UNIVERSIDAD TÉCNICA DE AMBATO

FACULTAD DE JURISPRUDENCIA Y CIENCIAS SOCIALES

CARRERA DE DERECHO

TEMA:

Análisis jurídico de la Sentencia No. 2064-14-EP de la Corte Constitucional y la Suplantación de Identidad con contenido sexual.

Propuesta de Trabajo de Titulación previo a la obtención del título de Abogada

AUTOR:

Jenifer Jadira Páramo Iza.

TUTOR

Dra. Mg. María Gabriela Acosta Morales.

Ambato- Ecuador

2025

PÁGINAS PRELIMINARES

TEMA:

ANÁLISIS JURÍDICO DE LA SENTENCIA No. 2064-14-EP DE LA CORTE CONSTITUCIONAL Y LA SUPLANTACIÓN DE IDENTIDAD CON CONTENIDO SEXUAL.

APROBACIÓN DEL TUTOR

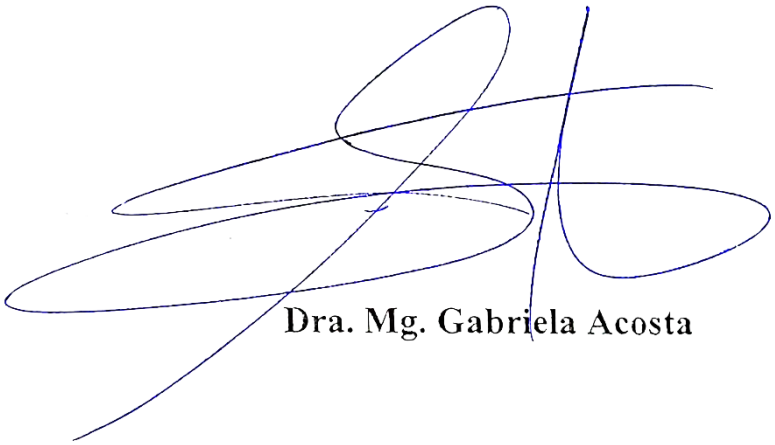
La suscrita Dra. Mg. María Gabriela Acosta Morales, en calidad de Tutor del Trabajo de Titulación

CERTIFICA:

Que la señorita Jenifer Jadira Páramo Iza, portadora de la Cédula de Ciudadanía número 050434198-3, habilitada para obtener el Título de Tercer Nivel; ha concluido su trabajo de titulación, modalidad **PROYECTO DE INVESTIGACIÓN** sobre el tema "**ANÁLISIS JURÍDICO DE LA SENTENCIA No. 2064-14-EP DE LA CORTE CONSTITUCIONAL Y LA SUPLANTACIÓN DE IDENTIDAD CON CONTENIDO SEXUAL",** previo a la obtención del título de Abogada; al cumplir con los requisitos técnicos, científicos, reglamentarios, metodológicos y jurídicos, autorizo la presentación del mismo ante el Organismo pertinente, para que sea sometido a evaluación por parte de la Comisión calificadora designada por el Honorable Consejo Directivo.

Ambato, 15 de enero de 2025.

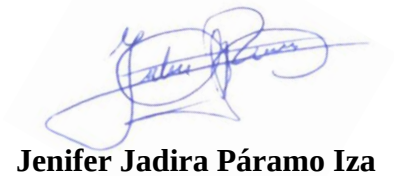
LO CERTIFICO



AUTORÍA DEL TRABAJO DE TITULACIÓN

Yo, Jenifer Jadira Páramo Iza, manifiesto que el presente trabajo denominado "**ANÁLISIS JURÍDICO DE LA SENTENCIA 2064-14-EP DE LA CORTE CONSTITUCIONAL Y LA SUPLANTACIÓN DE IDENTIDAD CON CONTENIDO SEXUAL"** es un trabajo original de mi propia autoría, desarrollado a través de la revisión previa de estudios realizados en mi formación académica y en fuentes bibliográficas, doctrinales y legales. Se exponen diversos enfoques y se ha incorporado criterios, ideas, conclusiones y recomendaciones cuya responsabilidad recae exclusivamente sobre el autor.

Ambato, 15 de enero de 2025



Jenifer Jadira Páramo Iza

050434198-3

AUTORA

DERECHOS DE AUTOR

Autorizo a la Universidad Técnica de Ambato para que convierta este trabajo de investigación un recurso accesible para su lectura consulta y procesos de investigación de conformidad con lo establecido en la normativa interna de esta institución de educación superior. Cedo los derechos de autor de mi Trabajo de Titulación con fines investigativos y de divulgación de conocimiento. Además, otorgo mi consentimiento expreso para la reproducción total o parcial de este trabajo investigativo, siempre y cuando; se enmarque en las regulaciones normativas universitaria, no se busque beneficio económico y se respete mis derechos de autor.

Ambato, 15 de enero de 2025



Jenifer Jadira Páramo Iza

050434198-3

AUTORA

APROBACIÓN DEL TRIBUNAL DE GRADO

Los miembros del Tribunal de grado APRUEBAN el Trabajo de Investigación del tema "**ANÁLISIS JURÍDICO DE LA SENTENCIA 2064-14-EP DE LA CORTE CONSTITUCIONAL Y LA SUPLANTACIÓN DE IDENTIDAD CON CONTENIDO SEXUAL"** presentado por la señorita Jenifer Jadira Páramo Iza, por cumplir con los requisitos técnicos, metodológicos y jurídicos de conformidad con el Reglamento de Graduación para la obtención del Título de Tercer Nivel de la Universidad Técnica de Ambato. Autorizo su presentación ante los organismos correspondientes.

Ambato, ... de 2025.

Para constancia firman

.....

