles. Conforme al presente análisis se determina que el mal uso de estos datos personales u mala convicción de las consecuencias que trae el consentimiento libre y voluntario que el usuario otorga en el uso de las aplicaciones móviles su desconocimiento.

"El dato personal es información sobre las personas independientemente del medio que se utilice para captarla, almacenarla, manejarla, usarla, registrarla o comunicarla." (De dato personal, s.f.)

"«Datos de carácter personal» significa cualquier información relativa a una persona física identificada o identificable («persona concernida»)" (Literal a del artículo 2)" (De dato personal, s.f.)

"«datos personales»: toda información sobre una persona física identificada o identificable (el «interesado»); se considerará identificable toda persona cuya identidad pueda determinarse, 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" (Literal –a- del artículo 2)" (De dato personal, s.f.)

"Se entiende por datos personales e información personal los datos referidos a una persona identificada o identificable que entren en el ámbito de la Directiva y sean recibidos desde la Unión Europea por entidades estadounidenses, cualquiera que sea la forma en que se registren" (De dato personal, s.f.)

Los presentes conceptos toman en cuenta que el dato personal no incurre únicamente a la información personal de cada persona sino que integra datos que pueden identificar a las personas sea de una forma tanto directa como indirectamente a través de los diferentes tipos de aplicaciones en la cual se proporciona la información tanto para la base de datos como para los usuarios que interactúan en su entorno social y académico con la finalidad de acceder a información sensible.

1.7.Tipos de datos personales

La legislación ecuatoriana prevé diferentes tipos de datos personales en los cuales determinan conceptos básicos para un mejor entendimiento de la información sensible del dato personal; encontramos los siguientes tipos de datos personales:

Cuadro 2

Datos biométricos	Dato personal único, relativo a las características físicas o fisiológicas, o conductas de una persona natural que permita o confirme la identificación única de dicha persona, como imágenes faciales o datos dactiloscópicos, entre otros.
Datos genéticos	Dato personal único relacionado a características genéticas heredadas o adquiridas de una persona natural que proporcionan información única sobre la fisiología o salud de un individuo.
Datos personales	Dato que identifica o hace identificable a una persona natural, directa o indirectamente.
Datos relativos	etnia, identidad de género, identidad cultural, religión, ideología, filiación política, pasado judicial, condición migratoria, orientación sexual, salud, datos biométricos, datos genéticos, datos relativos a las personas apátridas y refugiados que requieren protección internacional, y aquellos cuyo tratamiento indebido pueda dar origen a discriminación, atenten o

	puedan atentar contra los derechos y libertades fundamentales.
Datos relativos a la salud	datos personales relativos a la salud física o mental de una persona, incluida la prestación de servicios de atención sanitaria, que revelen información sobre su estado de salud.
Datos sensibles	Datos relativos a: etnia, identidad de género, identidad cultural, religión, ideología, filiación política, pasado judicial, condición migratoria, orientación sexual, salud, datos biométricos, datos genéticos y aquellos cuyo tratamiento indebido pueda dar origen a discriminación, atenten o puedan atentar contra los derechos y libertades fundamentales.
Datos personales crediticios	Datos que integran el comportamiento económico de personas naturales, para analizar su capacidad financiera.

Cuadro 2; Fuente: elaboración propia

Fuente bibliográfica: (NACIONAL, 2021)

Como refleja *"cuadro 2";* determina diferentes tipos de datos siendo estos que, posee una característica fundamental para cada una de las personas, como se refleja encontramos: **datos biométricos; genético; personal; crediticios; relativos a la salud y datos sensibles;** estos tipos de datos son de carácter privado por la cual, requiere de la autorización del titular

para su manipulación como tal de los datos, centrándonos únicamente en los datos personales ya que, son aquellos en la cual, las personas pueden tener acceso libre y voluntariamente, para identificar a las personas concadenado con los datos sensibles puesto que según la constitución de la republica define como:

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

19. El derecho a la protección de datos de carácter personal, que incluye el acceso y la decisión sobre información y datos de este carácter, así como su correspondiente protección. La recolección, archivo, procesamiento, distribución o difusión de estos datos o información requerirán la autorización del titular o el mandato de la ley" (CONSTITUYENTE, 2008)

La constitución de Ecuador en el año 2008, garantiza y reconoce como derecho fundamental la protección de datos personales su acceso como tal únicamente debe ser autorizado por el titular de los datos, no obstante, se reconoce este acceso mediante el uso de aplicaciones móviles determinando que cualquier persona puede acceder a dicha información sin tomar en cuenta la consecuencia que lleva consigo otorgar el acceso como tal de la información personal al uso de las aplicaciones móviles ya que, dicha información posee la calidad de dato sensible el cual se detalla en el *"cuadro 2"*; cuando este sea difundido a cualquier persona natural y por ultimo una vez conceptualizado las bases correspondientes a la protección de datos personales se logra determinar que, debe existir la autorización por la cual si se determinar como tal mas no el tratamiento del mismo de la información personal.

Capítulo II

Objetivo de aprendizaje: Como objetivo de aprendizaje es determinar, la vulneración del derecho a la protección de datos personales en las aplicaciones móviles centrándonos en aplicaciones específicas que cumple la función de la recopilación de información.

2. Desafíos en la protección de datos personales en relación a las aplicaciones móviles

Este capítulo se va a enfocar en el análisis del marco legal de la legislación ecuatoriana en relación a la ley de protección de datos personales de Ecuador frente a aplicaciones móviles conocidas como: Facebook – WhatsApp – Instagram, como pioneras del tratamiento de información personal a lo largo de la revolución tecnológica con la aparición de los dispositivos móviles.

2.1. Concepto y finalidad del marco legal de la ley de protección de datos personales de Ecuador.

"Art. 1.-Objeto y finalidad. -El objeto y finalidad de la presente ley es garantizar el ejercicio del derecho a la protección de datos personales, que incluye el acceso y decisión sobre información y datos de este carácter, así como su correspondiente protección, Para dicho efecto regula, prevé y desarrolla principios, derechos, obligaciones y mecanismos de tutela" (NACIONAL, 2021)

El objeto y finalidad de la ley de protección de datos es resguardar el derecho a la protección de la información personal proporcionada por cada uno de los usuarios u personas naturales que se encuentran bajo jurisdicción del Estado ecuatoriano misma que para llevar a cabo la tutela de este derecho, se toma en consideración el surgimiento de aplicaciones móviles como *Facebook, WhatsApp, Instagram,* las diferentes aplicaciones han realizado solicitudes de

accesos que permite a las aplicaciones móviles ingresar a información personal de cada persona natural sin tomar en cuenta los factores externos que permiten el acceso a dicha información.

Se considera a su vez el derecho a la privacidad de la persona, según el sistema interamericano de derechos humanos, lo define como:

"Toda persona tiene derecho a la protección de la ley contra los ataques abusivos a su honra, a su reputación y a su vida privada y familiar". (Vizcarra)

Según el sistema interamericano de derechos humanos considera la protección de datos personales un derecho que debe ser resguardado para evitar vulneraciones que engloban el derecho a la honra y/u reputación del titular de su información.

La protección de datos personales engloba derechos como la intimidad del titular de su información además que el derecho a la honra se encuentra relacionados entre sí por el hecho que, la información proporcionada corresponde a los titulares.

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

19. El derecho a la protección de datos de carácter personal, que incluye el acceso y la Decisión sobre información y datos de este carácter, así como su correspondiente protección. La recolección, archivo, procesamiento, distribución o difusión de estos datos o información requerirán la autorización del titular o el mandato de la ley." (CONSTITUYENTE, 2008)

La Constitución de la república reconoce que la protección de datos personales es de carácter personalísimo por lo que, al acceder a dicha información personal se requiere de la autorización del titular mismo por lo cual las entidades que adquieren la información deben realizar los respectivos tratamientos de la información en su base de datos reconociendo que los titulares de la información tienen el derecho a acceder a su información personal en la cual pueden tomar sus propias decisiones en base a su convicción en modificar, eliminar, entre

demás acciones para su respectiva información, conforme a la ley orgánica de protección de datos personales se estima que la protección de estos debe ser de manera íntegra para evitar dilaciones injustificadas que altere la información de los titulares, con la garantía de respetar su autonomía de la información con las respectiva necesidad de regular adecuadamente el acceso y utilización de la información.

En cuanto a la garantía del mismo establece la corte constitucional las cinco dimensiones en las cuales la información personal se lleva a cabo;

CUADRO 3

Hábeas Data informativo (derecho de acceso)	Es la dimensión procesal que asume el hábeas data para recabar información acerca del qué, quién, cómo y para qué se obtuvo la información considerada personal.
Hábeas Data aditivo (derecho de modificación)	Busca agregar más datos sobre aquellos que figuren en el registro respectivo, buscando actualizarlo o modificarlo según sea el caso.
Hábeas Data correctivo (derecho de corrección)	Resuelve rectificar la información falsa, inexacta o imprecisa de un banco de datos.
Hábeas Data de reserva (derecho de confidencialidad)	Persigue asegurar que la información recabada sea entregada única y exclusivamente a quien tenga autorización para ello.

Hábeas Data cancelatorio (derecho a la exclusión de información sensible)	Busca que la información considerada sensible sea eliminada, por no ser susceptible de compilación.

Cuadro 3; Elaboración propia del cuadro.

Fuente Bibliográfica; (Muñoz & Contreras, 2022)

El cuadro 3, expresa las 5 dimensiones del habeas data en la cual, los titulares de la información personal pueden acceder de cinco formas diferentes para garantizar su derecho reconocido en el Art. 66 numeral 19, de la constitución, en primer orden encontramos al **Habeas Data informativo**, la cual cumple con la función de otorgar al titular la forma en la que accedieron a su información personal y la razón por la cual se obtuvo dicha información, en un segundo orden encontramos el **Habeas Data aditivo;** el cual cumple con la función de modificar la información personal esta sea con la finalidad de corregirlo sea las veces que considere necesario, en un tercer orden encontramos al **Habeas Data correctivo;** esta cumple con la función de corregir como su palabra misma lo expresa, datos que, se encuentren por error o sean necesarios corregirlos para que la información que, se proporciona sea la correcta por parte del titular, en un cuarto orden encontramos al , **Habías Data de reserva. Este cumple** con la finalidad de que la información considerada como confidencial sea conservada u reservada como tal y mantenga al titular a su prioridad de forma precisa, requiriendo su autorización para acceder a ella y en un quinto orden encontramos al Habías Data **cancela torio. Este cumple** con la función de eliminar información personal que considere el titular sea necesario eliminar, estimando la protección del derecho a la privacidad misma del titular y su dignidad como tal, evitando filtraciones de su información que pueda afectar al titular.

En relación con las cinco dimensiones del Habeas Data, cabe recalcar que, en el uso de aplicaciones móviles, la información queda inmersa en la recolección indebida sin previo

consentimiento además el tratamiento que se estima por parte de las empresas creadoras de las aplicaciones móviles ya mencionadas trate la información de una forma adecuada por lo cual no se estima la base de datos correspondiente a la que es enviada, considerando que el tratamiento del mismo no es idóneo de ser divulgado en las aplicaciones en cuanto al entorno social en el que se encuentre.

2.2.Derecho a la intimidad.

"El derecho a la intimidad abarca aquello que se considera más propio y oculto del ser humano —entendiéndose por propio y oculto la información que mantiene para sí mismo—. Pero es insoslayable que el contacto permanente del ser humano con sus semejantes al interior de la sociedad a la que pertenece, así como todos aquellos avances tecnológicos que han venido desarrollándose en la sociedad, han comenzado a transgredir aquellos ámbitos que forman parte de la intimidad el ser humano." (González, La protección de datos personales: derecho fundamental del siglo XXI. Un estudio comparado, 2007)

La protección de datos personales engloba derechos más intrínsecos de las personas como la intimidad siendo este que es lo más autónomo de una persona según la información que posee se estima que el uso de aplicaciones móviles transgrede este derecho por la información que proporciona a la sociedad al momento de dar uso de las aplicaciones como *Facebook, Instagram y WhatsApp,* las aplicaciones mencionadas responden a la adquisición de datos sensibles frente a su entorno social en el que se encuentra. La Constitución de la república reconoce este **derecho a la intimidad** como:

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

20. El derecho a la intimidad personal y familiar." (CONSTITUYENTE, 2008)

La Constitución de la república reconoce el derecho a la intimidad personal y familiar, enfocándonos más en la intimidad personal puesto que los titulares deben resguardar su

información personal y protegerlo a base de las garantías jurisdiccionales, mecanismos de tratamiento de datos y técnicas informáticas que resguarda la información personal.

La ONU (Organización Naciones Unidas); expresa lo siguiente ante el derecho de la intimidad en su artículo 12;

"Nadie será objeto de injerencias arbitrarias en su vida privada, su familia, su domicilio o su correspondencia, ni de ataques a su honra o a su reputación. Toda persona tiene derecho a la protección de la ley contra tales injerencias o ataques." (General, 1948)

La ONU, expresa que, ninguna persona va a ser afectada en su vida privada garantizado como un derecho universal, la corte constitucional establece un concepto en relación al derecho a la intimidad;

"Supone la existencia y goce de una órbita reservada en cada persona, exenta del poder de intervención del Estado o de las intromisiones arbitrarias de la sociedad, que le permite a dicho individuo el pleno desarrollo de su vida personal, espiritual y cultural" (TIRADO, 2006)

Relaciona que el Estado, como tal, se va a privar de acceder a la información personal de cada titular del mimo, de la forma que el derecho a la intimidad se constituye para el libre desarrollo de la persona de una forma interpersonal. La corte constitucional de Colombia establece tres aspectos en que el derecho a la intimidad puede ser vulnerado;

Cuadro 4

Primera forma	Intromisión irracional en la órbita que cada persona a reservado.
Segunda forma	Divulgación de los hechos privados.
Tercera forma	Presentación tergiversada o mentirosa de circunstancias personales.

Cuadro 4; Elaboración propia del recuadro.

Fuente bibliográfica; TIRADO, M. X. (Junio de 2006)

Según el cuadro 4, determina las tres formas en las que, se puede vulnerar el derecho a la intimidad en su **primera forma**, es invadiendo el espacio personal de la persona de forma arbitraria y sin previo consentimiento, en su **segunda forma**; se destina a ser información que se considera personal u privada, esta divulgación llega a ser enviada a diferentes personas una vez determinado la divulgación se vulnera esta privacidad de los titulares de la información y en su **tercera forma**; hace referencia a que la información enviada de forma arbitraria sin previo consentimiento de los datos personales u considerados sensibles como tal en su tercera forma puede ser esta modificada u alterada para diferentes expectativas de la personas receptora de la información ya que, esta afecta de forma íntegra al titular de la información personal que es enviada a diferentes personas, estas tres formas hace relación a la vulneración de los datos personales o como se mencionó información sensible en las aplicaciones móviles mencionadas, en las cuales la divulgación de la información personal es de forma masiva a diferentes personas por lo cual, en coordinación con el cuadro 4 se determina la forma en la que se vulnera este derecho a la intimidad de la persona como titular de las mismas.

"Otra persona toma así conocimiento de una intimidad: Para ella surge entonces el deber Secreto" (CUBRÍA, 1970)

El presente autor expresa que, al momento de adquirir conocimiento de aspectos intimitos de una persona en su vida personal como sus datos u información como tal, surge el deber de dicha persona no divulgar la información confidencial adquirida u proporcionada por el emisor por lo cual, esta información no puede ser divulgada bajo ninguna circunstancia en caso de, ser filtrada u difundida incurre a una de las formas de divulgación de información personal vulnerando el derecho de los datos personales de cada usuario, tomando en cuenta que

al usar aplicaciones móviles ya mencionadas, esta proporciona de determinada forma información personal bajo propio consentimiento no obstante, no evita que, sea víctima de vulneración de datos personales al tratar de indebida forma la información proporcionada.

"En la actualidad nadie pone en tela de juicio la preeminencia del derecho a la intimidad, ante una modernidad imparable, que invade las esferas más intrincadas de la vida cotidiana del ser humano, sin una tutela adecuada en los ordenamientos vigentes en nuestro país, se pone de relieve que no existe una real construcción del referido derecho, ante una escasa jurisprudencia, que no acaba por determinar los alcances y conceptualización del mismo y la confusión que parece mediar entre intimidad y privacidad en su contenido." (Patricia, 2013)

El surgimiento y avance tecnológico del mismo ha permitido diferentes formas de vulneración al derecho a la intimidad en la sociedad sin tomar en cuenta que este tratamiento del mismo no ha sido regulado adecuadamente, por lo cual la falta de interés por parte del estado ha inferido de tal forma que este derecho reconocido sea vulnerado de diferentes formas en el uso de aplicaciones móviles. No obstante, no existe una regulación adecuada para proteger el contenido de la información generando divergencias al momento de proporcionar una regulación de los datos personales y del derecho a la intimidad mismo, debiendo ser el "deber ser" de dicha regulación, además de que se debe tomar en cuenta la diferenciación entre dato personal e intimidad del mismo.

Las aplicaciones móviles han avanzado tecnológicamente de tal forma que establecer preceptos jurídicos y bases legales sólidos en cuanto a la protección de datos personales ha tomado dificultades ya que dichas aplicaciones móviles invaden los datos personales de forma masiva e independientemente del tratamiento que se dé a la información adquirida por la empresa u usuarios que acceden a ella sin previo consentimiento.