Presidente

…… … ……

Miembro del Tribunal Miembro del Tribunal

DEDICATORIA

A mi madre, mujer de carácter fuerte, guerrera e indestructible, por su amor y su apoyo incondicional, quien ha sido mi fuente de inspiración, mi fortaleza en los momentos obscuros. Gracias por ser la luz de mi vida, por nunca soltar mi mano y dedicar toda su vida a cuidarme, guiarme y protegerme, por su esfuerzo y sacrificio. Sin usted no sería quien soy ahora.

A mi padre Daniel (†), por haberme dado la vida, confiar ciegamente en mí, brindarme su amor y ser mi ángel del cielo.

A mis hermanos Stalin y Anderson, que me impulsan a ser mejor persona cada día, gracias por su paciencia y por ser una parte esencial en mi vida. Sus palabras de aliento me han motivado a seguir adelante, en cada paso que doy su amor me acompaña siempre, gracias por ser incondicionales y a pesar de nuestras diferencias ser el complemento de mi vida.

A mi sobrino Said, que con su dulzura y amor puro desde su llegada ha iluminado cada día de mi vida.

A mi ángel del cielo Francisco, por amarme y protegerme durante toda su vida. Gracias por haber sido mi guía y luz durante 22 años. Sé que desde el cielo celebra nuestras metas, nos faltó una vida entera amor de mi vida, pero el cielo es afortunado de tenerlo, a pesar de no estar físicamente estoy segura de que su recuerdo vivirá en mi corazón siempre.

A mi abuelita Lucila, por ser mi compañera de vida, gracias por todo su amor cuidado y protección.

A toda mi familia, por acompañarme en este proceso, cada palabra de aliento fueron sin duda un impuso para continuar.

Jenifer Jadira Páramo Iza

AGRADECIMIENTO

Agradezco a Dios, por darme la vida, ser mi fuerza y refugio en todo momento, y permitirme alcanzar mis metas académicas

A la Universidad Técnica de Ambato por la oportunidad de formarme como profesional.

Agradezco infinitamente a mi tutora, Dra. Gabriela Acosta, por su invaluable orientación, apoyo constante y paciencia durante todo este proceso. Su conocimiento, su experiencia y su calidez humana han sido fundamentales para el desarrollo de este trabajo.

A mis amigas Dayana, Vanessa y Karla, gracias por todo lo compartido, por los momentos felices y los no tan felices, gracias porque sin ustedes no hubiese podido llegar hasta donde estoy.

A Betty, Erika, Gabriela, Melanie, Teresa, Nelly, René, Lorena y Luis, por estar presente durante toda mi vida y recordarme que no estoy sola.

A toda mi familia paterna y materna, por su amor, comprensión y aliento constante. Gracias por creer en mí y por estar siempre a mi lado, incluso en los momentos más difíciles, su apoyo ha sido mi mayor motivación.

ÍNDICE GENERAL DE CONTENIDOS

PÁGINAS PRELIMINARES ..... *ii*

TEMA: ..... *ii*

APROBACIÓN DEL TUTOR ..... *iii*

AUTORÍA DEL TRABAJO DE TITULACIÓN ..... *iv*

DERECHOS DE AUTOR ..... *v*

APROBACIÓN DEL TRIBUNAL DE GRADO ..... *vi*

DEDICATORIA ..... *vii*

AGRADECIMIENTO ..... *viii*

ÍNDICE GENERAL DE CONTENIDOS ..... *ix*

RESUMEN EJECUTIVO ..... *xii*

ABSTRACT ..... *xiii*

CAPÍTULO I. - MARCO TEÓRICO *1*

1.1 Antecedentes Investigativos **1**

Antecedentes históricos **5**

Definición y clasificación de datos. **9**

Datos Personales **10**

Datos personales en la era digital **13**

Características de los datos personales **17**

Alcance de los datos personales **17**

Componentes de los datos personales **18**

Tratamiento de datos personales **32**

Derecho a la protección de datos personales, privacidad e intimidad en el contexto digital. **38**

Contenido sexual en redes digitales **44**

Suplantación de identidad **46**

Teoría del delito **48**

Conducta 49

Tipicidad 50

Antijuridicidad 52

Culpabilidad 54

Corte Constitucional del Ecuador: Acción extraordinaria de protección y análisis de mérito **55**

Sentencia No. 2064- 14- EP de la Corte Constitucional **58**

Antecedentes 58

Alegaciones de las partes 58

Análisis constitucional 59

Análisis de Mérito 60
Resolución del problema jurídico. 62
Decisión 63

Influencia de la sentencia 2064-14-EP de la Corte Constitucional en la sanción de la conducta de suplantación de identidad en el contexto digital. ***63***

Bien jurídico protegido en la suplantación de identidad en el contexto digital ***65***

Suplantación de identidad con contenido sexual: Bien Jurídico afectado, Identidad, Identidad digital o Intimidad ***67***