"Art. 1.-Objeto y finalidad. -El objeto y finalidad de la presente ley es garantizar el ejercicio del derecho a la protección de datos personales, que incluye el acceso y decisión sobre información y datos de este carácter, así como su correspondiente protección, Para dicho efecto regula, prevé y desarrolla principios, derechos, obligaciones y mecanismos de tutela." (NACIONAL, 2021)

Como se puede observar en la Ley Orgánica de Protección de Datos Personales, únicamente garantiza la protección de "dato personal"; más no el tratamiento y protección del "derecho a la intimidad"; degenerando este derecho a que no se determine ni exista una protección como tal, además de la acción de *Habeas Data;* es la única fuente legal que permite dicha protección del derecho a la intimidad de la cual, no se ha presentado garantías en base al derecho a la intimidad.

2.3.Derecho a la honra.

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

18. El derecho al honor y al buen nombre. La ley protegerá la imagen y la voz de la persona." (CONSTITUYENTE, 2008)

La Constitución de la república reconoce el derecho a la honra, el buen nombre, el derecho a la imagen de los titulares cabe mencionar que, con base las aplicaciones móviles determinan la vulneración de estos derechos puesto que se divulga información de personas en situaciones comprometedoras afectando el derecho a la honra, el buen nombre.

Se ha presenciado que, en las plataformas ya mencionadas el derecho a la honra y buen nombre en relación al derecho a la imagen de la persona ha sido afectada por el hecho que la divulgación de imágenes, videos u datos catalogados como sensibles ha afectado a las personas por ser objeto de diversas divulgaciones en las aplicaciones de Facebook, WhatsApp e

Instagram, las aplicaciones mencionadas proporciona el uso público de los datos personales bajo un consentimiento proporcionado por parte de los titulares al momento de acceder y crear las cuentas correspondientes no obstante, el uso inadecuado ha generado la vulneración de los derechos de la honra, buen nombre e imagen ante la presencia de publicaciones inadecuadas en las aplicaciones.

"La honra puede ser afectada cuando exista una razón justa para ello, como por ejemplo, que existan pruebas fehacientes o una sentencia condenatoria por la comisión de un delito, caso en el cual no se está violando el derecho a la honra de la persona sobre la que se difunde información que le afecte la estima y respeto ganados." (López, 2014)

La difusión de información personal de manera pública afecta el derecho a la honra del titular no obstante, no cabe vulneración al derecho a la honra cuando este haya sido demostrado justificadamente que el titular cometió algún delito u acciones no penales por regla general, por lo cual, el derecho a la honra será garantizado para evitar vulneraciones de sus derechos por filtración de su información personal en las aplicaciones móviles ya mencionadas con anterioridad.

2.4.Derecho al buen nombre.

"El derecho al buen nombre se encuentra como derecho fundamental constitucional consagrado en el artículo 15 el cual determina que "todas las personas tienen derecho a su intimidad personal y familiar y a su buen nombre, y el Estado debe respetarlos y hacerlos respetar" (Constitución Política de Colombia, 1991), en el entendido de que el buen nombre es tanto personal como familiar refiriéndose al derecho que se tiene de gozar de una buena imagen y de humana reputación." (López, 2014)

El derecho al buen nombre según la constitución de Colombia hace referencia a que el titular de su información personal está protegida por el Estado de Colombia con la garantía de

que la información que posea no puede ser utilizada bajo ninguna circunstancia por terceras personas haciendo respetar ese derecho consagrado en su Constitución.

"El derecho al buen nombre lo adquieren los individuos, la familia o las agremiaciones a través del tiempo y por las conductas que realicen en su entorno. Por tanto, es la misma comunidad la que se encarga de realizar juicios de valor sobre lo actuado por los demás individuos. Este es un derecho de valor cuya protección está determinada por el comportamiento que ha tenido el individuo frente a la sociedad quien califica la conducta como intachable o no, y proyecta la buena imagen que el individuo transmite a la sociedad, imagen que debe ser respetada por los demás." (López, 2014)

El derecho al buen nombre es innato de la persona al momento de su nacimiento por lo cual la sociedad presenta diferentes aspectos para que este derecho sea garantizado y no sea manchado ya que los diferentes tipos de comportamientos que del titular realice va a influir en su entorno social en el que se encuentre rodeado.

2.5.Derecho a la imagen

"La protección de la imagen de la persona señala esta doctrina, salvaguarda la intimidad y "el poder de decisión sobre los fines a los que hayan de aplicarse las manifestaciones de la persona a través de su imagen, su identidad o su voz", nos dirá un autor español" (Alcalá, 2007)

La protección del derecho a la imagen está relacionado con el derecho a la intimidad por lo que este derecho va a influir en la toma de decisiones que destine el titular de su información determinando que, al existir la vulneración de este derecho se concatena con el uso que proporciono el titular.

"El derecho a la propia imagen surge del hecho que el ser humano está en el mundo de forma corpórea o física, esta realidad de la persona es una de las fuentes de datos e información más

importante sobre los individuos, al ser susceptible de ser captada la figura humana como cara externa de la persona, a través de distintos medios e instrumentos." (Alcalá, 2007)

El derecho a la imagen intrínsecamente toma relevancia por el hecho que, cada persona ocupa un lugar en el espacio característicamente física con sus determinadas cualidades que, diferencia a cada persona en la sociedad siendo capaces de percibir lo que sucede a nuestro entorno social en el que nos encontramos.

"El derecho fundamental a la propia imagen garantiza un ámbito de libertad respecto de sus atributos más característicos y propios de la persona, que la identifican en cuanto tal, como es la imagen física visible. Asimismo, protege el poder de decisión sobre los fines a los que haya de aplicarse las manifestaciones de la persona a través de la imagen y un ámbito de libre determinación sobre la materia." (Alcalá, 2007)

El derecho a la imagen es un derecho que determina a base de su arbitrio, cada persona llega a realizar actos que determine cómo va a ser presentada su imagen ante las demás personas, por lo cual se enfocará directamente en las libres acciones de cómo va a exponer su imagen ante la sociedad no obstante, ninguna otra persona puede perturbar este derecho reconocido, puesto que la finalidad que cumple es llevar a cabo de cómo se va a exponer ante el público sin necesidad de vulnerar su derecho a la honra, intimidad y buen nombre.

En relación con las aplicaciones móviles ya mencionadas, cabe mencionar que el derecho a la imagen se vulnera con gran magnitud puesto que la divulgación injuriosa por parte de terceras personas ante el uso malicioso de la información que proporciona el titular en las aplicaciones concatena a perjudicar al titular de su información.

"El derecho a la propia imagen tutela la proyección exterior y concreta de la persona en su figura física visible independientemente de la afectación de su honra, de su vida privada y del eventual derecho de propiedad, dotando a la persona de la facultad de decidir sobre el uso de

su imagen sin intromisiones ilegítimas, en la medida que expresan cualidades morales de la persona y emanaciones concretas de su dignidad de ser humano, configurando su ámbito personal e instrumento básico de su identificación, proyección exterior y reconocimiento como ser humano. Quedan fuera del ámbito del derecho a la propia imagen las representaciones que requieren mediación intelectual como es el caso de los retratos literarios u otras formas de mediación intelectual." (Alcalá, 2007)

El derecho a la imagen se enfoca y enfatiza a que los titulares de su información que es compartida a su entorno social no sea afectado de forma que, se garantice este derecho con el fin de protegerlo y así evitar dilaciones e injerencias innecesarias al momento de tratar la información por parte de un tercero confiriendo la autonomía propia de garantizar u fomentar el respeto a las personas que con el uso de las aplicaciones móviles se proyecte y fomente el derecho a la dignidad humana evitando así y garantizando el derecho a la imagen y los demás derechos que concatenan para que el titular sea percibido en la sociedad y en su entorno para un desarrollo integro tanto físico como psicológico para cada persona que proporciona datos en estas aplicaciones móviles ya mencionadas con anterioridad.

2.6.Datos personales en aplicación Facebook.

La plataforma de Facebook es, sin duda, la plataforma más usada hoy en día a nivel mundial, en la cual se reconoce como una de las aplicaciones pioneras de la adquisición de la información personal, al igual que las aplicaciones como Instagram y WhatsApp. Con cada característica que reconoce y diferencia cada una de ellas, Facebook cumple con la finalidad de conversar mediante chat con otras personas, publicar fotos y videos.

Se debe tomar en cuenta que estas funciones son propias y autónomas de la aplicación de Facebook desde su creación en el año de 2004 hasta la actualidad.

Hoy en día cabe mencionar que la aplicación de Facebook recopilación la información que se proporciona a la plataforma en el entorno social en el que se encuentra el titular accediendo a tratar diversos puntos controversiales.

"La dispersión de los usuarios y la constante reformulación tecnológica definen las redes online. Así «la Web 2.0 vuelve a dar protagonismo a la conversación social, impulsada por la metamorfosis profunda y continua de las tecnologías de la comunicación» (Ruiz & Masi, 2010: 9)." (Tello, 2013)

Hace referencia a que diferentes personas o usuarios se encuentran interconectadas en sí mismos en un mismo lugar. En este caso, la aplicación de Facebook ha determinado que simultáneamente la comunicación se encuentra en un solo servicio.

La aplicación Facebook es una herramienta en la cual las personas interactúan de forma simultánea con la finalidad de ejercer su derecho a la libre expresión, no obstante, existen casos en los que esta libertad de expresión es de un uso abusivo, atentando contra el derecho a la imagen y a la honra, derechos que son englobados por la protección de los datos personales.

"Si bien esta sociedad de la información ha supuesto una serie de ventajas para los usuarios de la misma, también es verdad que existen riesgos que pueden correr los datos personales que circulan en la web, sobre todo a través de las redes sociales." (Rosales, 2014)

Se toma en consideración que las personas hoy en día, al encontrarse en un mundo totalmente tecnológico en actividades cotidianas o en general sea por niños, adolescentes y adultos, al brindar este uso en la aplicación de Facebook y las demás ya mencionadas, se debe tomar en consideración que la información proporcionada está sujeta a ser mal utilizada por terceras personas vulnerando derechos fundamentales como su honra e imagen existiendo estos

riesgos en la privacidad ante la recopilación de la información de forma excesiva, como por ejemplo:

"Para poder iniciar nuestro análisis, es pertinente hacer una breve descripción del caso. A principios del año 2012 la directora de la Universidad Interamericana para el desarrollo, (UNID) sede Morelia, se percata de que en el perfil institucional de la Universidad en Facebook estaba publicada la fotografía de su perfil personal, pero editada por un tercero sin su consentimiento, en la cual aparecían dos monedas con el signo de pesos en sus ojos y una leyenda que decía: "UNID Ratera". La publicación duró alrededor de 3 días en la red, hasta que por peticiones de otros usuarios de Facebook fue retirada por el mismo servidor." (Rosales, 2014)

El presente ejemplo expresa la forma en la que se da la vulneración al derecho a la imagen, honra y buen nombre, y sobre todo los datos mismos, puesto que no determina el tipo de tratamiento malicioso que da a la información obtenida en la red social Facebook. Este caso se encontró en el Estado de México que atentó en contra de la directora de una universidad, demostrando que el tratamiento de los datos personales por terceras personas puede llegar a ser malicioso en la mayoría de los casos afectado al titular directamente, pese a que haya sido eliminada de la plataforma no evita que diferentes dispositivos hayan adquirido la información publicada en Facebook.

Cabe mencionar que se determina el derecho a la libre expresión, por lo cual este derecho es aplicado no obstante, posee fines que vulneran los derechos de las personas con la adquisición indebida de su información acarreando sanciones penales como no penales.

"Según Matilde Carlón, citada por Wilmar Arellano, la autodeterminación informativa se encuentra "caracterizada por ser manifestación de la autotutela de la propia identidad

informática en tanto cuanto permite controlar, en sentido amplio, los datos personales inscritos en un programa electrónico" (Rosales, 2014)

Según se estima con base en el siguiente precepto, según la autora expresa que cada titular de su información posee la capacidad de proteger su información personal y sus intereses en el uso de la aplicación de Facebook. No obstante, no se puede expresar su auto tutela en su máximo esplendor en la aplicación de Facebook, por el hecho de que no se regula por parte del titular quien puede acceder a la información y quien no puede acceder a ella, el simple hecho de otorgar un consentimiento que exige la aplicación no toma en consideración por desconocimiento por parte del titular los riesgos que puede generar su acceso.

"Las redes sociales, como Facebook, deben ampliar la protección de los datos de las personas que tienen bajo su soporte, dado que no basta con brindar la opción de solicitar que se retire una publicación no deseada, porque como hemos señalado, se pueden vulnerar derechos fundamentales durante el tiempo en que la publicación permanece en el portal. Más aún, si la mayoría de los datos que se suben a este sitio web son imágenes de personas." (Rosales, 2014)

Toma relación a que no se determinan mejores opciones sobre el cuidado y protección de los datos personales, por el hecho de que el tratamiento que este puede recibir no llega a ser el adecuado para el entorno social en el que se encuentran las personas determinando la existencia de la vulneración del derecho a los datos personales, honra, buen nombre y a la imagen, por lo cual, al momento de ser debido a la aplicación de Facebook, se confía el tratamiento de datos a la administración de la empresa, por lo cual, debido al malicioso tratamiento por parte de terceras personas, se vulneran estos derechos reconocidos por la constitución y demás órganos internacionales, por la filtración indebida y la mala utilización de la información.

"Ante tanta arbitrariedad sería conveniente contemplar, estatutariamente, una cierta participación de los usuarios en la administración y definición de políticas de uso y de privacidad a través de algún método reglado, como encuestas vinculantes, foros, medidas democráticas, etc. para evitar situaciones de abuso y la falta de consentimiento y legitimidad en el uso de ciertas políticas respecto a contenidos que son de los usuarios." (Ruiz, 2009)

Se determina que para evitar abusos en cuanto a la adquisición de la información por parte de los administradores no se ha determina a dónde o qué destino posee la información por lo cual, se estima que se apliquen políticas en coordinación con los titulares para la creación de políticas y privacidad para proteger a los usuarios su información y determinen el destino mismo y el tratamiento que estos aplican cuando ingresan a la aplicación móvil proporcionando información en determinados aspectos de la plataforma.

"Por otra parte, respecto a la protección de datos existen problemas técnicos y organizativos en estas redes sociales, que necesariamente habría que subsanar, como las posibles copias que pueden circular sin control o la reproducción de datos por otros usuarios o ante las propias debilidades y fallas de seguridad del propio sistema o ante robos de información o usos ilícitos de ésta." (Ruiz, 2009)

La protección de datos personales en cuanto a las aplicaciones móviles ya mencionadas no cumple con los estándares de protección puesto que existen casos en las que las denominadas "caídas", de estos sistemas ha generado a lo largo de su uso y actualización constante ha permitido que la información proporcionada no sea tratada adecuadamente y a su vez no se determina la forma en la que realizan el tratamiento de la información, conllevando así el hurto de la información personal proporcionada por cada uno de los titulares, aquí tomamos en consideración que la información adquirida de forma común corresponde o se denomina los "Hackeos" o "Phishing", puesto que, el titular accede de forma inequívoca a su libre arbitrio

sin necesidad de que sea adquirido por alguna tercera persona u propiamente de la administración responsable del tratamiento de los datos personales.

"En definitiva, lo que queremos hacer constar es la fragilidad y peligro para la protección de datos en redes sociales, por la negligencia del responsable de seguridad y la falta de seguridad de la tecnología o del propio sistema informático. Lo cual se minimizaría, por ejemplo y en último extremo, con el uso del anonimato como forma de preservar los datos." (Ruiz, 2009)

El uso de las redes sociales como Facebook, Instagram y WhatsApp, en relación a la protección de los datos sensibles influye en gran medida frente a sus regulaciones en seguridad y las herramientas informáticas para proteger la información personal por lo cual estas herramientas no han sido eficaces para solventar la vulneración de los datos personales no obstante, el anonimato en el uso de las redes sociales como Facebook, Instagram y WhatsApp, para evitar la vulneración de derechos como la imagen, honra y buen nombre.

Desconocen los riesgos inminentes que presenta el uso mismo de la aplicación puesto que no, presentan el consentimiento previo de sus padres u titulares legales que, se encuentren a su cargo desencadenando posibles vulneraciones a sus derechos fundamentales no obstante el uso inadecuado e informal de la aplicación Facebook ha conllevado a que, la filtración de información personal sea preocupante a nivel social y legal puesto que, se proporciona información u datos sensibles que puede afectar a los titulares de su información incurriendo a la adquisición ilegal por parte de los administradores u terceras personas que ingresan a esta red social con la finalidad de hacer acciones maliciosas que, afecte el derecho a la honra, la imagen el buen nombre y la intimidad mismo tal como se ha analizado por lo cual, las nuevas generaciones se encuentran inmersas a la publicación de sus datos personales sin ningún tipo de restricción.

"En las redes sociales, una vez dado de alta un usuario se le insta a incorporar la mayor cantidad de datos, y lo más precisos posible, y a invitar a otros amigos para que sigan el mismo procedimiento." (Perelló, 2009)

Se determina que el titular de su información, una vez que haya creado su usuario en la red social, este facilita la publicación de su información personal para que este sea de acceso público según lo vea pertinente. No obstante, en su entorno social en el que se encuentre familiares o amigos, podrán interactuar con el titular de la información que proporciona en la aplicación y en un segundo orden, el titular podrá interactuar con sus amigos y familiares en la red social, tomado en cuenta que terceras personas ajenas al titular, amigos y familiares, estas terceras personas tienen la facultad de difundir dicha información proporcionada.

2.7.Cambridge Analítica

"A mediados de marzo de 2018 el canal británico Chanel 41, el diario norteamericano Té New York Times2 y el británico Té Observar (Té Guardián) comenzaron a publicar material de investigación sobre como algunas corporaciones favorecían el supuesto "uso ilegal" de los datos personales de sus usuarios con fines electorales." (Vercelli, 2019)

En relación al caso Analítica, se estima que Facebook, en coordinación con otras empresas, proporcionó información de carácter personal vulnerando gravemente el derecho a la protección de datos personales con fines meramente políticos, estimando que varias empresas adquirieron toda la información sin consentimiento alguno de cada persona.

"Los datos personales de los usuarios de Facebook Inc. habían sido colectados a través de Global Sáciense Resecar, una empresa fundada por Aleksander Kogan, un psicólogo social ruso de la Universidad de Cambridge, Reino Unido, que trabajaba sobre programas de "felicidad y amabilidad" (chapines and quindes)." (Vercelli, 2019)

La forma en la que adquirieron a la información personal de cada persona recae el simple hecho de que los usuarios interactuaron con la aplicación generada por el creador, *Aleksander Kogan,* con la finalidad de cumplir con determinadas investigaciones que realizó con este consentimiento "otorgado" por cada uno de los usuarios. No se determinó la finalidad del mismo y la forma en la que iba a ser tratada dicha información. Los desarrolladores de *Global Sciense Resecar* en coordinación con las políticas de Facebook, concierne a la recopilación de la información personal. Esta información proporcionaba datos meramente personales de cada titular que accedió al programa de *Aleksander Kogan,* en conjunto con la recopilación de Facebook.

"Estas características de la plataforma Facebook Inc. permitieron que Kogan obtenga no sólo los datos personales de los 270.000 usuarios que efectivamente interactuaron con su aplicación, sino que -según datos estimativos de Facebook Inc.- los perfiles colectados de los usuarios podrían alcanzar los 87.000.000 millones (inicialmente se supuso que eran 50 millones y luego 70 millones)." (Vercelli, 2019)

La recopilación de información ha sido crucial de tal forma que, al acceder a más de 270.000 mil usuarios, se estimó que los valores hayan incrementado más conforme los usuarios hayan accedido a las plataformas otorgadas por Donación, determinado así la vulneración a los datos personas accediendo de forma ilegítima y arbitraria. No se estimaba únicamente una aplicación a la que ingresaron los usuarios sino más bien existieron más aplicaciones que cumplen con la misma función de recopilar la información personal de cada uno de los usuarios.

"En Cambridge Analítica no sólo querían mostrar anuncios publicitarios dentro de Facebook Inc.: pretendían crear perfiles según rasgos similares (aproximados) de personalidad para enviar anuncios micro segmentados a los diferentes grupos de votantes (grupos de personalidad de los votantes según rasgos psicométricos)." (Vercelli, 2019)

A pesar de la recopilación de la información, la empresa relacionaba varios aspectos en los cuales se desarrollaba el uso de publicidad de forma cotidiana como se la conoce hoy en día, sino más bien, generaban usuarios con características similares a la información recopilada para enviar publicidad para persuadir a las personas con la publicidad y con los algoritmos que posee Facebook, se estimaba generar cambios a los titulares de su información.

"Una vez que el escándalo estalló Facebook Inc. intentó esquivar las responsabilidades. Acusó a Aleksander Kogan de fraude, de haber "vendido" los datos a Cambridge Analítica y, sin mediación, le suspendió la cuenta." (Vercelli, 2019)

Una que estimó la filtración de los datos personales y fue difundido, la empresa de Facebook expresó su culpabilidad al psicólogo Kogan de ofertar los datos personales a la empresa de Cambridge Analítica, pese a aquello, Facebook suspendió su cuenta. El prestigio de Facebook empezó a ser cuestionado por las filtraciones de la información personal que alojan, por lo cual, el creador de Facebook Mark Zuckerberg pidió disculpas a la comunidad social que fue afectada. No obstante, las disculpas que ofreció el creador de Facebook no fueron las adecuadas, puesto que la información ya fue filtrada de forma ilegítima.

En base a todo lo expuesto por el caso Cambridge Analítica, se determina que, la filtración de los datos personales fueron de forma masiva en contra de la voluntad de las personas generando así polémica entre la ética de Facebook y su creador al permitir este tipo de tratamiento sin consentimiento previo de cada uno de los usuarios afectados ya que se la vulneración de los derechos reconocidos como la honra, imagen, datos personales, buen nombre, no estima que, allegados tuvo acceso dicha información proporcionada puesto que únicamente la información adquirió el psicólogo Kogan, generando la gran incógnita si la información tratada de forma ilegal fue transferida a personas externas de su investigación para tratar la información sea por terceras personas u diferentes administradores de diferentes

plataformas por lo cual, el derecho a la protección de datos personales se ha visto incurrido a múltiples vulneraciones de derechos reconocidos.

"Facebook recopila esta información a través de distintas opciones (sentinas), entre ellas las solicitadas al cumplimentar los datos del perfil o la exploración a través de su célebre opción «me gusta»: «Los «me gusta» de Facebook pueden ser usados para predecir automáticamente y con exactitud un rango de características personales altamente sensibles, incluidas: la orientación sexual, la etnicidad, las perspectivas políticas y religiosas, rasgos de la personalidad, inteligencia, felicidad, el uso de sustancias adictivas, la separación de los padres, edad y género» (Kosinskia, Stillwella & Graepelb, 2013)." (Tello, 2013)

La recopilación de información de Facebook demuestra que la otra forma en la que recopilan la información es al momento de interactuar con la red social al darle su uso específico como tal. Según la autora estima que esta información recopilada puede determinar los gustos de cada usuario conforme al algoritmo que constituye Facebook. Con la información proporcionada, la aplicación puede determinar los gustos y el contenido que este desea ver, enganchando más tiempo a la persona a seguir usando y proporcionar más información de la que se estima que es de carácter personal.

2.8.Protección de datos personales en Instagram.

"En internet cada clic, visita o registro se archivan en alguna parte; a esto se le llaman huellas digitales, que viene a ser el ADN digital que los usuarios generan y dejan en plataformas digitales cuando interactúan, incluidas las redes sociales (Muhammad et al, 2018)." (Mendieta Toledo, 2020)

En la forma en cómo se interactúa cada uno de los usuarios de la plataforma de Instagram, se estima el uso mediante el cual decidan en donde la información deberá ser guardad en este sitio así mismo tomando en consideración que esta información proporcionada

se la puede revisar a lo largo de su día, semana, meses y años tomando en cuenta al momento de existir un algoritmo por el cual se registra cada movimiento e interacción la cual se realice en las publicaciones tanto de fotos, videos y demás, queda registrado en una base de datos tal cual como se ha analizado, esta base de datos no cumple con los estándares de seguridad adecuados para garantizar la protección de datos personales en los se estima que proteja la aplicación móvil, en relación con Facebook puesto a su creador **Mark Zuckerberg,** con la compra de la aplicación Instagram esta se acata a las políticas de su comprador no obstante, como se ha analizado las políticas de Facebook relacionadas con Instagram no son las adecuadas puesto que, existe filtraciones de la información personal, vulneración al derecho a la honra, imagen y buen nombre.

En cada interacción que realicemos cada en las aplicaciones móviles ya mencionadas se estima que, se impregna el conocido **"ADN DIGITAL**", que quiere decir esto;;

"Es la capacidad que tiene una organización de absorber y utilizar información, herramientas y tecnologías digitales para el mejoramiento de sus miembros y el progreso." (Wang, 2019)

El ADN digital impregnado por cada usuario es recopilado por la base de datos con el fin de tratar la información por lo cual, es una herramienta que, fomenta el desarrollo integro de la aplicación, la información como ventaja, no obstante, la desventaja que, determina es la recopilación de la información personal que, no es tratada en su debida forma.

"Además, es preciso mencionar que hay redes sociales como Facebook, que permite almacenar tanta información de carácter personal como la ubicación exacta donde se encuentra el usuario, lo que se encuentra haciendo, contactos telefónicos, relaciones familiares, pero, de cierta forma también depende del usuario si permite la visualización de tal información al público, por consiguiente, encontramos otras redes sociales como Instagram, Twitter que al igual que Facebook permiten compartir fotos e imágenes en tiempo real, que al estar a la visualización publica de una

determinada cantidad de contactos que se tenga pueden ser utilizados con fines delictivos vulnerando, la intimidad de las personas." (VULNERACIÓN DEL DERECHO A LA INTIMIDAD EN REDES SOCIALES: UNA REALIDAD SOCIOJURÍDICA, 2020)

En sentido estricto por regla general la aplicación de Facebook posee la capacidad de almacenar la información de cada usuario exponiendo sus datos sensibles como tal, lo mencionamos la empresa de Facebook al momento de comprar Instagram se acoge a sus políticas permitiendo a sus usuarios exponer su información sensible siempre y cuando lo deseen, no obstante, el uso mal intencionado de estos datos sensibles no exime de ninguna responsabilidad penal a la persona que, realice dicho acto malicioso, en cuanto a Instagram la publicación de fotos y videos que, se considere sensible se encuentra en todo sentido por el hecho que, las personas pueden acceder a dicha información libre y voluntariamente sea la cuenta o usuario se encuentre en acceso para todo público u en privado el otorgar el consentimiento inequívoco genera esta vulneración de los derechos fundamentales reconocidos.

Cuadro 5

Pregunta	E1	E2	E3
3. ¿A través de que redes sociales se produce frecuentemente la vulneración de derecho a la intimidad?	• Whatsapp. • Youtube. • Facebook. • Instagram. • Twitter.	• Whatsapp • Youtube • Facebook • Instagram • Twitter • Skype	• Facebook • Whatsapp • Youtube • Twitter • Googl • Linkedin, Instagram
Interpretación			
• Las entrevistas realizadas, tuvieron como resultado que los mallas sociales por las cuales se produce con frecuenta la vulneración a la intimidad Whatsapp, Youtube, Facebook, Instagram,Twitter.			

IMAGEN 2; FUENTE; (Salazar Ramon, 2022)

La encuesta realizada por el autor en el cuadro 5, Salazar Ramón, Dante Francisco demostró que, la vulneración de datos personales son persistentes en las aplicaciones mencionadas con relación a una filtración de información es masiva por cada uno de los usuarios no obstante, en la aplicación de Instagram proporciona a cada uno de los usuarios la posibilidad de publicar su información por lo cual, está sujeto a que, la información proporcionada en la red social de Instagram sea objeto de actos maliciosos tomado en consideración que, estos actos realizados no exime de cualquier tipo de responsabilidad penal en cualesquiera de los casos como ya se vio analizado en caso de Facebook, esta aplicación de igual forma recaba información y las resguarda en una base de datos en la que, los usuarios no poseen conocimiento del mismo y del tratamiento proporcionado.

"Para Ortega et ál., 2018 nos muestra el caso examinado por la Corte donde se hace un análisis sobre la cantidad de usuarios que se encuentran en las redes sociales, determinando que las mismas tienen alto impacto e influencia de personas, por lo tanto, al publicar una información y opinión, estas alcanzarían a tener un alcance masivo permitiendo a terceras personas tener acceso a dichas publicaciones; poniendo en peligro derechos fundamentales como el buen nombre, la honra, el honor, la imagen, entre otros." (VULNERACIÓN DEL DERECHO A LA INTIMIDAD EN REDES SOCIALES: UNA REALIDAD SOCIOJURÍDICA, 2020)

El presente autor expresa una divulgación masiva de información personal u datos sensibles en la aplicación de Instagram o cualquiera en la que, se concentre para recopilar información la cual puede ser perjudicial para el entorno social en donde una personas se la encuentra, hay que ser puntuales es propenso a ser objeto de actos en su contra dependiendo el caso en específico la filtración de estos datos o el uso indebido sin previo consentimiento ha sido perjudicial en el año 2024 ya que, la información proporcionada no toma riendas a ser reguladas pese a la determinación políticas de seguridad no es suficiente para establecer parámetros de seguridad en los que, permita que la información sea protegida de manera eficiente para los usuarios que, son afectados por este tipo de vulneración de los derechos fundamentales y de sus datos personales por el tratamiento indebido que se proporciona.

2.9.Protección de datos en WhatsApp.

La aplicación móvil de WhatsApp es un sistema informático que hace relación a la mensajería instantánea la cual, fortalece la comunicación con determinadas personas las que esta requiere de un número telefónico para poder brindar los servicios de comunicación a través de esta aplicación, conforme va evolucionando dicha aplicación, los sistemas de seguridad deben hacer conjuntamente para evitar que, la información proporcionada sea resguardada en su base de datos correspondiente a su tratamiento como tal, llegar a las dilaciones injustificadas que atente contra la integridad personal de cada persona utiliza los servicios de la aplicación.

"La agenda se escanea periódicamente y los contactos son guardados en una base de datos de la aplicación en formato SQLite denominada "wad" y cuyo contenido esta descrito más adelante" (M. M ÓJICA L ÓOPEZ, 2017)

La aplicación de WhatsApp, funciona con el previo registro de contactos a nuestros dispositivos móviles los cuales contiene el número de teléfono en el cual se contacta con la persona por la aplicación de WhatsApp registra los contactos paulatinamente en determinados tiempos y son enviados a la base de datos de WhatsApp por lo cual, contiene la información personal de cada uno de los contactos son registrados día a día en la aplicación móvil.

"Al almacenamiento externo del teléfono se tiene acceso total, de lectura y escritura por parte de aplicaciones y usuarios. Aquí se almacenan todos los archivos multimedia que se envían y reciben (fotos, audios y videos) sin ningún tipo de cifrado. En cambio, las conversaciones sí se guardan en una base de datos cifrada, pero, a pesar de ello, algunos investigadores han conseguido recuperar la clave de cifrado." (M. M ÓJICA L ÓOPEZ, 2017)

"El almacenamiento interno del teléfono es una zona de memoria más interesante ya que, a pesar de que solo es accesible desde terminales "rooteados" (un móvil "rooteado" es aquel cuyo sistema operativo ha sido modificado para tener control total sobre ´el), toda la información aquí almacenada carece de cifrado. En esta zona podemos encontrar las bases de datos que almacenan las conversaciones, las fotos de perfil de los contactos, sus estados, etc." (M. M ÓJICA L ÓOPEZ, 2017)

Se denota la forma en la que, la aplicación registra la información tanto en el dispositivo móvil de forma externa como interna como tal, esta base de registro que, realiza WhatsApp de manera periódica almacena toda la información en el dispositivo y la base de datos interna al dispositivo para el tratamiento de la información por lo cual, en un primer aspecto dicha información almacenada es cifrada por los administradores no obstante, el acceso a las

conversaciones, imágenes, fotos, videos y audios son expuestos por el mismo dispositivo exponiendo chats y multimedia que, puede perjudicar a la personas a quien se trata su información.

"La aplicación se divide en dos partes bien diferenciadas:

- *El módulo encargado del escaneo de los usuarios de WhatsApp y la visualización de los datos. Esta es la parte que se encarga de actualizar la agenda de contactos, copiar las bases de datos de WhatsApp, rellenar las bases de datos propias de la aplicación y por ´ultimo mostrar los resultados obtenidos.*
- *El módulo de grabación de movimientos. Esta parte es la que automatiza todo el proceso anteriormente comentado. Se trata de un sistema de grabación de clics y movimientos del ratón que permite reproducirlos más tarde automáticamente."* (M. M ÓJICA L ÓOPEZ, 2017)

Se denota la forma en la que, la aplicación registra la información tanto en el dispositivo móvil de forma externa como interna como tal, esta base de registro que, realiza WhatsApp de manera periódica almacena toda la información en el dispositivo y la base de datos interna al dispositivo para el tratamiento de la información por lo cual, en un primer aspecto dicha información almacenada es cifrada por los administradores no obstante, el acceso a las conversaciones, imágenes, fotos, videos y audios son expuestos por el mismo dispositivo exponiendo chats y multimedia que, puede perjudicar a la personas a quien se trata su información.

Cuadro 6

	Contenido	Directorio	Fichero
1	Imágenes	/data/data/com.csic.whatsappscan/files/	<telefono>_<número_de_orden>.png
2	Fichero de la grabación	/data/data/com.csic.whatsappscan/cache/	eventsRecord.log
3	Base de datos de WhatsApp	/data/data/com.csic.whatsappscan/databases/	wa.db
4	Base de datos de WhatsappScan	/data/data/com.csic.whatsappscan/databases/	spy.db

Cuadro 6, Nota: Obtenido de, M. M ÓJICA L ÓOPEZ, J. L. (2017).

El presente cuadro 6, se puede observar los datos escaneados por parte de la aplicación WhatsApp, son destinados a diferentes puntos del almacenamiento interno del dispositivo además de los datos son enviados a una base de datos propiamente son desarrolladores de la aplicación, cada fichero u dato contenido en el dispositivo contiene su registro único diferenciándose de los demás permitiendo identificar la información de una forma mucho más detallada y exacta.