1.2 Objetivos ***72***

Objetivo general **72**

Objetivos específicos **72**

CAPÍTULO II. - METODOLOGÍA ***73***

2.1 Materiales **73**

2.2 Métodos **74**
Técnicas e instrumentos 74
Nivel de investigación 76
Modalidad de investigación 76
Métodos 76

CAPÍTULO III. - RESULTADOS Y DISCUSIÓN ***80***

3.1 Análisis y discusión de los resultados **137**

CAPÍTULO IV. - CONCLUSIONES Y RECOMENDACIONES ***139***

4.1. Conclusiones **139**

4.2 Recomendaciones **139**

C. MATERIALES DE REFERENCIA ***149***

Referencias Bibliográficas **149**

Anexos **166**

Índice De Tablas Y Figuras

Tabla 1: *Evolución del delito de suplantación de identidad. 8*
Tabla 2: *Componentes y alcance de la definición de datos personales. 11*
Tabla 3*: Reconocimiento jurídico de datos personales en la legislación española, europea, colombiana y ecuatoriana.....23*
Tabla 4: *Comparación de la protección jurídica de los bienes jurídicos afectados en la suplantación de identidad con contenido sexual. 70*
Tabla 5: *Conducta de suplantación de identidad con contenido sexual. 80*
Tabla 6: *Evaluación del daño a la víctima en los casos de suplantación de identidad. 90*
Tabla 7: *Procedimientos específicos para recabar evidencias. 96*
Tabla 8: *Influencia de la Sentencia N° 2064-14-EP/21 .....103*
Tabla 9: *Tipificación de la conducta de suplantar la identidad con contenido sexual en el contexto digital.....108*
Tabla 10: *Criterios de la Corte sobre el tratamiento de datos personales. 112*
Tabla 11: *Determinación del tratamiento de datos personales por los operadores de justicia. 117*
Tabla 12: *Estándares de las empresas privadas para la protección de datos personales....120*
Tabla 13: *Protección de datos personales en el sistema jurídico actual 123*
Tabla 14: *Obstáculos en el sistema judicial para aplicar la Sentencia N°2064-14-EP/21. .126*
Tabla 15: *Recomendaciones para mejorar el sistema judicial en la protección de datos personales. 129*
Tabla 16: *Las fotografías íntimas como datos personales sensibles. 131*
Tabla 17*: Conclusiones y recomendaciones en función de los objetivos.....139*

Figuras

Figura 1: *Dra. Amparo Tasipanta- Fiscal Multicompetente en el cantón Latacunga. 166*
Figura 2: *Dra. Maricela Yánez- Fiscal de violencia de género en el cantón Latacunga.....166*
Figura 3: *Verónica Altamirano Guerra- Asistente de Fiscalía en el cantón Latacunga.....167*
Figura 4: *Dr. Jorge Nagales- Asistente de Fiscalía en el cantón Latacunga.....167*
Figura 5: *Dr. Fabián Altamirano - Juez de Garantías Penales en el cantón Ambato 168*

RESUMEN EJECUTIVO

La identidad es entendida como el conjunto de datos personales que singulariza a un individuo dentro de las relaciones sociales. El creciente avance tecnológico que se evidencia en la actualidad provoca que la sociedad cambie su forma de relacionarse con otros individuos. En este sentido, los datos personales que se comparten en las redes digitales son susceptibles de ser usados sin el consentimiento de su titular por terceras personas, con fines delictivos que atentan a bienes jurídicos como la propiedad, identidad e intimidad. En este contexto, el uso de datos personales sensibles con la finalidad de suplantar la identidad con contenido sexual es frecuente, más aún en un mundo cada vez más digitalizado. Esta conducta vulnera derechos tradicionales como, la intimidad, privacidad, imagen, honra, dignidad y protección de datos personales. Estos derechos gozan de protección jurídica constitucional, sin embargo, es necesario que el derecho se adapte a las nuevas modalidades que surgen en el entorno digital. De tal forma que, los criterios adoptados por la Corte Constitucional en la sentencia N°2064-14-EP/21 deben ser incorporados en la práctica legal. Por ello, esta investigación mediante la aplicación de un marco metodológico explicativo tiene por objeto analizar la influencia de la Sentencia N°2064-14-EP/21 en el marco jurídico penal del Ecuador. Para obtener y analizar la información que conduce a la ejecución del proyecto se empleó los métodos, inductivo, analítico, sintético, histórico y comparativo. Además, se emplearon siete entrevistas dirigidas a fiscales, jueces penales y abogados en libre ejercicio, con la finalidad de conocer la percepción que los profesionales sobre el tema de estudio. La relevancia de la investigación yace de la necesidad de una adecuación a la normativa penal para sancionar los delitos que surgen en el entorno digital. Para lo cual, la línea investigativa que adopta el presente proyecto es de Comunicación, Sociedad, Cultura y Tecnología. Los resultados de la investigación demuestran que, la sentencia *in examine* contiene criterios fundamentales para el análisis de los derechos que surgen en la era digital y para la determinación de la responsabilidad penal de la conducta de suplantar la identidad con contenido sexual en el contexto digital. Además, mediante el Derecho Comparado se ha logrado verificar que la normativa penal ecuatoriana no garantiza una verdadera protección a los derechos de las personas víctimas de delitos digitales, puesto que no contempla una reparación integral.

Palabras clave: Datos personales, contenido sexual, identidad, intimidad, evolución tecnológica, consentimiento.

ABSTRACT

Identity is understood as the set of personal data that singles out an individual within social relations. The growing technological progress that is evident today causes society to change the way it relates to other individuals. In this sense, personal data shared in digital networks are susceptible to be used without the consent of the owner by third parties for criminal purposes that infringe legal rights such as property, identity and privacy. In this context, the use of sensitive personal data with the purpose of impersonating the identity with sexual content is frequent, even more so in an increasingly digitized world. This conduct violates traditional rights such as intimacy, privacy, image, honor, dignity and protection of personal data. These rights enjoy constitutional legal protection; however, it is necessary that the law adapts to the new modalities that arise in the digital environment. In such a way that, the criteria adopted by the Constitutional Court in judgment N°2064-14-EP/21 must be incorporated into the legal practice. Therefore, this research through the application of an explanatory methodological framework aims to analyze the influence of Ruling N°2064-14-EP/21 in the criminal legal framework of Ecuador. To obtain and analyze the information leading to the execution of the project, inductive, analytical, synthetic, historical and comparative methods were used. In addition, seven interviews were conducted with prosecutors, criminal judges and lawyers in free practice, to know the perception of the professionals about study. The relevance of the research lies in the need for an adaptation of the criminal law to punish the crimes that arise in the digital environment. For which, the research line adopted by this project is Communication, Society, Culture and Technology. The results of the research show that the sentence under examination contains fundamental criteria for the analysis of the rights that arise in the digital era and for the determination of criminal liability for the conduct of impersonation with sexual content in the digital context. In addition, through comparative law, it has been verified that the Ecuadorian criminal law does not guarantee a real protection of the rights of the victims of digital crimes, since it does not contemplate a comprehensive reparation.