En Ecuador no se estima que, la protección de datos personales no es la adecuada en cuanto al tratamiento brindado de la información personal no es la correcta ya que, las filtraciones indebidas sin consentimiento de los titulares degeneran a la vulneración de los derechos reconocidos en la constitución de Ecuador, siendo víctimas de injurias en su contra, acciones que atentan contra la integridad, honra, imagen y buen nombre.

2.10. WhatsApp Plus

El servicio de WhatsApp plus es una aplicación la cual proviene de WhatsApp, con características diferentes y similares en todo sentido, no obstante, esta aplicación con denominación “Plus”; otorgar al usuario accesos indebidos en la que, el usuario puede acceder a imágenes eliminadas, mensajes eliminados, estados publicados y posteriormente son eliminados vulnerando los derechos reconocidos en la constitución.

Imagen 2

Imagen 2; Elaboracion propia, por motivos de privacidad no se expone los chats del usuario.

Imagen 3

Imagen 3, Elaboración propia, por motivos de privacidad no se expone los chats del usuario.

Como se puede observar los dos tipos de WhatsApp cumplen con las mismas funciones de mensajería instantánea como se puede observar en imagen 2 y 3, no obstante, la imagen 2 es representado por WhatsApp Plus a comparación de la segunda imagen (2), es presentado por la aplicación WhatsApp que, comúnmente se utiliza, en la imagen 2 se puede observar diferentes funciones que, WhatsApp normal no posee como es el “modo avión” y el modo “fantasma”.

Como se puede observar, presenta la función de "Modo Avión", esta facilita la desconexión de mensajería instantánea como si la persona no estuviera conectada a internet.

Imagen 4; Elaboración propia, por motivos de privacidad no se expone los chats del usuario.

Como se puede observar, el "modo fantasma", brinda el acceso a que, el usuario interactúe de forma normal en la aplicación WhatsApp, con la condición de que, toda interacción no será visible para los demás usuarios.

Imagen 5, Elaboración propia, por motivos de privacidad no se expone los chats del usuario.

Imagen 6, Elaboración propia, por motivos de privacidad no se expone los titulares de los estados del usuario.

Imagen 7, Elaboración propia, por motivos de privacidad no se expone los titulares de los estados del usuario.

Como se puede observar en la imagen 4 un usuario comparte su información en un estado de WhatsApp sin ningunt itpo de inconvenientes, se determina la vulenracion de esta imagen u dato contedio en el Estado por el hecho que, la aplciacon de WhatsApp Pluss permite el acceso a la imagen sin ningun tipo de consentimietno como se puede observar en la imagen 5 por lo cual, este acceso a esta informacion vulenra el derecho a la intimidad de la persona sin tomar en concideracion que, no se determina un numero exacto de usuarios que posean dicha aplicación "Plus", la vulenracion del erecho a la intimidad esta presente en todo momento tanto en Estados publicados, como mensajes de texto, imágenes y videos.

La aplicación plus de whatsApp, es una fuente de vulneracion de derechos fundametnales en Ecuador por lo cual, su adquisicion no es nada complejo ya que, esta se encuentra en diferentes paginas webs que, permiten el acceso como tal de esta aplicación, sin la necesidad del consentimiento del titular de su informacion siendo que estos derechos vulnerados versan sobre la afectación que pueden llegar a tomar las acciones maliciosas de los terceros que adquieren la información.

2.11. Caso No. 2064-14-EP

La presente sentencia emitida por la corte constitucional a fecha 27 de enero de 2021, trata el tema de los datos personales que, presenta una acción de habeas data cancelatorio con la finalidad de eliminar datos que, son difundidos en la aplicación WhatsApp impedir el contenido sensible que fue divulgado en la aplicación móvil. La corte expresa que, se considera datos sensibles en la divulgación de información en la aplicación de WhatsApp, la corte constitucional evaluó la dimensión de un dato sensible otorgado por los usuarios a terceras personas.

En primer lugar, establece la dimensionalidad del habeas data,

"Art. 92.- Toda persona, por sus propios derechos o como representante legitimado para el efecto, tendrá derecho a conocer de la existencia y a acceder a los documentos, datos genéticos, bancos o archivos de datos personales e informes que sobre sí misma, o sobre sus bienes, consten en entidades públicas o privadas, en soporte material o electrónico. Asimismo, tendrá derecho a conocer el uso que se haga de ellos, su finalidad, el origen y destino de información personal y el tiempo de vigencia del archivo o banco de datos." (CONSTITUYENTE, 2008)

El habeas data se refiere directamente a, los titulares de su información y la capacidad la cual poseen para acceder a sus archivos sean personales, informes, archivos los cuales, se encuentren en diferentes entidades tanto públicas como privadas, con la facultad de conocer la forma en la que, su información personas va a ser tratada tanto en documentación, informes y datos en general que, sea contendió bajo cualquier dispositivo electrónico o documentación en físico.

2.11.1 ¿Se considera las fotografías intimidas y personales como datos personales?

"La corte constitucional analiza el alcance de las fotografías si constituye dato personal y define: Con base en todo lo anterior, se concluye que las fotografías efectivamente constituyen datos personales, mismos que se encuentran amparados bajo la garantía jurisdiccional de hábeas data, en virtud de que, habiendo considerado los medios que razonablemente pueda emplear un tercero para identificar al titular, se ha determinado que en efecto estos datos permiten identificar a la parte actora, aun cuando en algunas de ellas a simple vista no se logre desprender su identidad." (Constitucional, 2021)

La corte constitucional reconoce que, las fotografías forman parte de los datos personales reconociendo que, están resguardadas por la garantía del habeas data y sus 5

dimensiones por lo cual, el titular de la información viera conveniente realizar para su tratamiento, en Ecuador este reconocimiento como tal, ha formalizado la garantía que, la información va a ser protegida ya que, la imagen logre reconocer al titular de la información se considera como dato personal.

"En conclusión, esta Corte encuentra que se ha configurado un tratamiento no autorizado de datos personales, por parte de la demandada, de las imágenes íntimas y personales de la parte actora. Motivo por el cual, se procederá a analizar si es que lo anterior tiene consecuencias con relación a la vulneración de derechos constitucionales y, por ende, está protegido por la acción de hábeas data." (Constitucional, 2021)

La corte analizo además el tratamiento que, recibió la divulgación de estos datos personales de la parte actora determinado que, no fueron los adecuados ya tomado en consideración que, sin el consentimiento de la titular de la información se divulgo a terceras personas ajenas a la parte actora degenerando vulneraciones al derecho a la intimidad, honra, imagen y buen nombre del titular.

"En conclusión, esta Corte encuentra que se ha configurado un tratamiento no autorizado de datos personales, por parte de la demandada, de las imágenes íntimas y personales de la parte actora. Motivo por el cual, se procederá a analizar si es que lo anterior tiene consecuencias con relación a la vulneración de derechos constitucionales y, por ende, está protegido por la acción de hábeas data." (Constitucional, 2021)

En base a todo lo analizado por la corte constitucional en el presente caso determina que, las fotografías forman parte de datos personales de los titulares que envían dicha información por lo cual, dicha divulgación sin previo consentimiento puede llegar a acarrear sanciones penales por vulnerar los derechos fundamentales tal como lo hemos tratado en el capítulo anterior de los titulares de su información catalogando que, dicha información posee

la calidad de ***dato sensible***, este dato sensible está sujeto a toda garantía jurisdiccional para evitar tratos maliciosos de la información que, se proporciona en la aplicación móvil WhatsApp.

En conclusión del presente capítulo las otras aplicaciones más utilizadas a nivel nacional y mundial se ha determinado que, no cumple con todos los estándares de seguridad se estima que realicen en consideración con el trato maliciosos de la información por parte de terceros y de la administración misma de los desarrolladores no se determina la seguridad adecuada para proteger los datos personales y datos sensibles de los titulares, estando sujetos a vulneración de los derechos fundamentales reconocidos en la constitución de Ecuador puesto que, el uso indebido de Facebook, Instagram y WhatsApp, recopila información que, el titular proporciona de forma masiva ante un consentimiento inequívoco de proporcionar su información ante la redes sociales tratadas pese a que, existe vulneración de los datos personales de cada titular o usuario de su información no existe una garantía solidad de resguardo, protección y tratamiento garantizado del mismo la falta de información de los términos de políticas y seguridad de la aplicaciones tratas en este capítulo no cumple con los estándares básicos de seguridad en la informática ya que, a nivel mundial se determinó el trato inadecuado de información proporcionada por los desarrolladores de Facebook otorgando a empresas que, no tiene anda que ver en cuanto al tratamiento de esta información mientras que, el usuario siga proporcionando más información en las redes sociales seguirá aumentando el riesgo de vulneración de sus derechos fundamentales.

Capítulo III

Objetivo de aprendizaje: Como se ha determinado en el posterior capitulo se ha determinado la existencia de la vulneración de los derechos fundamentales por lo cual se va a determinar qué tipo de sanciones recae el tratamiento indebido de los datos personales u datos sensibles.

3. Sanciones por vulneración de derechos fundamentales en el tratamiento de datos personales y sensibles

La vulneración de los derechos fundamentales, en el uso adecuado de las aplicaciones móviles ya tratadas en la aplicación de Facebook, Instagram, WhatsApp, ha generado polémica por el simple hecho que, el tratamiento que, brinda Ecuador no es el adecuado por lo cual, una adecuada protección de los datos personales se envuelve en diferentes conflictos por actos maliciosos ocasionados por cada persona que accede a esta información acarreando a sanciones penales para poder garantizar la protección de estos derechos reconocidos.

3.1.¿Qué es infracción penal?

"Art. 18.- Infracción penal. - Es la conducta típica, antijurídica y culpable cuya sanción se encuentra prevista en este Código." (Nacional, 2024)

El código orgánico integral penal expresa, la infracción penal es aquella conducta detallada en el presente código expresando que, cada una de las acciones van en contra de la ley siendo culpable en relación a la acción que realiza en contra de la voluntad de otra persona y en cuanto a la sanción hacemos una referencia de una manera directa en el Código Orgánico Integral Penal al omento de aplicar una sanción adecuada en las acciones antijurídicas tomando en consideración el poder punitivo del Estado.

El presente condigo expresa dos tipos de infracción penal, primero las "**Contravenciones"** y el segundo los "**Delitos";** en el presente análisis trataremos directamente

los delitos en relación a las aplicaciones móviles diferenciando el **delito** y **delito informático**, cada una de ellas con características diferentes que, los diferencia por lo cual, el **Delito es,** según una concepción formal lo expresa como,

"Establecen que el delito es una conducta humana que se opone a lo que la ley manda o prohíbe bajo la amenaza de una pena." (MACHICADO, 2010)

Según el presente autor expresa que, el delito es aquella acción que comete una persona y este está reconocido en el ordenamiento jurídico como acción que, se prohíbe con la finalidad de que, si comete una acción prohibida este será sancionado con una pena privativa de libertad restringiendo el derecho a la libertad por la acción antijurídica y culpable en contra de una tercera persona vulnerado sus derechos fundamentales y reconocidos por la constitución e instrumentos internacionales.

Dichas acciones corresponden a una persona o grupo de personas realicen acciones las que, se encuentren en contra de la normativa u la ley afectando los derechos de las personas que no han cometido ningún tipo de acción penal por regla general estas acciones se realizan de forma presencial u sistematizada en un entorno social o lugar determinado para una comisión de dicho delito.

A diferencia del delito informático según la autora Davara Rodríguez define al delito informático como:

"La realización de una acción que, reuniendo las características que delimitan el concepto de delito, sea llevada a cabo utilizando un elemento informático/o telemático, o vulnerado los derechos del titular de un elemento informático, ya sea hardware o software." (Rivadeneira & Pino, 2013)

"Delincuencia informática es todo acto o conducta ilícita e ilegal que pueda ser considerada como criminal, dirigida alterar, socavar, destruir, o manipular, cualquier sistema informático

o alguna de sus partes componentes, que tenga como finalidad causar una lesión o poner en peligro un bien jurídico cualquiera." (Rivadeneira & Pino, 2013)

Se considera que, los actos que constituyan delito informático debe concadenarse con el uso de sistemas informáticos que llegan a ser, PC y dispositivos móviles para vulnerar los derechos fundamentales de los titulares por lo cual, el delito informático recaba sus acciones en adquirir de forma ilegal datos personales u datos sensibles de cada persona que, sea víctima de aquello por el uso inadecuado que, se brinda al información o se tiene acceso sin los permisos brindados por el titular, expresando que, la alteración de la información adquirida puede ser perjudicial para los titulares de su información.

3.2.Finalidad del Delito Informático.

Según el autor, Parker establece las finalidades del Derecho Informático,

Propósito de investigación de la seguridad	Abuso informático es cualquier acto intencional o malicioso que involucre a un computador como objeto, sujeto, instrumentos o símbolo donde la víctima sufrió o podría haber sufrido una perdida y el perpetrador obtuvo o pudo haber obtenido una ganancia (Parker, Nycum And Oura, 1973).
Propósito de investigación y acusación	Delito informático es cualquier acto ilegal cuya perpetración, investigación o acusación exige poseer conocimiento de tecnología informática (Departamento de Justicia de Estados Unidos).

Propósito legal	Delito Informático es cualquier acto tal como está especificado en una ley sobre delito informático en la jurisdicción en que la norma se aplica
Otros propósitos	Abuso informático (sea cual sea su objetivo), es cualquier delito que no puede ser cometido sin computador.

Cuadro 7, Elaboración propia del Cuadro.

Fuente Bibliográfica: Rivadeneira, J. J., & Pino, S. A. (2013).

Según el autor Parker, en el cuadro 7 expresa determinadas finalidades que puede tomar el cometimiento de un delito informático, con relación al uso indebido de los sistemas exponiendo gravemente la información de los usuarios siendo estos propensos a la pérdida de su información como primer aspecto que se considera un uso indebido expone a los titulares en relación a la información y la presencia de un agresor el cual posee conocimiento del uso de los sistemas informáticos o de tecnología como tal para poder acceder a esta información adquirida de forma ilegal no obstante, los diferentes medios de investigación legal no son los adecuados para llegar con el presunto titular de la acción penal ya que, la persecución que realizan no es la forma adecuada ya que, por falta de sistemas tecnológicos lo cuales brinden apoyo al momento de investigar un delito informático a pesar de, establecer conductas típicas antijurídicas y culpables no es suficiente para procesar a los presuntos actores del delito existiendo un abuso informático en la sociedad por la adquisición de información de forma ilegal que va en contra de los derechos reconocidos en la constitución de Ecuador y a su falta de preparación informática en esta rama de derecho las violaciones a estos derechos fundamentales aumentan drásticamente conforme el uso de las aplicaciones móviles se van evolucionando.

Estas cuatro finalidades que persigue el derecho informático el autor ha manifestado que, concierne al patrimonio de los titulares de las mismas ya que, son mucho más propensos a ser víctimas de estos delitos informáticos haciendo relación que, puede desencadenar una serie de vulneraciones como se ha mencionado al derecho a la honra, imagen, buen nombre entre otras más únicamente no se requiere del uso de sistemas computarizados considerando desde el uso de dispositivos móviles se puede acceder a información de carácter personal cumpliendo con el cuarto punto del cuadro 7 ya que, cumple con la finalidad del tratamiento indebido de la información con propósitos muy ajenos a los tres primeros ya que pertenecen al carácter patrimonial y no de datos personales como tal.

En cuanto al uso con las aplicaciones móviles tratadas en el capítulo anterior la víctima es mucho más propensa a ser afectado por un delito informático dicha información la cual pasa todos los días el tráfico de datos al ser masivo no existe regulaciones especificas pese que, en Ecuador exista la ley de protección de datos personales no quiere decir que, el tratamiento en las aplicaciones es de forma adecuada.

3.3.Características del delito informático.

1. ***"Dependencia de la tecnológica:*** *la relación estrecha con la tecnología hace que los usuarios se conviertan en dependientes de ella.*
2. ***Anonimato y suplantación de identidad:*** *la relativa facilidad para "desparecer" en el mundo virtual dificulta el rastreo de los responsables de acciones maliciosas u ilegales. Además, es sencillo para el atacante hacerse pasar por quien no es encubrir su identidad.*
3. ***Facilidad de adaptación:*** *las herramientas pueden ser modificadas fácilmente para adaptarse al medio y a las dificultades encontradas durante su empleo.*
4. ***Escalabilidad:*** *un solo programa dañino (o ataque o transacción) puede generar grandes ingresos (más por menos).*

5. ***Universalidad de acceso:*** *cualquiera puede convertirse en un delincuente porque las herramientas "están al alcance de todos", al igual que las víctimas.*
6. ***Proliferación de herramientas y códigos:*** *este ítem se encuentra relacionado directamente con el punto anterior, ya que internet provee las herramientas necesarias para que cualquier persona con escasos conocimientos pueda llevar adelante un delito informático.*
7. ***Dificultad para perseguir a los culpables:*** *las jurisdicciones internacionales son un escollo difícil para establecer legales y llegar a un atacante.*
8. ***Intangibilidad de las pruebas:*** *teniendo en cuenta que este tipo de delitos se llevan a cabo en el mundo virtual obtener pruebas válidas y lograr que la corte las comprenda y considere reviste una cierta dificultad.*
9. ***Grupos de delincuentes profesionales:*** *miles de grupos integrados por distintos personajes con diversos niveles de conocimiento técnico, legal y financiero (trabajo interdisciplinario) logran una profesionalización del cibercriminal difícil de imaginar.*
10. ***Escasa conciencia por parte del usuario:*** *el mismo suele utilizar cualquier tipo de tecnología sin recibir capacitación al respecto."* (Rivadeneira & Pino, 2013)

Las características del delito informático plantea diferentes características en la que puede realizar un delito informático sea este porque la tecnología avanza drásticamente y la sociedad se hace mucho más dependiente a ella en sentido estricto, el uso indebido de este a generado que los atacantes puedan utilizar información falsa para acceder a ella y fácilmente ocultar sus acciones maliciosas en contra de las victimas limitando el acceso a ser reconocidos e identificados, en las aplicaciones móviles las personas que adquieren esta información con cuentas falsas permanecen en el anonimato para el cometimiento del delito informático por lo cual la aplicación al ser dañina para el titular con previo consentimiento forzosos que exige la

aplicación con el desconocimiento del mismo no permite la protección segura ya que, la persona que está dispuesta a realizar dicho acto ilícito incurre a que este delito con conocimiento y con las herramientas que se encuentran disponibles para cada usuario tomando en consideración que, internet facilita el acceso a sistemas que facilitan la adquisición de los datos personales de los titulares de su información además del uso de la aplicación misma la adquisición indebida aumenta el riesgo de los datos personales a ser adquiridos, a nivel legal la adquisición de las pruebas pueden resultar difíciles de adquirir puesto que, se debe determinar si la información proporcionada en la aplicación móvil u dispositivo eléctrico del presunto infractos corresponda a ser verídica sin ningún tipo de alteraciones por lo cual, los sistemas legales adoptan programas y medios que faciliten la verificación de la información no obstante a nivel, legal posee su grado de complejidad al momento de adquirirlo como tal, ya que para este cometimiento de delitos las personas inconscientemente brindan la información personal sin conocer los riesgos potenciales que, estos pueden provocar u generar en el entorno social en el que se encuentra.

3.4.Bien jurídico protegido en delito informático.

El bien jurídico protegido en relación a los delitos informáticos se debe tomar en cuenta que, los delitos tradicionales deben ser adecuados con el uso de las aplicaciones móviles y en general con sistemas informáticos por lo cual, consideramos que los bienes jurídicos protegidos determinar la forma en la que, se va realizar la persecución del mismo.

Al referirnos de bienes jurídicos protegidos en delitos informáticos son bienes intangibles puesto que, esta vulneración no es física en contra del titular de la información, no obstante, a diferencia del bien tangible estos requieren de daños físicos, sexuales entre otros que, demuestre el acto lesivo en contra de la persona.

“En fin la protección de la información como bien jurídico protegido debe tener siempre en cuenta el principio de la necesaria protección de los bienes jurídicos que señala que la

penalización de conductas se desenvuelva en el marco del principio de "dañosidad" o "lesividad". Así una conducta solo puede conminarse con una pena resulta del todo incompatible con los presupuestos de una vida en común pacifica, libre y materialmente asegurada." (Rivadeneira & Pino, 2013)

Señala que, la información en los sistemas informáticos forma parte como bien jurídico que se debe proteger las conductas indebidas al mal uso de dicha información debe ser sancionada conforme lo disponga el código orgánico integral penal en relación con las amenazas en dispositivos electrónicos son constantes pese a la educación de seguridad informática que se posea no es suficiente para proteger los datos personales de cada uno de las personas de cualquier forma se va a ser víctima de estas acciones maliciosas, además del bien jurídico protegido de la información se hallan inmersos 4 bienes jurídicos más.

*"**El patrimonio,** en el caso de la amplia gama de fraudes informáticos y las manipulaciones de datos que da a lugar.*

***La Reserva, La Intimidad Y Confidencialidad De Los Datos,** en el caso de las agresiones informáticas a la esfera de la intimidad en forma general, especialmente en el caso de los bancos de datos.*

La Seguridad o fiabilidad del tráfico jurídico y probatorio, en el caso de falsificaciones de datos o documentos probatorios vía medios informáticos.

***El derecho de propiedad,** en este caso sobre la información o sobre los elementos físicos, materiales de un sistema informático, que es afectado por los de daños y el llamado terrorismo informático."* (Rivadeneira & Pino, 2013)

Estos bienes jurídicos que, protege en el derecho informático hace referencia a un patrimonio de los titulares de la información se encuentra envueltos ante acciones maliciosas y manipulación vulnerando la intimidad de los usuarios para ello, se estima que la información

es confidencial y estos posee un carácter de datos sensibles ocultándolo ante terceros que intenten atentar contra este derecho tomando en cuenta la seguridad informática al ser primordial en las aplicaciones móviles ya tratadas en el capítulo anterior para poder prevenir el tratamiento indebido de los mismos estableciendo bases legales sólidas para protegerlos como tal, el bien jurídico protegido en el ámbito informático debe ser de gran importancia por la constitución de Ecuador garantiza y protege estos derechos fundamentales con la finalidad que, los titulares de su información personales y/o datos sensibles pueden llevarse a cabo bajo un tratamiento adecuado y optimo no obstante, las acciones maliciosos se encuentran inmersas en diferentes ámbitos por aquellos que actúan de forma que va en contra de derecho la vulneración de estos bienes jurídicos implica una serie de consecuencias para los titulares de su información vulnerada ya que, los derechos protegidos en estos como la honra, intimidad, protección de datos personales, datos sensibles y buen nombre se encuentran intrínsecamente relacionado a una determinación de acuerdo al entorno social entraña actos maliciosos que se genera en su contra, la vulneración de estos derechos al ser reconocidos como bienes jurídicos son reconocidos como tal para su protección y resguardo para evitar y sancionar con penas privativas de libertad para garantizar un correcto funcionamiento del sistema punitivo de Ecuador.

3.5.Tipicidad de los delitos informáticos de Ecuador en el uso de aplicaciones móviles.

En Ecuador existen delitos informáticos que, son tipificados en el Código Orgánico Integral Penal para garantizar los derechos protegidos y reconocidos por la constitución puesto que como se ha determinado al vulneración de los datos personales en las aplicaciones móviles de Facebook, Instagram y WhatsApp, los titulares de la información son propensos a ser víctimas de cualquier tipo de delito informático pese a los sistemas de seguridad brindados por los desarrolladores de las aplicaciones mencionadas esta vulneración puede ser realizada tanto

por personas jurídica como privadas quienes, con el conocimiento necesario pueden acceder a los datos personales u sensibles de personas que, se encuentran en las aplicaciones móviles aprovechando el desconocimiento de las demás personas.

Este cumple con 3 elementos específicos para la constitución del delito informático, el primero es el **sujeto,** que es determinado por la persona autora del delito informático, en segundo orden el **medio,** por el cual corresponde al sistema con el que va a cometer el acto ilícito y como tercer punto encontramos el **objeto,** siendo este el beneficio que es otorgado al momento de cometer el delito.

Para poder analizar la tipificación de los delitos informáticos en el Código Orgánico Integral Penal analizaremos la forma en la que, se analiza un artículo del código, **primero¸** se debe entender cuál es la finalidad de la tipicidad de los delitos,

"Art. 1.- Finalidad. - Este Código tiene como finalidad normar el poder punitivo del Estado, tipificar las infracciones penales, establecer el procedimiento para el juzgamiento de las personas con estricta observancia del debido proceso, promover la rehabilitación social de las personas sentenciadas y la reparación integral de las víctimas." (Nacional, 2024)

La finalidad del poder punitivo del Estado es procesar a los presuntos infractores sobre el cometimiento de un delito con la garantía de que, cumplan con un procedimiento de rehabilitación social por lo cual estos puedan ser reinsertados en la sociedad por lo cual, esta es la finalidad que promete el sistema punitivo del Estado para llevar a cabo diferentes programas de rehabilitación social, equilibrando la justicia penal con la protección de los derechos reconocidos en la constitución y tratados internacionales.

En **segundo**, lugar entendamos la forma en la que se interpreta el código orgánico integral penal,

Art. 13.- Interpretación. - Las normas de este Código deberán interpretarse de conformidad con las siguientes reglas:

"1. La interpretación en materia penal se realizará en el sentido que más se ajuste a la

Constitución de la República de manera integral y a los instrumentos internacionales De derechos humanos.

Los tipos penales y las penas se interpretarán en forma estricta, esto es, respetando El sentido literal de la norma.

Queda prohibida la utilización de la analogía para crear infracciones penales, ampliar los límites de los presupuestos legales que permiten la aplicación de una sanción o medida cautelar o para establecer excepciones o restricciones de derechos." (Nacional, 2024)

La interpretación del código orgánico integral penal va a ser en sentido literal en la que, se aplicara el tipo penal con la conducta realizada por el presunto infractor precautelando las interpretaciones arbitrarias por cada uno de los profesionales de derecho para evitar dilaciones en el proceso penal.

En **tercer,** lugar cabe determinar la forma de analizar el tipo penal de una conducta penal en el siguiente ejemplo,

"Art. 178.- Violación a la intimidad. - La persona que, sin contar con el consentimiento

La autorización legal, acceda, intercepte, examine, retenga, grabe, reproduzca, difunda O publique datos personales, mensajes de datos, voz, audio y vídeo, objetos postales, información contenida en soportes informáticos, comunicaciones privadas o reservadas" (Nacional, 2024)

Para el respectivo análisis se debe considerar al **sujeto activo – sujeto pasivo - conducta y Verbo rector**

Sujeto Activo, en la presente norma se relaciona a cualquier persona sea natural o jurídica.

Sujeto Pasivo, hace referencia a la persona afectada sea natural y o jurídica.

Verbo Rector, el verbo rector define la conducta a realizar en este caso, *acceda,*

"intercepte, examine, retenga, grabe, reproduzca, difunda O publique", es la que, determina la acción.

Conducta, es la acción a realizar correlacionado con el verbo rector siendo tal,

"La persona que, sin contar con el consentimiento la autorización legal, acceda, intercepte, examine, retenga, grabe, reproduzca, difunda O publique datos personales, mensajes de datos, voz, audio y vídeo, objetos postales, información contenida en soportes informáticos, comunicaciones privadas o reservadas", es la conducta que va a determinar que el sujeto activo cometa para constituir la tipicidad de la norma establecida

Analizado la forma en la que se debe interpretar la norma penal analizaremos los siguientes delitos tipificados en el código orgánico integral penal con su respecta sanción penal.

"Art. 174.- Oferta de servicios sexuales con menores de dieciocho años por medios electrónicos. - La persona, que utilice o facilite el correo electrónico, chat, mensajería instantánea, redes sociales, blogs, foto blogs, juegos en red o cualquier otro medio electrónico o telemático para ofrecer servicios sexuales con menores de dieciocho años de edad, será sancionada con pena privativa de libertad de siete a diez años." (Nacional, 2024)

El art. 174, del código orgánico integral penal reconoce como delito la oferta sexual con menores de dieciocho años por medios electrónicos se toma en consideración que, los medios electrónicos constituyen a teléfonos móviles u computadoras el sujeto activo en el uso de aplicaciones móviles va a ofrecer servicios sexuales con el uso de menores de adolescentes

considerando que, en el presente tipo penal se aborda temas de delitos sexuales, vulneración de los datos personales, honra, buen nombre, intimidad e imagen ya que, los adolescentes son forzados a dar servicios sexuales por las redes sociales en la que se divulgan datos sensibles no obstante, la persona que ofrezca estos servicios serán sancionados con pena privativa de libertad de siete a diez años.

"Art. 178.- Violación a la intimidad. - La persona que, sin contar con el consentimiento la autorización legal, acceda, intercepte, examine, retenga, grabe, reproduzca, difunda O publique datos personales, mensajes de datos, voz, audio y vídeo, objetos postales, información contenida en soportes informáticos, comunicaciones privadas o reservadas" (Nacional, 2024)

Se reconoce en el Art. 178, como vulneración al derecho a la intimidad y datos personales la persona que acceda a datos sensibles del titular de la información y en relación a las aplicaciones móviles este derecho se ve vulnerado en todo momento por el acceso indebido de la información personal.

Capítulo IV

Objetivo general: Como hemos analizado las sanciones penales que acarrea en Ecuador, se determina que, no posee una gran estructura estricta en cuanto a su aplicación puesto que, se ha determinado varios casos de filtración de datos personales que atente contra la integridad de la víctima por lo cual, en el presente capitulo analizaremos la estructura legal de la ley de protección de datos de Ecuador y la ley de datos personales de España comparando la forma en la que llevan a cabo el tratamiento y a la protección de los datos personales en las aplicaciones tratadas en capítulos anteriores.

4. La protección de datos personales en ecuador y España desde una perspectiva legislativa.

La ley de protección de datos de Ecuador y la ley de datos personales de España comparando la forma en la que llevan a cabo el tratamiento y a la protección de los datos personales en las aplicaciones tratadas en capítulos anteriores ya que cada estado adopta medidas que se considera necesarias para el tratamiento de la información.

4.1.Estado de España

En el estado español, existe lo que se denomina la agencia española de protección de datos, esta normativa establece varias dimensiones con respecto a la protección de datos el cual inclusive añade medidas de prevención para menores de edad y la acarrea responsabilidad tanto para los menores de edad como de igual manera a los padres o tutores de los menores en cuyo caso exista alguna vulneración a esta norma, es decir, la presencia de la existencia de una sanción para los menores de edad y padres o tutores de los menores en caso de infracción alguna en aplicaciones móviles, cuya normativa va más en énfasis a los menores de edad, por la razón que al ser personas vulnerables mayormente a engaños son quienes exponen

información sensible a personas que dan mal uso a las aplicaciones móviles, poniendo en riesgo sus datos personales, sensibles, su imagen, etc.

En la agencia española de protección de datos, como se manifestó con anterioridad, existe medidas de prevención en lo cual se estableció 4 medidas las cuales son las siguientes:

- Marco regulatorio.
- Marco de ejercicio de potestades.
- Marco institucional de educación digital.
- Marco institucional de salud digital.

4.2.Marco Regulatorio.

En este marco manifiesta lo siguiente:

"*Promoverá la adopción de disposiciones complementarias y en desarrollo de la Ley de Protección Integral de la infancia y la juventud."* (datos, 2024)

Establece que el estado será quien desarrolle y ejecute las medidas necesarias para la protección de los datos personales y sensibles de los menores de edad, cuya población es quien más usa las aplicaciones móviles en la actualidad, promoviendo una sociedad de usuarios consientes sobre la información que exponen a sus amigos y terceras personas que puedan observar dicha información al instante que la cual es publicada ante la sociedad.

"Participará activamente en la elaboración de Directrices sobre menores por el Comité Europeo de Protección de Datos en el ámbito del Reglamento general de protección de datos." (datos, 2024)

El estado de España, tendrá participación continua dentro del Comité Europeo, cuya actuación del estado deberá ser de manera conjunta con los otros estados miembros del comité, las normas creadas o reformadas deberán ser incluidas en el estado, en su propia legislación.

"Promoverá la regulación del tratamiento de los neurodatos y los correlativos neuroderechos, especialmente en el ámbito de los servicios dirigidos a menores (videojuegos, realidad virtual, meta verso)." (datos, 2024)

La intervención del estado será directamente en las aplicaciones móviles incluso en la realidad virtual, cuyo apogeo se ve ligado con las aplicaciones móviles, el estado deberá planificar y poner en ejecución estos planes como medidas para prevenir que los menores de edad los cuales usan aplicaciones móviles sean conscientes sobre la información que comparten dentro de aplicaciones móviles, además como debe ser su correcto tratamiento para la protección de los datos personales y sensibles.

En este marco, podemos constatar mediante la intervención del estado para promover normas actualizadas a la realidad, es una vía factible para que se dé un correcto uso de las aplicaciones móviles así llegar a evitar cualquier delito informático, ya que las principales víctimas a estos ciber delitos son los menores de edad los cuales no conocen los riesgos al momento en exponer su información o datos sensibles en las aplicaciones móviles, manifestando de tal forma que son la población con más ataques cibernéticos por el incorrecto manejo de dichas aplicaciones.

4.3.Marco de ejercicio de potestades.

En las potestades se estableció en donde podrá intervenir el estado para ejecutar sea una sanción penal, deberá actuar vago lo siguiente:

"Ejercitará sus potestades sancionadoras, como la limitación temporal o definitiva del tratamiento de datos personales, incluida la suspensión del tratamiento de datos de las páginas web de contenidos pornográficos que vulneren la normativa de protección de datos." (datos, 2024)

Según las potestades otorgadas en esta normativa, podrá actuar para sancionar, inclusive con el cierre total de páginas dedicadas a publicar videos no actos para todo público, aquí interviene las aplicaciones móviles de Facebook, wasap e Instagram, de un modo compaginado, es decir, que mediante estas aplicaciones se puede contactar a personas por un medio de engaños y lo más común son menores de edad, compartan datos sensibles, no obstante, cabe recalar en estas aplicaciones al ser de uso común conteniente dicha información en ocasiones dudosas del actuar de las personas se filtra dicha información a terceros para publicar videos pornográficos en páginas web, por lo cual tiene la potestad de inclusive cerrar dichas páginas que han estado usando datos sensibles que se han filtrado de dichas aplicaciones, quiere decir, que la información, datos personales y sensibles de los usuarios de estas aplicaciones corren el riesgo que se filtre información, como ya sucedió con la aplicación de Facebook sobre su tratamiento incorrecto que venida información de usuarios a cambio de dinero, y dichas aplicaciones al tener el mismo propietario, se tiene una desconfianza sobre el adecuado uso y tratamiento se da a los datos de usuarios, pero que lamentablemente a estar de sus políticas de privacidad se continua con estas afectaciones.