Key words: Personal data, sexual content, identity, privacy, technological evolution, consent

CONTENIDOS

CAPÍTULO I. - MARCO TEÓRICO

1.1 Antecedentes Investigativos

En la actualidad con el avance tecnológico acelerado que ha tenido la sociedad, el tema sobre los datos personales implica un abordaje investigativo profundo. La difusión de estos datos personales ahora trasciende fronteras. Estas implicaciones sociales permiten que los delincuentes operen tras de una pantalla sin que para ello exista sanción alguna. Por ejemplo, la suplantación de identidad con contenido sexual en el ámbito digital provoca que los datos personales sean transferidos sin el consentimiento y a nombre del titular. El estudio adquiere relevancia en el ámbito del Derecho Penal, puesto que permite examinar los presupuestos jurídicos establecidos por la Corte Constitucional en la Sentencia No. 2064- 14- EP que se deben considerar sobre el tratamiento de los datos personales en el ámbito digital, además permite identificar mediante el abordaje del Derecho Comparado cómo el tratamiento de datos personales en redes digitales conlleva a cometer el delito de suplantación de identidad con contenido sexual, sus implicaciones y sanciones.

La investigación se fundamenta en estudios desarrollados con anterioridad en torno al uso arbitrario y sin consentimiento de los datos personales en las redes digitales. Además, se realizó una revisión de investigaciones que abordan el tema de la suplantación de identidad en la era digital, esto permite tener una visión más clara sobre el problema que se indaga.

Los datos personales en la era digital son propensos a ser utilizados sin el consentimiento de los usuarios de las redes en línea, es así que surge la necesidad estatal de regular la protección y el tratamiento de los datos personales. Pues, la Constitución de la República del Ecuador (CRE) reconoce que la protección de estos datos ha sido reconocida como un derecho de libertad (Art. 66. 19). En esta misma línea, Gómez et al. (2020) en su trabajo investigativo titulado “El derecho a la protección de datos personales, tecnologías digitales y pandemia por COVID-19 en Colombia” concluyeron que:

> La garantía del derecho a la protección de datos también depende del adecuado diseño de las herramientas tecnológicas y nuevos modelos de gobernanza de la información, lo que significa que en su desarrollo deben participar no solo expertos en sistemas de

> información, sino también científicos de datos, especialistas en inteligencia artificial, en bioética, bioderecho, y en derechos humanos. (p. 289)

En este sentido, cuando una persona navega en internet a través de un perfil, permite que más usuarios de la red tengan acceso a su información personal como nombres, apellidos, fotografías, entre otros datos. Es decir, la información pasa de un plano íntimo y privado a forzosamente ser de carácter público. Esta situación trae consigo que usuarios externos aprovechen que los datos personales se encuentran desprotegidos y se apropian de ellos con la finalidad de cometer actos delictivos a nombre del titular y afectar su dignidad. En las redes sociales, por ejemplo, la esfera de privacidad resulta imposible de alcanzar, debido a que sin el consentimiento del usuario digital, su información personal se replica constantemente por encontrarse en un espacio de libre acceso.

La protección de datos personales es fundamental por cuanto hoy en día está en riesgo la identidad de la colectividad dado a las múltiples formas de acceder a la misma en las redes digitales, por aquel Guijosa (2013) en su trabajo de pregrado titulado "Protección de Datos Personales en Redes Sociales Digitales" realiza un abordaje de la temática en México y concluye que:

> En el ciberespacio, entre muchas otras cosas, existen redes de comunicación interactivas orientadas a la socialización llamadas redes sociales digitales. Dentro de estas redes los usuarios se relacionan, interactúan e intercambiando grandes cantidades de información, mucha de esta referente a las actividades cotidianas de cada persona. (p. 65)

Es decir, los datos que los usuarios comparten en internet se difunden de forma masiva provocando que éstos sean apropiados de una forma ilícita con la finalidad de cometer actos penalmente relevantes a nombre del titular y afectar a la dignidad, buen nombre e intimidad de la persona. Al respecto, Porcelli (2019) en su investigación titulada "La Protección de los Datos Personales en el Entorno Digital. Los Estándares de Protección de Datos en los Países Iberoamericanos" integra el significado actual sobre el derecho a la privacidad en el ámbito digital y la regulación legislativa para la protección de los datos personales y concluye que:

> La idea es que no termine la vida privada sino que se reconfigure, se adapte y actualice la legislación para asegurar el derecho a la intimidad, a la dignidad y al honor conforme la economía digital vigente en este siglo XXI, para lo cual, en primer lugar hay que

> reconocer y comprender el funcionamiento de este fenómeno para después regularlo técnica y jurídicamente. (p. 494)

El tratamiento de los datos personales en la era digital conlleva a efectuar diferentes actividades ilícitas sin el consentimiento de su titular. En la actualidad, con el surgimiento de las redes digitales, es importante reconocer que los usuarios crean una identidad digital a través de internet, que permite que un individuo sea identificable dentro de la red. Esto permite la interacción entre los individuos quienes pueden recibir, enviar, compartir, difundir información personal o no, a través de una pantalla y sin mayores implicaciones, Liceda (2011), en su investigación "Identidad Digital" estudia el presupuesto de la identidad en el contexto tecnológico y establece que:

> Una persona puede elegir participar en forma activa en Internet o no, lo cierto es que muchos de sus datos personales van a estar "colgados" en la red. Esos datos van a configurar su imagen digital, es decir la proyección de esa persona en los entornos digitales. En el caso de que la persona participe en forma activa en internet, va a tener la posibilidad de generar varias imágenes digitales según los datos que aporte en cada servicio. Tanto los datos que brinde la persona como aquellos que aporten terceros (sean ciertos o no) van a afectar su reputación (dado que modificarían o generarían su imagen y por tanto la valoración que de ella hagan los terceros). Pero en forma alguna podemos aceptar que exista una "identidad digital" puesto que, al menos en estos momentos, no existe la posibilidad de plasmar la universalidad de datos y la conciencia de ella en Internet. (p. 303)