"Apoyará a las autoridades audiovisuales en la promoción de códigos de conducta para la protección de los y las menores en los servicios de comunicación audiovisual y de intercambio de vídeos a través de plataformas." (datos, 2024)

Este método de intervención y ejecución es necesario, ya que al apoyar a personas que saben sobre la seguridad informática, y en el ámbito del derecho informático, se puede exigir la creación de normas sobre un correcto comportamiento para todos los usuarios de las aplicaciones móviles como lo son Facebook, wasap, e Instagram, donde el comportamiento no permitido deberá ser sancionado, haciendo referencia a que las personas deben tener conciencia sobre qué información divulgar y que información no, ya que al ser datos sensibles ponen en riesgo la honra de la persona, su imagen, etc.

"Impulsará la elaboración de códigos de conducta por empresas prestadoras de servicios digitales que incluyan medidas de protección a los y las menores en cuanto al tratamiento de sus datos, la información que se les proporciona y la obtención del consentimiento o el de sus progenitores o tutores." (datos, 2024)

Las normativas creadas por las personas jurídicas que brindan este servicio digital, es necesario, inclusive para los adolescentes y niños que lo utilizan, ya que deben saber cómo su información va a ser utilizada y que datos personales o sensibles no deben compartir dentro de las aplicaciones móviles como Facebook, Instagram y wasap, cuyos datos deben ser tratados cuidadosamente, además se añade como deben actuar los padres o tutores de los menores de edad ante cualquier conflicto que exista y que también sean parte de la educación que deben recibir sobre qué información se puede o no se puede brindar dentro de las aplicaciones móviles mencionadas con anterioridad.

4.4.Educación digital.

La educación dentro de este ámbito es primordial, no solo se incluye a los menores de edad, como hemos analizado existe también una responsabilidad para los padres, representantes legales o tutores, debido a que las aplicaciones móviles como lo es Facebook, wasap, e Instagram, son herramientas de comunicación pero con la alta vulneración de datos sensibles y personales de los usuarios, por lo cual una educación hacia los menores que son más susceptibles a estas filtraciones de terceros es necesaria para que conozcan los riegos que existe y como pueden ser evitados.

La intervención de los padres o tutores del menor para que el consentimiento debe ser necesaria, no obstante por lo general los padres o tutores también desconocen de los riesgos por lo cual se aplica capacitaciones no necesariamente de manera personal si no puede ser con videos en otras plataformas como lo es YouTube, lo primordial a esto es que conozcan sobre

cómo son tratados los datos personales y sensibles y que los comuniquen a sus hijos o representados para así evitar conflictos, cometimiento de delitos cibernéticos, filtración de información personal o sensible, etc.

A continuación, analizaremos que expresa este cuerpo legal sobre la educación digital:

"Colaborará con las Administraciones educativas para dotar al Coordinador de Bienestar y Protección, de obligada presencia en cada centro, de recursos frente a la difusión de contenidos ilícitos en Internet y la violencia digital escolar." (datos, 2024)

Las escuelas y colegios también tienen la potestad de educar a los adolescentes y niños que dan uso a las aplicaciones móviles, ya que el deber de educar únicamente no será de los padres o tutores si no que se añade también a las instituciones educativas, para dar a conocer los riesgos, y como son tratados los datos personales y sensibles, es decir que educando continuamente a los menores de edad se logra que a futuro pueda también a educar a personas que lo necesiten o que no sepan los riesgos de exponer sus datos personales o sensibles en las aplicaciones móviles.

"Colaborará con el Ministerio Fiscal en la concienciación de las responsabilidades en las que se incurren por la difusión de datos personales (imágenes, audios, información) en el ámbito digital, tanto los y las menores como sus progenitores y tutores, y en el ejercicio de las actuaciones a que den lugar los ilícitos penales que se ocasionen." (datos, 2024)

Cuando hablamos de educación, debemos añadir sobre las responsabilidades penales que sanciona la legislación española, es necesario ya que, al dar a entender que actos que sean en contra del marco legal tendrá su respectiva sanción tanto para quien ejecuto el delito, así como los padres tendrán también una responsabilidad en caso de relacionarse con las actividades decidas los menores de edad, es decir si el padre o tutor tiene también un grado de

participación en el delito cometido dentro de las aplicaciones móviles como Facebook, wasap, e Instagram.

"Fomentará el intercambio de buenas prácticas en educación digital entre centros educativos y otros agentes involucrados en la formación de los y las menores." (datos, 2024)

La intervención del sistema educativo con agentes expertos en sistema informático es necesario, ya que al tener expertos para dar conocimiento a los menores de edad sobre los riegos que existe, además que herramientas y la conducta que deben evitar en cualquier conflicto a futuro, ya que los datos personales y sensibles expuestos dentro de estas aplicaciones móviles cuelga de un hilo muy delgado para su filtración y posterior mal uso.

4.5.Bienestar digital.

"Animará y apoyará las iniciativas encaminadas a investigar las consecuencias de un uso inadecuado o adictivo de redes sociales y servicios digitales equivalentes y contribuirá a la difusión de recursos, basados en la evidencia científica y destinados a prevenir, detectar y tratar las situaciones derivadas de este tipo de conductas adictivas." (datos, 2024)

Tendrá la iniciativa principal en analizar sobre los malos usos de los datos personales y sensibles que da las personas al instante de un mal manejo de los mismos, cuyo fin es la prevención, es decir, se identifica primero las causas directas del mal tratamiento de los datos y a su vez se busca lo que sería una solución más factible, con respuesta positiva en poco tiempo para evitar que se siga cometiendo estos malos actos.

4.6.Análisis comparativo con la legislación ecuatoriana.

En el estado ecuatoriano, a diferencia del estado de España, Ecuador ejecuta la protección de datos de una manera alejada a la española, ya que en Ecuador, en el cuerpo legal denominado "LEY ORGANICA DE PROTECCION DE DATOS", la participación de los padres o tutores con respecto a sus datos personales es en la representación de sus datos

personales o sensibles, a diferencia del estado español que hace que sean responsables de este derecho sobre los menores de edad pero no queda únicamente esta función si no que se añade las responsabilidades sean civiles o penales también al padre o tutor del menor si se demuestra la existe participación al momento del cometimiento de delitos entre padre o tutor con el menor de edad dentro de las aplicaciones móviles.

Una diferencia notoria es sobre la inexistencia de los cuatro marcos analizados de la ley española en Ecuador, las diferencias son muy notorias, ya que en España, se busca la intervención continua del estado para prevenir y buscar soluciones al momento del cometimiento de algún delito dentro de las aplicaciones o como evitar el mal tratamiento que se le da a los datos personales o sensibles, añade también una importancia hacia los menores de edad ya que ellos al ser la población con más riesgos en poner expuesto información sensibles de sus padres o tutores, incluso de ellos mismo, son más propensos a ser víctimas de delitos o que su información personal o sensible se filtre por terceros dejando como efecto la vulneración de su imagen, de su nombre etc.

En el cuerpo legal español añade también lo que sería la participación de varias instituciones tanto públicas como privadas para poder brindar el conocimiento necesario a los padres o tutores, así como a los menores de edad sobre los riesgos y como evitar que su información sea filtrada o que eviten ser víctimas de algún delito.

En Ecuador realizando un análisis comparativo con España, la legislación ecuatoriana se queda limitada ante la legislación española, ya que en este estado se da demasiada importancia en el uso correcto de las aplicaciones móviles de Facebook, Instagram y wasap, en el Ecuador no existe esta importancia, demostrando así la falta de interés por parte del legislativo.

Capítulo V

Objetivo general: Como se ha determinado en la legislación española los diferentes medios u características que posee su marco legal de protección de datos con la diferencia con Ecuador se determina las diferentes diferencias que posee cada estado en cuanto a la regulación de los datos personales, en el presente capítulo analizaremos y compararemos el marco legal de la legislación ecuatoriana a diferencia con la chilena.

5. La protección de datos personales en ecuador y chile desde una perspectiva legislativa.

En la legislación chilena su normativa fue promulgada en la década de los noventa y con el paso del tiempo ha tenido actualizaciones por las nuevas tecnologías, y en este caso en concreto por las aplicaciones móviles.

5.1.Finalidad.

"Artículo 1º.- El tratamiento de los datos de carácter personal en registros o bancos de datos por organismos públicos o por particulares se sujetará a las disposiciones de esta ley, con excepción del que se efectúe en ejercicio de las libertades de emitir opinión y de informar, el que se regulará por la ley a que se refiere el artículo 19, N° 12, de la Constitución Política." (PRESIDENCIA, 2023)

Los datos serán protegidos tanto por instituciones públicas como privadas, esto es necesarias, para evitar omisiones por parte de estas, de manera que serán responsables tanto el estado como la entidad privada, únicamente no se podrá regir la normativa cuando se enfoque en aspectos de libertad de expresión estos se enfocará y será tratado en el ámbito constitucional.

5.2.Definiciones.

CUADRO 8

Almacenamiento de datos	*La conservación o custodia de datos en un registro o banco de datos.*
Bloqueo de datos	*La suspensión temporal de cualquier operación de tratamiento de los datos almacenados.*
Comunicación o transmisión de datos	*Dar a conocer de cualquier forma los datos de carácter personal a personas distintas del titular, sean determinadas o indeterminadas.*
Dato caduco	*El que ha perdido actualidad por disposición de la ley, por el cumplimiento de la condición o la expiración del plazo señalado para su vigencia o, si no hubiese norma expresa, por el cambio de los hechos o circunstancias que consigna.*
Dato estadístico	*El dato que, en su origen, o como consecuencia de su tratamiento, no puede ser asociado a un titular identificado o identificable.*

Datos de carácter personal o datos personales	*Los relativos a cualquier información concerniente a personas naturales, identificadas o identificables.*
Datos sensibles	*Aquellos datos personales que se refieren a las características físicas o morales de las personas o a hechos o circunstancias de su vida privada o intimidad, tales como los hábitos personales, el origen racial, las ideologías y opiniones políticas, las creencias o convicciones religiosas, los estados de salud físicos o psíquicos y la vida sexual.*
Eliminación o cancelación de datos	*La destrucción de datos almacenados en registros o bancos de datos, cualquiera fuere el procedimiento empleado para ello.*
Fuentes accesibles al público	*Los registros o recopilaciones de datos personales, públicos o privados, de acceso no restringido o reservado a los solicitantes.*
Modificación de datos,	*Todo cambio en el contenido de los datos almacenados en registros o bancos de datos.*
Organismos públicos, las autoridades	*Las autoridades, órganos del Estado y organismos, descritos y regulados por la Constitución Política de la República, y los*

	comprendidos en el inciso segundo del artículo 1º de la ley N° 18.575, Orgánica Constitucional de Bases Generales de la Administración del Estado.
Procedimiento de disociación de datos	*Todo tratamiento de datos personales de manera que la información que se obtenga no pueda asociarse a persona determinada o determinable.*
Registro o banco de datos	*El conjunto organizado de datos de carácter personal, sea automatizado o no y cualquiera sea la forma o modalidad de su creación u organización, que permita relacionar los datos entre sí, así como realizar todo tipo de tratamiento de datos.*
Responsable del registro o banco de datos	*La persona natural o jurídica privada, o el respectivo organismo público, a quien compete las decisiones relacionadas con el tratamiento de los datos de carácter personal.*
Titular de los datos	*La persona natural a la que se refieren los datos de carácter personal.*
Tratamiento de datos	*Cualquier operación o complejo de operaciones o procedimientos técnicos, de carácter automatizado o no, que permitan*

	recolectar, almacenar, grabar, organizar, elaborar, seleccionar, extraer, confrontar, interconectar, disociar, comunicar, ceder, transferir, transmitir o cancelar datos de carácter personal, o utilizarlos en cualquier otra forma.

Cuadro 8; Elaboración propia del cuadro; Fuente bibliográfica; (PRESIDENCIA, 2023)

Como se puede observar en el Cuadro 8, el estado de Chile, expresa las diferentes definiciones en cuanto a los datos personales a comparación del Estado de Ecuador ya que, encontramos diferentes definiciones como, **almacenamiento de datos** definiéndolo como: el resguardo de la información, **bloqueo de datos,** relacionado con la interrupción de la información del titular, **comunicación o transmisión de datos,** es otorgar la información personal del titular a terceras personas, **dato estadístico,** haciendo referencia a que la información adquirida no puede relacionarse con el titular de la información personal, como entre otras definiciones detallan con más precisión el tratamiento que reciben los datos personales de cada persona en la legislación chilena además que, existe una excepción en el tratamiento de la información que, cuando se trata de libertad de expresión por medio de los titulares este se regirá por la constitución chilena.

5.3.Habeas data chileno.

"El recurso de habeas data puede revestir dos modalidades: una preventiva, cuando tenga por objeto permitir al titular de los datos personales ser informado sobre la existencia de bancos o registros de datos que contengan información que le concierne y, si así fuese, acceder a ellos; y una correctiva, cuando a través de él se exige que determinados datos personales sean corregidos, bloqueados, cancelados, pues el tratamiento que se hace de ellos es indebido, en

el sentido de que vulnera o conculca sus derechos. Así entonces, el habeas data se configura como el instrumento a través del cual los titulares de datos pueden ver protegidos sus derechos frente a acciones que resulten ilegales o arbitrarias o que importen un uso indebido de información de carácter personal que le concierne por parte del responsable del fichero o banco de datos." (Verac, 2018)

El habeas data chileno posee dos finalidades que, se enfocan en corregir y prevenir, la finalidad preventiva es aquella que, brinde el acceso a la información de los titulares de sus datos personales acceder a sus registros que posea cada persona, y la correctiva que cumple con la finalidad de la información de los titulares puede ser modificada, anulada u eliminada actualizada siempre y cuando el titular lo viere conveniente actualizar su información de carácter personal.

A comparación de Ecuador se asemeja en cuanto al habeas data que, cumple con la misma finalidad la cual es acceder a la información de cada uno de los titulares de la información personal además, el habeas data en ecuador posee cinco dimensiones a comparación de la chilena que posee dos dimensiones, ***Habeas Data informativo*** - ***Habeas Data aditivo*** - ***Habeas Data correctivo*** - ***Habeas Data de reserva*** - ***Habeas data cancela torio,*** cada una de ellas cumple con determinadas funciones para la protección de datos personales de los titulares en cuanto a la legislación chile estas dimensiones la expresa en su ley de protección de datos personales en las definiciones y facultades que posee los titulares de su información, ***Bloqueo de datos*** - ***Eliminación o cancelación de datos*** - ***Modificación de datos***, cumpliendo con sus características diferentes y su método de aplicación como tal.

5.4.Principios.

La legislación chile se rige bajo los siguientes principios rectores,

- ***"Licitud de tratamiento****, los datos personales sólo pueden tratarse con el*

consentimiento de su titular o por disposición de la ley."

- ***Principio de finalidad**. Los datos personales deben ser recolectados con fines específicos, explícitos y lícitos. El tratamiento de los datos personales debe limitarse al cumplimiento de estos fines.*
- ***Principio de proporcionalidad**. Los datos personales que se traten deben limitarse a aquellos que resulten necesarios en relación con los fines del tratamiento.*
- ***Principio de calidad**. Los datos personales deben ser exactos y, si fuera necesario, completos y actuales, en relación con los fines del tratamiento.*
- ***Principio de responsabilidad**. Quienes realicen tratamiento de los datos personales serán legalmente responsables del cumplimiento de los principios, obligaciones y deberes de conformidad a esta ley.*
- ***Principio de seguridad**. En el tratamiento de los datos personales se deben garantizar niveles adecuados de seguridad, protegiéndolos contra el tratamiento no autorizado, pérdida, filtración, destrucción o daño accidental y aplicando medidas técnicas u organizativas apropiadas.*
- ***Principio de información**. Las prácticas y políticas sobre el tratamiento de los datos personales deben estar permanentemente accesibles y a disposición de cualquier interesado de manera precisa, clara, inequívoca y gratuita."."* «principios rectores de la ley de datos de chile - Buscar con Google».

Los principios rectores que emana la legislación chilena se rigen con la finalidad del tratamiento de datos personales sea con el consentimiento de un titular para la modificación, cancelación u adición de información, siendo tal que un adecuado procesamiento del uso de la información del titular recae únicamente a su responsabilidad y la norma emanada para el tratamiento además que la recopilación de información de los titulares de la información debe ser exacta y especifica limitando los fines del tratamiento de la información adquirida no

obstante, la información debe ser completa e integra por lo cual brindar la seguridad necesaria debe ser adecuada conforme a las disposiciones legales que requiere la protección de los datos personales con técnicas óptimas para el desarrollo integro como tal.

5.5.Tratamiento de datos.