La identidad está conformada por todos aquellos datos que permiten diferenciarnos en una sociedad. Además, es importante tener en cuenta que en la actualidad un dato personal no solo es el nombre, apellido, número de cédula, sino que éste ha evolucionado y ahora los datos personales también incluyen fotografías y otros caracteres que hagan identificable a una persona. En esta línea, es fundamental que el delito de suplantación de identidad con contenido sexual sea analizado bajo los lineamientos del tratamiento de datos personales y datos personales sensibles. En este caso es necesario realizar un abordaje de los antecedentes investigativos que se relacionan con el delito de suplantación de identidad con la finalidad de contextualizar el marco jurídico, doctrinario y bibliográfico que se pretende proyectar en el estudio.

Al respecto vale mencionar que este delito atenta contra el derecho a la identidad que según la CRE es parte de los derechos de libertad. Es así que establece que toda persona tiene derecho a la identidad personal y colectiva que incluye entre otros, tener nombre y apellido (Ar. 66. 28). Partiendo de los supuestos anteriores Moreno et al. (2022) en su trabajo de investigación titulado "Regulación Global para evitar la Suplantación de Identidad Digital" concluyen que:

> La suplantación de identidad es una conducta contraria a al respeto de la dignidad y derecho de la persona al libre desarrollo de su personalidad. El Estado debe velar por la protección y garantizar el ejercicio del derecho a la identidad, que, en los últimos tiempos, gracias al desarrollo de las tecnologías, abarca la identidad digital. (p. 696)

Entonces, la suplantación de identidad se entiende como aquel acto de apropiación indebida de los datos personales de un individuo que tiene como finalidad asumir la identidad de otro en el ciberespacio. Este acto incluye la utilización no autorizada de credenciales de autentificación, infiltración a cuentas ajenas, entre otros, cuya finalidad es el menoscabo de la reputación del titular o la afectación económica. Este delito está ligado al derecho fundamental de la privacidad, el cual se transgrede mediante la publicación no consentida de información personal, excediendo los límites de la libertad de expresión y vulnerando el derecho a la intimidad. Además, esta práctica ilícita puede dar lugar a la diseminación de contenido falaz o descontextualizado, comprometiendo la integridad de la información en el ecosistema digital.

Las evidencias encontradas en estos estudios reflejan la necesidad de una adecuación del marco jurídico penal respecto del delito de suplantación de identidad en el contexto digital. En este escenario Borghello y Temperini (2012) en su investigación "Suplantación de Identidad Digital como delito informático en Argentina" afirmaron que, "esta identidad digital está en situación de crisis, debido a los duros embates por parte de los ciberdelincuentes dedicados al robo y suplantación de identidades digitales" (p. 92).

Además, una investigación desarrollada por Chomczyk (2020) y leída en el trabajo de Moreno et al. (2022) demuestra que, países como Argentina, Bolivia, Brasil, Chile, Colombia, Costa Rica, Cuba, Ecuador, El Salvador, Guatemala, Haití, Honduras, México, Nicaragua, Panamá, Paraguay, Perú, República Dominicana, Uruguay y Venezuela carecen de regulación normativa eficiente que vele por la protección del derecho a la identidad en el entorno digital (pp. 692- 693). Es así que, esta situación provoca que las víctimas de estos actos que atentan

contra sus derechos reconocidos constitucionalmente queden en indefensión y que los infractores continúen atentando contra el bien jurídico protegido.

Este delito va en constante incremento con las nuevas tecnologías y su falta de regulación implica la impunidad frente a los ciberdelincuentes. La suplantación de identidad puede tener varios fines, entre los cuales se vale mencionar que, el beneficiarse económicamente a través de la captación de información financiera, o a su vez, atentar contra la dignidad y la reputación de la persona a quien suplantan la identidad. El segundo presupuesto es al que se enfoca la presente investigación. Por ello, se debe citar a Aquino (2020), quien en su tesina titulada "Comparación de Regulaciones Jurídicas sobre la Prevención del Robo de Identidad entre México y Argentina del Año 2010 Al 2018" menciona que:

> El delito de robo de identidad es un problema grave a nivel internacional pues el uso de la tecnología y el avance informático ha sido un significativo punto clave, pues mediante el uso del internet en la actualidad se ha convertido en la principal herramienta para llevar a cabo el robo de datos para posteriormente cometer el delito de robo de identidad. (p. 91)

Es decir, el robo de identidad o suplantación de identidad como lo denomina el Código Orgánico Integral Penal (COIP) evoluciona a la par de la sociedad digital, por ello es importante realizar un estudio doctrinario, jurídico y bibliográfico del estado actual de este tipo penal, de sus implicaciones legales y afectaciones a los Derechos Fundamentales reconocidos en la Constitución y en los Instrumentos Internacionales de Derechos Humanos.

Antecedentes históricos

La evolución tecnológica ha facilitado el acceso, uso y difusión de información personal en entornos digitales, provocando nuevos desafíos en la protección de los derechos fundamentales, como la privacidad y la identidad. Desde la expansión del uso del internet, el tratamiento de datos personales como nombres, imágenes, videos y otros elementos sensibles ha experimentado un notable incremento, lo que ha transformado no solo las relaciones sociales y económicas, sino también la dinámica jurídica en torno a la protección de la identidad y los datos personales.

Tal es el caso del delito de suplantación de identidad cuando involucra contenido sexual, que ha tomado relevancia en los últimos años debido a la facilidad con que se pueden generar

perfiles falsos, acceder a información privada o incluso modificar contenido audiovisual. Este fenómeno ha planteado serios desafíos en el ámbito penal, donde se discuten las condiciones de juzgamiento y sanción de estos delitos que no solo vulneran la identidad, sino que también constituyen agresiones directas contra la dignidad, intimidad, la integridad y la privacidad sexual de las víctimas. Las primeras normativas sobre el tratamiento de estos delitos datan de las últimas décadas, pero ha sido necesario un constante proceso de adaptación de las legislaciones para responder a la velocidad con la que las tecnologías avanzan y, con ellas, los medios para cometer estas infracciones.

A nivel internacional, distintos países han impulsado reformas penales que tipifican la suplantación de identidad con fines de difamación o explotación sexual. Sin embargo, el tratamiento judicial de estos casos varía considerablemente dependiendo de las particularidades jurídicas de cada jurisdicción, lo que ha generado debates sobre la proporcionalidad de las sanciones y la necesidad de armonizar criterios de justicia en delitos de esta naturaleza. Por esta razón, es importante realizar un abordaje de los antecedentes históricos sobre el manejo de la información personal y el juzgamiento del delito de suplantación de identidad con contenido sexual en el contexto nacional e internacional.

La protección de los datos personales aparece con el reconocimiento de los Derechos Humano a partir del siglo XVIII conectado al derecho a la intimidad. Es decir, la protección de los datos personales en la antigüedad no constituía un derecho reconocido expresamente, sino que de forma muy ambigua éste se vinculaba con el derecho a la intimidad. García (2007) dice que autores Samuel Warren y Louis Brandeins en 1890 a través de sus obras literarias sentaron las bases técnico- jurídicas de la privacidad. Siendo así que el derecho a la intimidad se reconoció expresamente en 1948 con la Declaración Universal de los Derechos Humanos, involucraba derechos como, la inviolabilidad de domicilio y de las comunicaciones, el secreto a la correspondencia (p. 754).

Ahora bien, cuando se habla de la protección de los datos personales Nisa (2020) explica que existen cuatro teorías. La primera denominada Spharentheorie o Teoría de las esferas o círculos concéntricos expuesta por Heinrich Hubmann en 1957 quien divide a la intimidad en tres esferas, la esfera en la que se encuentran aquellos datos que siendo privados bajo el consentimiento del titular llegan a difundirse en los espacios público; la segunda esfera se configura por aquellos datos que el titular considera confidenciales y puede transferir a otra persona de su confianza; la tercera esfera que son los datos más íntimos del individuo.

Por otro lado, Fernando Madrid Condesa en 1984 presenta la Teoría del Mosaico, que en lo principal considera que los datos son conceptos relativos y depende de la recepción de estos datos lo privado o público. Por su parte, en la Teoría del Right to Privacy o Theories of the Common Law of Torts que aparecen en países del Common Law presentada p en 1960 por William Prosser se menciona que para reclamar la protección de los datos debe reunir requisitos como: Intrusión en los asuntos privados del individuo, divulgación de datos íntimos que afecten a su titular, publicidad de los datos que afecten el prestigio de la persona, apropiación del nombre de la persona, voz o imagen.

Finalmente, la teoría más reciente publicada en el 2007 por Herman Tavani denominada La Restricted Acces/ Limited Control (RALC) Theory of Privacy, que intenta unificar las anteriores teorías y busca establecer qué datos son realmente necesarios de ser protegidos, sostiene que el hecho que una persona tenga acceso a la información privada, esto no quiere decir que tenga control sobre la misma.

En esta misma línea, hay que reconocer que el uso de datos personales provoca vulneraciones a derechos reconocidos constitucionalmente. Además, cuando estos datos son utilizados con la finalidad de efectuar actos ilícitos que afecten a la economía, dignidad y honra de la persona, a través del poder punitivo del Estado se impone sanciones penales. Tal es el caso del delito de suplantación de identidad, en el cual una persona sin el consentimiento del titular de los datos utiliza, nombres, apellidos o cualquier otro dato que identifique a una persona, con la finalidad de hacerse pasar por el titular y cometer a su nombre actos que afectan su reputación y dignidad, más aún cuando este acto incluye contenido sexual de la víctima. Cabe destacar que, este delito y su modo de operar a evolucionado conforme la sociedad avanza.

En la actualidad, la identidad es considerada desde distintas aristas que permite abordar el tema desde una perspectiva más amplia, de tal forma que, en el pensamiento de Cabrera et al. (2019) la identidad se divide en dos:

> La física y la digital, esta última, originada por el acelerado crecimiento que los medios de comunicación han tenido en los últimos años, marcado tendencias importantes en lo económico, fiscal y social, pero principalmente en la vida cotidiana y el desarrollo de sus actividades personales, laborales y de entretenimiento, naciendo así la identidad electrónica. (p. 243)

Cabrera et at. (2019) estudian la suplantación de identidad desde su yacimiento, encontrando que la recolección de información en inicios se dio de forma física, estos actos se efectuaban a través del hurto de billeteras, carteras, etc., el robo de identidad se lo conoció como Dumpster divig que consistía en buscar en la basura aquellos documentos que contengan información personal de los individuos. Considerablemente fue evolucionando a la manipulación de los datos personales de bancos, instituciones financieras a través del hackeo de claves en sistemas electrónicos. Este problema social se intensifica con la aparición de las nuevas tecnologías y en 1996 aparece el fraude por Suplantación de Identidad o Phishing, que trajo como consecuencia la apropiación de cuentas de American On line (p. 246).

Por otro lado, a juicio de Aquino (2020) este delito nace en Roma durante la edad antigua, evolucionando de forma acelerada hasta la actualidad.