"Artículo 10.- No pueden ser objeto de tratamiento los datos sensibles, salvo cuando la ley lo autorice, exista consentimiento del titular o sean datos necesarios para la determinación u otorgamiento de beneficios de salud que correspondan a sus titulares." (PRESIDENCIA, 2023)

El tratamiento de datos personales en la legislación chilena se debe cumplir con aspectos muy específicos para el tratamiento de la información ya que, al ser considerado como dato sensibles se requiere de tratamientos muy rigurosos, siendo la **autorización legal,** por parte del titular el estado debe establecer pautas en la que un tratamiento de la información sea adecuada además que, debe existir el **consentimiento del titular**, determina la importancia del titular de la información debe dar el acuerdo u consentimiento para la información personal deba ser tratada mediante las técnicas informáticas de tratamiento sin existir o padecer de dolo y fuerza el consentimiento este tratamiento busca de determinada forma, **beneficios en el área de la salud,** en la cual el titular de la información personal pueda acceder a beneficios de salud para su debido tratamiento por lo cual el tratamiento indebido incurre a perjuicios en contra de los titulares de la información.

A comparación del estado de Ecuador el tratamiento de datos personales de igual forma se debe realizar con el titular quien autorice de manera consentida el tratamiento de su información sea para modificación, cancelación, adición y demás dimensiones las que presente en cuanto al tratamiento de la información, no obstante, este tratamiento lo hace el mismo titular en coordinación con las entidades públicas o privadas que se encuentren a cargo de la información proporcionada, en cuanto la relación que posee este tratamiento de los datos

sensibles con el uso de aplicaciones móviles incurre en, la ley de protección de datos personales en Ecuador nace por la sentencia número, 2064-14-EP en la cual determinan las finalidades del tratamiento y su finalidad de datos personales en cuando al uso de la aplicación de mensajería instantánea WhatsApp no obstante a comparación de chile su ley de protección de datos personales nace a través de la ley 19.628 en el año de 1999, mediante un proyecto de ley propuesto ante el congreso que lo conforma siendo tal una diferencia trascendental entre ambas legislación en las que, el estado chileno asienta como bases legales sobre la protección de los datos personales de cada persona considerando, en relación a las aplicaciones móviles se ha determinado la vulneración de los derechos reconocidos por cada legislación puesto que, no se determina aun la regulación del tratamientos que recibe cada usuario puesto, como se ha determinado en capítulos anteriores que existe la presencia de una vulneración del mismo y el tratamiento malicioso no se estima técnicas adecuadas para llegar a los presuntos responsables de este tiramiento malicioso de la información .

Capítulo VI

Objetivo general, como se ha analizado en los capítulos la vulneración de los datos personales están presentes en el entorno social de las aplicaciones de Facebook, Instagram y WhatsApp, en el presente capitulo analizaremos las sanciones que acarrea la filtración de información en el caso de Instagram, Morgan Stanley y Samsung.

6. Análisis de los casos Instagram, Morgan Stanley y Samsung.

Los presentes casos hacen referencia a la presencia de una filtración de información que se ha llevado a cabo en el año 2022 por parte de la aplicación móvil y las empresas mencionadas accedan a la información y brinden la información a terceras personas vulnerando este derecho reconocido a nivel internacional además que, en cuanto a la aplicación Instagram se enfoca directamente ante el uso y publicación de los datos personales en la aplicación Instagram por la cual varios adolescentes acceden a la aplicación de forma ilegítima utilizando fechas inexactas de nacimiento para ser otorgado su cuenta como tal en el uso de cuentas comerciales.

6.1.Caso Instagram.

El caso Instagram se especifica directamente en el sentido que, menores de edad accedieron a cuentas comerciales filtrando la información de correos electrónicos y demás información de los titulares que así mismos sin ningún tipo de prohibición se toma en consideración que los adolescentes no poseen la capacidad cognitiva eficiente para llevar a cabo dichos actos toda esta información filtrada por los mismos adolescentes al crear su cuenta falsa determina que, no existe regulaciones por parte de los adolescentes en cuanto a la seguridad que proporciona la aplicación.

6.2.Reglamento General de Protección de Datos

La aplicación de Instagram en el presente caso estima que, vulnero el reglamento general de protección de datos conforme lo establece la unión europea para poder tratar los datos personales de cada uno de los usuarios,

"Cualquier persona menor de 18 años tiene automáticamente su cuenta configurada en privada cuando se une a Instagram, por lo que solo las personas que conocen pueden ver lo que publican, y los adultos no pueden enviar mensajes a los adolescentes que no los siguen. Nos comprometimos plenamente con el DPC a lo largo de su investigación, y estamos revisando cuidadosamente su decisión final" (Aguilar R. , 2022)

Se estima que, los menores de 18 años al configurar su cuenta de Instagram son enviados u direccionados de manera predeterminada a cuentas privadas por lo cual la filtración de información es casi nula a excepción de los usuarios u cuentas que aceptan como seguidores quienes podrán tener acceso a las cuentas no obstante, personas adultas no pueden acceder a estas cuentas hasta que el adolescente cumpla con la mayoría de edad, en relación al caso se estima que adolescentes incurren a mentir en su entorno social como lo es en su edad considerando que existe un medio de seguridad idóneo ante la detección de información falsa proporcionada por los adolescentes que acceden de forma maliciosa a la cuenta creada con el propósito de acceder a las herramientas proporcionadas por Instagram.

6.3.Caso Morgan Stanley

La empresa Morgan Stanley fue sancionado por el hecho que, proporciono la información de datos incurre por el hecho que el tratamiento de la información,

"Según la denuncia de la SEC, la firma habría permitido que unos 1000 discos duros (HDD) sin cifrar y unas 8000 cintas de copia de seguridad procedentes de centros de datos clausurados fueran revendidos en sitios de subastas sin haber sido borrados previamente."

(De Nicola, La SEC multa a Morgan Stanley con 35 millones de dólares, por un fallo en la seguridad de los datos, 2022)

Se toma en consideración que, la empresa como tal permitió la venta de la información personal de datos conteniendo datos sensibles como tal determinando que los medios de seguridad empleados por la empresa no fueron los adecuados suscitándose dicho suceso en el año de 2022, el acceso a esta base de datos corresponden a discos duros (HDD), que contiene la información, el acceso a la información por parte de terceras personas es notable ya que, al ser subastado la información no se estima como tal el grado de vulneración de los derechos englobados hacia la protección de datos personales como tal.

"De hecho, en lugar de destruir los discos duros o emplear a un equipo informático interno para borrarlos, Morgan Stanley habría contratado a una empresa de mudanzas no identificada y sin experiencia, supuestamente, en el desmantelamiento de soportes de almacenamiento para que se encargara del hardware." (De Nicola, La SEC multa a Morgan Stanley con 35 millones de dólares, por un fallo en la seguridad de los datos, 2022)

La empresa ignora todos los estándares de seguridad en tal sentido que, realiza una sub -contratación para el tratamiento de cancelación u eliminación de la información, siendo tal que corresponde a una empresa de mudanzas no capacitados para la eliminación de la información expuso un riesgo inminente de los datos personales de cada uno de los titulares de la información por el tratamiento indebido que presto la empresa contratada debido que al no tomar en consideración los estandartes de seguridad la filtración de la información fue inminente y las vulneraciones al derecho a la privacidad fue a gran escala por la filtración, una vez filtrada se determina información que se vendió a terceras personales ajenas al servicio propuesto.

6.4.Caso Samsung.

"Samsung ha detectado el incidente y ha tomado medidas para asegurar los sistemas afectados. Como parte de nuestra investigación en curso, hemos contratado a una empresa externa líder en ciberseguridad y estamos coordinando con las fuerzas del orden", aseveró la compañía." (De Nicola, Samsung revela una filtración de datos, tras el ataque de julio, 2022)

La empresa desarrolladora de dispositivos móviles presenta en 4 de julio de 2022 la filtración de datos ocurrido en su sistema de seguridad adquiriendo los datos de forma ilegítima de cada uno de los usuarios de Samsung estimando que, el ataque de la información de los datos personales suscita de forma que, la información adquirida no involucra el robo de número de tarjetas de débito o crédito registrado en la empresa Samsung,

"En el presente caso todavía no se ha notificado ni hecho público ninguna sanción a la empresa por parte de la autoridad competente, sin embargo, se entiende que Samsung ha aplicado varias medidas de seguridad para la mitigación de riesgos y ha cumplido con el principio de información a los titulares de datos personales." (Meythalerzambrano, 2022)

La filtración de datos de Samsung no fue sancionada por ningún estado en la cual se dio la filtración de la información sin ninguna motivación alguna, no obstante, las medidas de seguridad aplicadas por Samsung son reforzadas ya que prioriza la seguridad de sus usuarios en cuanto a su información personal además que al no existir sanción alguna pone en duda la responsabilidad de la empresa de Samsung en cuanto a su responsabilidad por deficiencia en cuanto al tratamiento de la información y sus medidas de seguridad.

Conclusión

- La ley de protección de datos personales no ha sido determinada como prioridad del estado ecuatoriano puesto que, como se ha demostrado en la presente tesis existe la

vulneración de la información personal de cada uno de los titulares que se han visto afectados por filtraciones y tratamiento maliciosos por los usuarios.

- Determinando que, el uso de aplicaciones móviles como Facebook, Instagram y WhatsApp, son fuente de filtración de información exponiendo la falta de conocimiento de los titulares de la información personal a pesar que, existe medidas de seguridad aplicadas por los desarrolladores de las aplicaciones correspondientes no ha sido suficiente para secar con la vulneración de derechos fundamentales tratados y analizados en la presente investigación.
- Tomando en consideración que el Art. 1 de la ley orgánica de protección de datos personales de Ecuador es clara en cuanto a su finalidad esta no cumple con todos los parámetros de seguridad para garantizar este derecho que según la constitución de la republica reconoce a nivel de redes sociales.
- El Estado ecuatoriano se encuentra en las bases legales básicas para considerar que, el uso de las aplicaciones móviles genera un riesgo inminente en cuanto a la filtración de la información personal a medida que las aplicaciones móviles van surgiendo en nuevos aspectos tecnológicos en cuanto a sus actualizaciones que cada vez son mucho más frecuentes.
- En la ley de protección de datos personales estima que el tratamiento de datos es realizado tanto por el sector público como privado y entidades bancarias que posee la información en coordinación con el titular de su información y su previo consentimiento para poder acceder a ella como tal.
- Se estima que el tratamiento de brinda las empresas desarrolladoras de las aplicaciones tratadas no tiene acceso el Estado pese a que la empresa debe regirse por el marco legal de la poye de protección de datos personales este marco legal es pasado por alto ignorando los estándares de seguridad que exige el Estado siendo

estos mínimos ya que, como se mencionó la filtración de datos personales en Ecuador son constantes y priorizar la regularización de la información en aplicaciones móviles es casi nulo para garantizar la protección de este derecho.

- Dentro de la encuesta realizara a diferentes personas considera que la información si puede ser filtrada por parte de los desarrolladores de las aplicaciones tratadas puesto que, la base de datos a la que va dirigida no puede el Estado realizar el tratamiento respectivo puesto que no se encuentra en su jurisdicción como tal, debido a que existen casos de tratamiento maliciosos de la información reconociendo que la información personal es filtrada por diferentes medios sea por los desarrolladores como se analizó en el caso de Facebook y su filtración de la información o por terceras personas que realizan actos que vulneran su derecho a la imagen, la honra, el buen nombre y sus datos perianales.
- Además la sentencia 2064-14/EP, determina el riesgo inminente que existe en el uso indebido de la aplicación móvil WhatsApp, en cuanto a su tratamiento malicioso debido que el uso no autorizado de la información sensible generar consecuencias perjudiciales tanto en los datos personales adquiridos de forma maliciosa y la distribución de la misma a terceras personas ajenas a las conversaciones particulares debido a que, en el entorno social en el que se encontrase la persona puede influir de forma negativa su desarrollo integro como persona.
- La vulneración de estos derechos al ser frecuentes no existe una tipificación penal singularizada como tal ya que, en el uso de las aplicaciones móviles acarrea sanciones penales no obstante la sanción impuesta no incurre a poseer cierta gravedad como tal, además que el delito tipificado con más recurrencia a ser vulnerado es el derecho a la intimidad ya que, al considerarse como dato sensible

este debe ser resguardado y tener la garantía que los diferentes medios tecnológicos eviten o cesen de forma exponencial este derecho.

- En conclusión existe la vulneración del derecho a la protección de datos personales en Ecuador puesto que, no existe una marco legal solido que proteja los derechos reconocidos por la constitución ya que, el tratamiento indebido u malicioso de la información personal u dato sensible se ve afectado exponencialmente por las diferentes aplicaciones móviles tratadas en la presente investigación exponiendo la hipótesis planteada y determinado que, la vulneración de este derecho de protección de datos personales se encuentra vulnerado en diferentes lugares del Estado puesto que, en menores de edad la filtración de información es mucho mas exponencial ante cualquier sujeto que acceda a la información de forma ilegal sin consentimiento y brindar un tratamiento malicioso.

Recomendaciones

- ➔ Como recomendación es priorizar que, las distintas funciones del Estado determine mediante el uso de políticas públicas la adecuación y regularización del uso de aplicaciones frente al entorno de los datos personales ya que, como se demostró la vulneración de este derecho el Estado no presente como eje central que los medios tecnológicos están formando parte del día a día de la sociedad incurriendo a que la información que se proporcione de forma exponencial por cada titular de su información se vea afectada por un tratamiento indebido.
- ➔ Como segunda recomendación es detallar y reformar la finalidad de forma clara y precisa de la protección de los datos personales, por el hecho que, únicamente se enfoca en el sector publico mas no en el sector privado por el hecho que, las entidades de Facebook, Instagram y WhatsApp, forman parte del sector privado y un tratamiento adecuado de los datos personales no es determinado como tal ya que

al ser enviado a una base de datos determinada la información que se proporciona por parte de los titulares al mero desconocimiento del tratamiento es propenso a un tratamiento indebido con repercusiones muy perjudiciales a nuestros derechos a la intimidad, honra, buen nombre e imagen.

- ➔ Tercera recomendación, de forma conjunta de la Asamblea Nacional en coordinación con el presidente de la republica enfocarse más en la protección de los datos personales en el uso de las redes sociales ya mencionadas y tratadas en la presente investigación, fomentar el tratamiento adecuado de la información en relación a políticas públicas que determine la responsabilidad penal del tratamiento inadecuado de la información.
- ➔ Cuarta recomendación, tipificar delitos cometidos en el uso inadecuado de las aplicaciones móviles de Facebook, Instagram y WhatsApp, ante la vulneración del derecho a la honra, buen nombre, imagen, propiedad intelectual y demás aspectos importantes que la legislación ecuatoriana no toma en consideración a comparación de otras legislaciones analizadas en el presente proyecto.

Referencias Bibliográficas

I. Adrián, Y. (22 de 08 de 2019). *Concepto de - Definición de*. Obtenido de Concepto de - Definición de: https://conceptodefinicion.de/informatica/

II. Aguilar, P. A. (2015). ¿DERECHO INFORMÁTICO Ó INFORMÁTICA JURÍDICA? *Facultad de Derecho, Universidad Nacional Autónoma de México (UNAM), México*, 19-24. Obtenido de https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=&cad=rja&uact=8&ved=2ahUKEwj55O7Fl66EAxXaRjABHdxmCkcQFnoECBkQAQ&url=https%3A%2F%2Fdialnet.unirioja.es%2Fdescarga%2Farticulo%2F7242751.pdf&usg=AOvVaw3PGcbPQJmUv01Ll06zkNdy&opi=89978449

III. Aguilar, R. (09 de 06 de 2022). *Xataka.com*. (Xataka, Editor) Obtenido de Xataka.com: https://www.xataka.com/privacidad/sancion-historica-para-instagram-instagram-se-enfrenta-a-405-millones-euros-multa-incumplir-rgpd

IV. Alcalá, H. N. (2007). EL DERECHO A LA PROPIA IMAGEN COMO DERECHO FUNDAMENTAL IMPLÍCITO. FUNDAMENTACIÓN Y CARACTERIZACIÓN. *scielo*. Obtenido de https://www.scielo.cl/scielo.php?script=sci_arttext&pid=S0718-00122007000200011

V. Baena, M. R. (14 de Noviembre de 2019). *App&Web*. Obtenido de App&Web: https://www.appandweb.es/blog/historia-aplicaciones-moviles/

VI. Broadcom. (19 de 09 de 2022). *VMware*. Obtenido de VMware: https://www.vmware.com/es/topics/glossary/content/application-security.html

VII. Constitucional, C. (27 de enero de 2021). *Corte Constitucional*. Obtenido de Corte Constitucional: http://esacc.corteconstitucional.gob.ec/storage/api/v1/10_DWL_FL/e2NhcnBldGE6J3

RyYW1pdGUnLCB1dWlkOic1MDM5NmI5Ny1hZmFiLTQ1OWEtYWRlMC1jNjdmNzM1NTMzYjAucGRmJ30=

VIII. CONSTITUYENTE, A. (2008). *CONSTITUCIÓN DE LA REPÚBLICA DEL ECUADOR.* MONTECRISTI: REGISTRO OFICIAL.

IX. Creel., O. A. (s.f.). *Derecho Informático.* Obtenido de https://d1wqtxts1xzle7.cloudfront.net/57275933/Derecho_Informatico-libre.pdf?1535680177=&response-content-disposition=inline%3B+filename%3DDerecho_Informatico.pdf&Expires=1708221200&Signature=OJu5x3ghlRUpjDrcm-x7h5OeIhL7MtoiGKAucW9D8r8Su5qCa28ubOcKq4D4Kpe