Tabla 1: *Evolución del delito de suplantación de identidad.*

EVOLUCIÓN DEL DELITO DE SUPLANTACIÓN DE IDENTIDAD
EDAD ANTIGUA
La suplantación de identidad tiene sus bases en el delito de falsedad que en Roma era castigado de conformidad con lo establecido en la Ley Cornelia de Falsis. El primer caso de robo de identidad surge en Roma en dónde debido al aumento de senadores en el siglo I a.C y a la poca población masculina que cumplieran con los requisitos exigidos por los altos mandos para ocupar estos cargos, los esclavos manipulaban la información personal para acceder a estos cargos públicos. La *Lex Cornelia de falsis,* sancionaba el delito de falsedad inicialmente con la muerte del infractor.
EDAD MEDIA
Todavía no se hablaba de la suplantación o robo de identidad para la edad media, aún se mantenía sus cimientos en el delito de falsedad, pero más apegado con el Derecho canónico. Por lo cual, la mentira se consideraba un pecado ante Dios que tenía como castigo la muerte a través de la horca o el exilio. En 1539, surge el primer caso de robo de identidad como tal. Un individuo, aprovechándose de la similitud que tenía con un hombre llamado Martin Guerre, suplanta la identidad de este y ejecuta actividades a su nombre, como el vivir y tener descendencia con su esposa. Al ser descubierto, el impostor fue condenado a la horca como castigo a su acto que iba en contra de las normas de Dios.
EDAD MODERNA (siglo XV al XVIII)

Aparece el delito de suplantación de identidad, debido al incremento de casos de robo o usurpación de identidad mediante el uso de documentos que acreditaban la identidad de la víctima, este acto tenía como fin generar beneficios económicos.
EDAD CONTEMPORÁNEA (siglo XVIII al siglo XXI)
La edad contemporánea es caracterizada por los grandes avances de la sociedad, entre ellos se puede enmarcar, la revolución industrial, las guerras mundiales y principalmente, el avance tecnológico. En esta época, la suplantación de identidad toma mayor relevancia causada por el robo de identidad mediante los documentos encontrados en la basura, el robo de carteras físicas y tarjetas de crédito.
ERA DIGITAL
Phishing y Pharming, robo de identidad con la finalidad de generar recursos económicos. Los datos son sustraídos principalmente a través de tarjetas de crédito, de débito, cuentas bancarias, comercio o correos electrónicos.

Nota: Aquino (2022).

En 1837 el Ecuador en su normativa penal no contemplaba aún el delito de suplantación de identidad, sin embargo, como se dijo *ut supra*, este delito tiene su fundamento en las actuaciones de falsificación de monedas o documentos. Así, El Código Penal de 1837 del Ecuador integra en el título IV "De los Delitos contra la Fe Pública" el delito de la Falsificación de monedas, además en el Capítulo III refiere sobre "De las falsedades que se cometen en documentos públicos y privados, y en los Pesos y Medidas" en la sección II "De las falsedades en documentos privados" y se establece:

> Art. 255.- Los que a sabiendas y en perjuicio de tercero, contrahicieren o alteraren escritos o documentos privados, o borraren, suprimieren, o arrancaren lo que estuviere en ellos escrito, o añadieren lo que no estaba o se mudaren en el nombre o apellido, o fingieren firma, rúbrica o sello, o falsificaren, o contrahicieren las marcas, sellos o contraseñas de algún individuo en particular o de alguna fábrica o establecimiento mercantil que algunos tengan, o de cualquiera otra manera cometieren falsedad en documento privado, serán condenados en la pena de reclusión por dos a seis años.

Definición y clasificación de datos.

Es importante señalar que el término "dato" es sinónimo de información, referencia, documento. Bajo esta línea Jara (2021) considera que los datos son aquella información sobre

algo determinado, que ayuda a obtener el conocimiento exacto o a su vez deducir las consecuencias de un hecho (p. 104). De la misma forma, el Diccionario panhispánico del español jurídico señala que dato es la información suficiente para el conocimiento de algo. Entonces, constituyen información estructurada sea de entidades, personas, objetos o sistemas, que permite describir fenómenos, identificar patrones, representar aspectos específicos de los individuos, sus relaciones, objetos, etc., capaces de ser recopilados, archivados, procesados o transmitidos y que pueden estar contenidos en fichas, ficheros, ordenadores, redes, o cualquier otro soporte material.

Además, son antecedentes que conllevan a tener un conocimiento exacto sobre cualquier cosa a la que se refiera, así como para verificar las consecuencias legítimas de un hecho, debido a que, representan ideas, sentimientos, sensaciones y aspectos de la realidad física. El conocimiento generado con los datos se materializa mediante de códigos comunes de comunicación que utiliza la humanidad. Considerando esto, la importancia de los datos radica en la calidad de información que proporcionan y la protección jurídica que genera.

De manera puntual, los datos, según Jara (2021) se clasifican en:

- **Datos según el soporte sobre el cual se materializa:** Datos analógicos, datos digitales.
- **Datos según su fuente de conocimiento:** Datos brutos o primarios y datos derivados o secundarios.
- **Datos según su contenido:** Datos personales (el subrayado me corresponde), datos no personales y datos anonimizados.
- **Datos según si los datos son públicos o privados.**

Si bien el término "datos" abarca una definición amplia y general, es esencial tomar este concepto como base para el presente estudio. Así también, es importante diferenciar el término “datos” de “información” el primero debe entenderse como una recopilación en bruto de forma sea numérica, cualitativa, en letras, caracteres u otros que representan simbólicamente, mientras que la información se constituye como el conjunto de datos procesados y asociados a una persona determinada o determinable.

Datos Personales

La sociedad es el conjunto de individuos que se relacionan entre sí, conviven y se desarrollan cultural, social y económicamente. Esta convivencia implica que cada persona genere aspectos propios que los ayude a identificarse dentro de un conglomerado. En este contexto, aparecen

los datos personales cuya finalidad es singularizar a los individuos. Para Ayjón (2020), los datos personales constituyen aquella información relativa al sujeto como nombres, apellidos, edad, sexo, fecha y lugar de nacimiento, domicilio, documento nacional de identidad o pasaporte (pp. 93- 94). Añadido a esto, Machuca et al. (2022) aluden que estos datos son los registros o información que vinculada o no con otros datos revela la identidad de una persona viva (p. 248). Son una subcategoría de los datos en general y adquieren carácter personal cuando estos se vinculan con sujetos de la especie humana. De manera que, el ordenamiento jurídico a reconocido el derecho a su protección.