X. CUBRÍA, M. I. (1970). *El derecho a la intimidad.* Oviedo: Universidad de Oviedo. Obtenido de https://digibuo.uniovi.es/dspace/bitstream/handle/10651/19294/0119561.pdf?sequence=1

XI. datos, A. E. (2024). Menores, salud digital y privacidad. *Estrategia y líneas de acción: Menores, salud digital y privacidad*, 1-11. Obtenido de https://www.aepd.es/guias/estrategia-menores-aepd-lineas-accion.pdf

XII. De dato personal, D. (s.f.). *Ugto.mx*. Obtenido de Ugto.mx: https://nodo.ugto.mx/wp-content/uploads/2017/03/Introducci%C3%B3n-y-antecedentes-del-derecho-a-la-protecci%C3%B3n-de-datos-personales.pdf

XIII. De Nicola, M. (26 de 09 de 2022). *Ciberseguridadlatam.com*. Obtenido de Ciberseguridadlatam.com: https://www.ciberseguridadlatam.com/2022/09/26/la-sec-multa-a-morgan-stanley-con-35-millones-de-dolares-por-un-fallo-en-la-seguridad-de-los-datos/

XIV. De Nicola, M. (04 de 09 de 2022). *Ciberseguridadlatam.com*. Obtenido de Ciberseguridadlatam.com: https://www.ciberseguridadlatam.com/2022/09/04/samsung-revela-una-filtracion-de-datos-tras-el-ataque-de-julio/

XV. Díaz, K. M. (28 de 7 de 2022). *abogacía*. Obtenido de abogacía: https://www.revistaabogacia.com/derecho-informatico-importancia-y-evolucion/

XVI. General, A. (1948). *Declaración Universal de Derechos Humanos.* París. Obtenido de https://www.ohchr.org/sites/default/files/UDHR/Documents/UDHR_Translations/spn.pdf

XVII. González, A. G. (2007). La protección de datos personales: derecho fundamental del siglo XXI. Un estudio comparado. *scielo*. Obtenido de https://www.scielo.org.mx/scielo.php?script=sci_arttext&pid=S0041-86332007000300003general

XVIII. Hernández', J. C. (2012). La protección de datos personales en Internet y el Habeas Data. *Revista Derecho y Tecnología*, 69. Obtenido de https://www.corteidh.or.cr/tablas/r32012.pdf

XIX. Hernández, O. S., Borrego, R. H., & Brito, H. R. (2021). Metodología para evaluar el nivel de seguridad de las aplicaciones móviles sobre plataforma Android en ETECSA. *Serie Científica de la Universidad de las Ciencias Informáticas*, 11. Obtenido de https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=&ved=2ahUKEwiE-ZSu9bWEAxWwVzABHYYuAwEQFnoECBsQAQ&url=https%3A%2F%2Fdialnet.unirioja.es%2Fdescarga%2Farticulo%2F8590609.pdf&usg=AOvVaw0Ve7JBtCujnQAP9ZL6RIX8&opi=89978449

XX. López, A. P. (2014). Visión de la Corte Constitucional, respecto a los derechos de libertad de expresión e información: una relación desde el derecho al buen nombre, a la intimidad y a la honra. *scielo*. Obtenido de http://www.scielo.org.co/scielo.php?pid=S1794-44492014000200018&script=sci_arttext

XXI. M. M ÓJICA L ÓOPEZ, J. L. (2017). An´alisis de la privacidad de WhatsApp Messenger. *nstituto de Tecnolog´ıas F´ısicas y de la Informaci´on (ITEFI), Consejo Superior de Investigaciones Científicas (CSIC)*, 109-114. Obtenido de https://www.iiis.org/CDs2017/CD2017Summer/papers/CA890ED.pdf

XXII. MACHICADO, J. O. (2010). *APUNTES JURÍDICOS*. Obtenido de APUNTES JURÍDICOS: https://ermoquisbert.tripod.com/pdfs/concepto-delito.pdf

XXIII. Mendieta Toledo, G. L. (24 de junio de 2020). *Repositorio Academico UPC.* Obtenido de Repositorio Academico UPC:

XXIV. Meythalerzambrano. (23 de 12 de 2022). *Meythalerzambrano*. Obtenido de Meythalerzambrano: https://www.meythalerzambranoabogados.com/post/casos-de-filtraciones-de-datos-del-a%C3%B1o-2022

XXV. Moreno, E. V. (Febrero de 2022). *REPOSITORIO NACIONAL PUCE.* Obtenido de REPOSITORIO NACIONAL PUCE: https://repositorio.pucesa.edu.ec/bitstream/123456789/3467/1/77638.pdf

XXVI. Muñoz, V. d., & Contreras, Á. D. (2022). *# La Corte Dice 500 criterios jurisprudenciales año 1* (3° edición: enero 2022 ed.). Guayaquil, Guayas, Ecuador: Role Mchine Imprenta Fráfica.

XXVII. NACIONAL, A. (2021). *LEY ORGÁNICA DE PROTECCIÓN DE DATOS PERSONALES.* QUITO: REGISTRO OFICIAL. Obtenido de https://www.finanzaspopulares.gob.ec/wp-content/uploads/2021/07/ley_organica_de_proteccion_de_datos_personales.pdf

XXVIII. Nacional, A. (2024). *CÓDIGO ORGÁNICO INTEGRAL PENAL.* Quito: Registro Oficial.

XXIX. Patricia, C. C. (2013). El contenido del derecho a la intimidad. *scielo*, 45. Obtenido de https://www.scielo.org.mx/pdf/cconst/n29/n29a3.pdf

XXX. Perelló, E. M. (2009). IMPACTO DE LAS REDES SOCIALES EN EL DERECHO A LA PROTECCIÓN DE DATOS PERSONALES. *Universidad de Alcalá*, 115. Obtenido de https://core.ac.uk/reader/58906850

XXXI. PRESIDENCIA, M. S. (2023). *SOBRE PROTECCION DE LA VIDA PRIVADA.* Santiago de Chile, Chile: Congreso nacional de Chile. Obtenido de http://www.leychile.cl/N?i=141599&f=2012-02-17&p=

XXXII. Rivadeneira, J. J., & Pino, S. A. (2013). *DERECHO Y LAS NUEVAS TECNOLOGÍAS* (Primera ed.). Quito, Pichincha, Ecuador: Departamento Jurídco.

XXXIII. Rosales, L. E. (2014). Los derechos a la intimidad, a la propia imagen y al honor vulnerados por el ejercicio abusivo de la libertad de expresión en Facebook. *derecom*, 47.

XXXIV. Ruiz, C. B. (2009). LAS REDES SOCIALES Y LA PROTECCION DE DATOS HOY. *Universidad de Alcalá*, 307-313. Obtenido de https://core.ac.uk/download/pdf/58906859.pdf

XXXV. Salazar Ramon, D. F. (2022). *Universidad Cesar Vallejo Repositorio Digital Institucional.* Obtenido de Universidad Cesar Vallejo Repositorio Digital Institucional: https://repositorio.ucv.edu.pe/bitstream/handle/20.500.12692/99447/Salazar_RDF-SD.pdf?sequence=1&isAllowed=y

XXXVI. Sanchez, E. R. (04 de 06 de 2019). *Universitat de Catalunya.* Obtenido de Universitat de Catalunya: https://openaccess.uoc.edu/handle/10609/95927

XXXVII. Tello, L. (2013). Intimidad y «extimidad» en las redes sociales. Las demarcaciones éticas de Facebook. *Grupo Comunicar*, 205-213.

XXXVIII. TIRADO, M. X. (Junio de 2006). *UNIVERS IDAD DE LOS ANDES.* Obtenido de UNIVERS IDAD DE LOS ANDES: https://repositorio.uniandes.edu.co/server/api/core/bitstreams/de586df3-ea5a-438d-84d2-ca23396ebf88/content

XXXIX. Valdés, J. T. (2008). *DERECHO INFORMATICO* (Cuarta edición ed.). (E. C. Gutiérrez, Ed.) San Ángel, México: Marcela 1. Rocha Martínez. Obtenido de https://d1wqtxts1xzle7.cloudfront.net/53806525/DERECHO-INFORMATICO-4-EDICION_1-libre.pdf?1499639538=&response-content-disposition=inline%3B+filename%3DDERECHO_INFORMATICO_4_EDICION_1.pdf&Expires=1708221013&Signature=F4pbZgozoD2zYtl6v5scI7-kJP7XR7FDP12TiLx

XL. Verac, E. O. (2018). La protección de datos y el habeas data en Chile. *PERSPECTIVAS revista de ciencias jurídicas y políticas*, 130-131.

XLI. Vercelli, A. (2019). La (des)protección de los datos personales: análisis del caso Facebook Inc. - Cambridge Analytica. *Simposio Argentino de Informática y Derecho*,

1-10. Obtenido de http://sedici.unlp.edu.ar/bitstream/handle/10915/71755/Documento_completo.PDF-PDFA.pdf?sequence=1&isAllowed=y

XLII. Vizcarra, A. E. (s.f.). *Organización de los Estados Americanos.* Obtenido de Organización de los Estados Americanos: http://www.oas.org/es/sla/cji/docs/informes_culminados_recientemente_Proteccion_Datos_Personales_CJI-doc_541-17_corr1.pdf

XLIII. VULNERACIÓN DEL DERECHO A LA INTIMIDAD EN REDES SOCIALES: UNA REALIDAD SOCIOJURÍDICA. (2020). *Revista, Ciencia y Libertad en Germinación*, 27-30. Obtenido de https://revistas.unilibre.edu.co/index.php/germinacion/article/view/9143/8056

XLIV. Wang, S. (23 de 12 de 2019). *ViewSonic Library*. Obtenido de ViewSonic Library: https://www.viewsonic.com/library/es/educacion/el-adn-digital-educativo-preparese-para-la-innovacion-en-tecnologia-en-la-educacion/

Anexos

- El presente anexo corresponde a la encuesta realizada en cuanto al tratamiento de los datos personales a diferentes personas en el uso de aplicaciones de Facebook. Instagram, y WhatsApp.

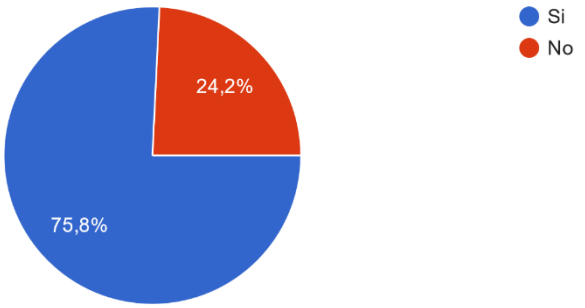
1.

- La primera pregunta realizada en cuanto a la encuesta las personas encuestadas reconocen que, las aplicaciones móviles de Facebook, Instagram y WhatsApp, recopila la información pese al conocimiento que posee de las aplicaciones aceptan el riesgo de la filtración de su información personal.

2.

¿ Conoce usted acerca de la filtración de información de datos personales a la base de datos de las aplicaciones de Facebook, Instagram y WhatsApp.?

33 respuestas

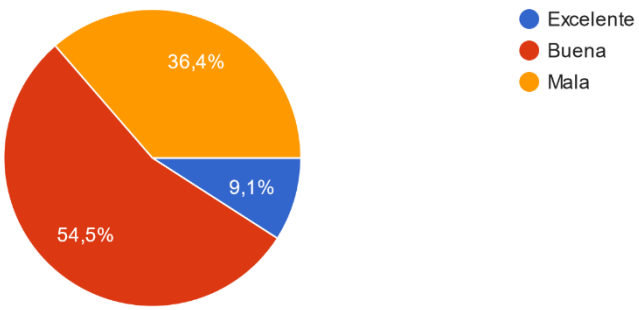


- La filtración realzada corresponde al juicio llevado acabo por parte de Estado Unidos en contra de su creador Mar Zuckerberg, en la que se determino que la información proporcionada por cada uno de los usuarios fue filtrada, siendo tal que, 8 personas equivalente al 24. % desconocen del presente caso.

3.

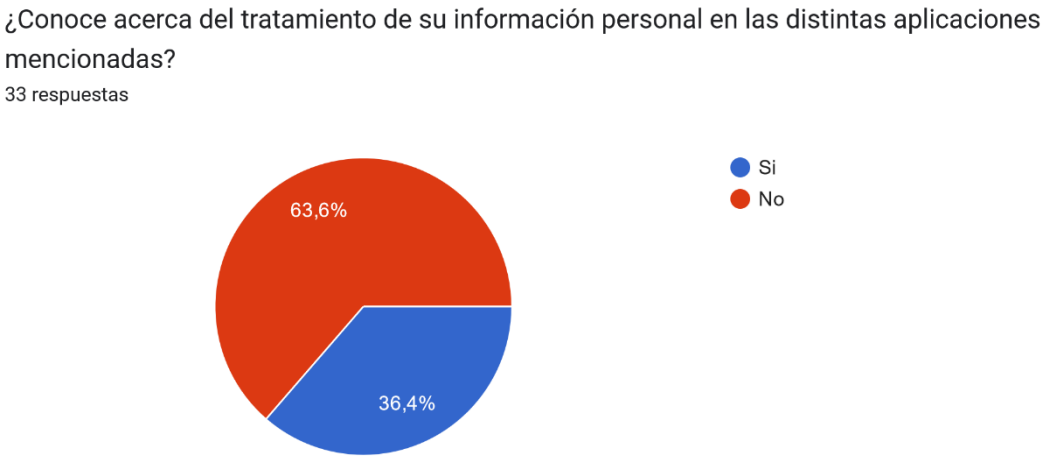
Qué tan confiable es para usted la seguridad de las aplicaciones de Facebook, Instagram y WhatsApp en su entorno social.

33 respuestas



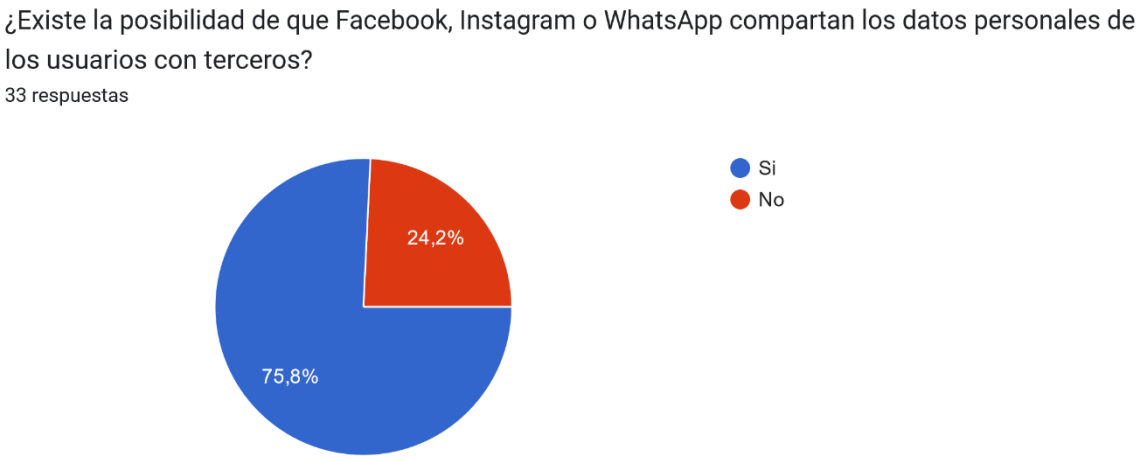
- La siguiente pregunta corresponde a que le 9.1 % considera que las políticas de privacidad de las aplicaciones tratas son eficientes para su protección de su información, el 36.4% considera que es mala pese a que si existe vulneración y filtración de la información y en cuanto al 54.5 % considera que es buena la información siendo que acepta tal como está las políticas de privacidad de la información.

4.



- En la presente pregunta se estima que, el 63,6 % desconoce el tratamiento que este brinda los desarrolladores de las aplicaciones móviles en cuanto a la adquisición de la información mientras que el 36,4 % si conoce el tratamiento realizado-

5.



- El 75.8 % correspondiente a la presente pregunta considera que si existe vulneración y filtración de su información a terceras personales mientras que el 24.2 % desconoce por completo esta filtración de la información.

■ *Encuesta realizada en formularios Google, link, https://docs.google.com/forms/d/e/1FAIpQLSeBkhORbmSI59R1-je-IpEILVyfOIOMJZrHAcvMH6KxkRfb1A/viewform?usp=send_form*

Universidad Católica de Cuenca

AUTORIZACIÓN DE PUBLICACIÓN EN EL REPOSITORIO INSTITUCIONAL

Felipe Josue Andrade Arias portador(a) de la cédula de ciudadanía Nº **0150747335**. En calidad de autor/a y titular de los derechos patrimoniales del trabajo de titulación **"Análisis del marco legal de la protección de datos personales frente a las aplicaciones móviles en Ecuador"** de conformidad a lo establecido en el artículo 114 Código Orgánico de la Economía Social de los Conocimientos, Creatividad e Innovación, reconozco a favor de la Universidad Católica de Cuenca una licencia gratuita, intransferible y no exclusiva para el uso no comercial de la obra, con fines estrictamente académicos y no comerciales. Autorizo además a la Universidad Católica de Cuenca, para que realice la publicación de éste trabajo de titulación en el Repositorio Institucional de conformidad a lo dispuesto en el artículo 144 de la Ley Orgánica de Educación Superior.

Cuenca, **09 de mayo de 2024**

F: .....

Felipe Josue Andrade Arias

C.I. **0150747335**