En esta misma línea, es preciso citar el Dictamen 4/2007 sobre el concepto de datos personales, elaborado por el Grupo de Trabajo sobre la protección de datos del artículo 29 en el que se menciona "estos datos pueden definirse como propiedades biológicas, características fisiológicas, rasgos vitales o acciones repetibles cuando dichas características y/o acciones son a la vez exclusivas de ese individuo" (p. 12). Es decir, existe una vinculación entre el dato y la persona.

En efecto, los datos personales que se vinculan a los individuos son considerados como bienes jurídicos protegidos. Siendo así, en el ámbito legal, el Convenio n°. 108 del Consejo de Europa del 25 de enero de 1981 uno de los primeros instrumentos jurídicos en reconocer el derecho a la protección de los datos personales, establece que "datos de carácter personal significa cualquier información relativa a una persona física identificada o identificable" (Art. 2.a).

Es importante definir cuando una persona es considerada identificada o identificable. Para ello, es necesario citar a Roca (2021) quien menciona que, es identificable cuando un dato no muestra la identidad de la persona o aporta información suficiente sobre ésta, pero permite establecer una investigación para saber su identidad. Mientras que, es identificada cuando sin la necesidad de ejecutar investigaciones y a través de un dato personal se logra conocer la identidad, señala como ejemplo, el DNI o el pasaporte (p. 217). Es decir, los datos tienen como fin construir la identidad de los individuos, es algo propio, íntimo y privado.

Tabla 2: Componentes y alcance de la definición de datos personales.

"Cualquier información relativo a una persona identificada o identificable"	
Componentes	**Alcance**
	Permite la conceptualización amplia de datos personales. Abarca información objetiva, como aquella en la que se determina una sustancia en

Cualquier información	la sangre, y/o subjetiva, que involucra las opiniones y valoraciones. Además, desde el punto de vista del contenido, el concepto de datos personales incluye la información relativa a la vida privada, familiar y pública del individuo. En definitiva, la información contenida sea en forma física o almacenada en la memoria de un ordenador y en cualquier forma, sea alfabética, numérica, gráfica, fotográfica o acústica, es parte de los datos personales. En definitiva, el abanico de información que engloba esta definición hace que la información personal de un individuo trascienda más allá de la esfera de la intimidad.
Relativo a	Engloba al hecho del "vinculo" o "relación" que deben tener estos datos con las personas. Dado que los datos se refieren a una persona cuando señalan la identidad, características o el comportamiento del individuo o si la información obtenida sirve para saber de quién se trata, es decir establecer su identidad, solo ahí aparece el vínculo entre dato y persona. También se habla de un vínculo cuando el uso de estos datos cause un impacto a los derechos de los titulares.
Persona física	Alude al individuo de la especie humana, considerado por el código civil ecuatoriano como persona natural.
Identificado	Una persona es considerada identificada cuando dentro de la colectividad logra distinguirse de todos los miembros que la integran. Se señalan indicadores que hacen que una persona sea identificada directa o indirectamente signos externos de la apariencia de la persona, altura, color de cabello, ropa, número de identificación, elementos específicos, características de su identidad física, fisiológica, psíquica, económica, cultural o social. ***Directa:*** Un indicador común establece la identidad (nombre y apellido). ***Indirecta:*** Es necesario la combinación de más indicadores para establecer la identidad (un nombre común debe vincularse con otros indicadores como fecha de nacimiento, etc.)
Identificable	No establece la identidad por sí sola, sino que debe efectuarse un análisis profundo para determinar la identidad e individualidad del sujeto. Se pueden señalar características fisiológicas únicas del individuo.

Nota: Información extraída del Dictamen 4/2007 sobre el concepto de datos personales.

Corral y Peschard (2010) consideran que la función principal de los datos personales es otorgarle al individuo entre otras cosas, identidad; describen y precisan aspectos comunes como su origen, edad, lugar de residencia, trayectoria en el ámbito académico, laboral o profesional y aspectos íntimos como su psiquis, salud, características físicas, ideológicas o su vida sexual (p. 6). En este sentido, la gestión de los datos personales dirigidos a preservar la privacidad del individuo es fundamental para proteger su dignidad. Pues, el avance tecnológico en el manejo adquiere una dimensión diferente, ya que el acceso y uso inadecuado de los datos personales genera afectación a los derechos de las personas.

En este contexto, los datos personales se involucran directamente con los derechos fundamentales y libertades de las personas reconocidos a nivel constitucional y en instrumentos jurídicos nacionales e internacionales, llegando adquirir incluso un valor económico, puesto que los datos son claves en el tráfico financiero y empresarial. Para adquirir la categoría de "personales" es fundamental que los datos de forma independiente o combinada con otra información identifique a un individuo de los demás. Pues la sociedad civil constantemente comparte y difunde sus datos personales, ya sea de manera física o virtual, siendo estos un componente de la identidad del individuo en la colectividad.

Autores como Cornejo y Sánchez (2023) señalan que los datos de carácter personal forman parte fundamental de la identidad y contienen información confidencial de los individuos (p. 996). Además, por su relevancia en la vida de las personas y su impacto en la privacidad, los datos personales son considerados bienes jurídicos protegidos en varias legislaciones incluida la ecuatoriana.

Datos personales en la era digital

La revolución industrial caracterizada por los avances económicos, sociales y tecnológicos provocó una transformación en la sociedad. Es así como el advenimiento tecnológico fue la base sobre la cual se cimienta la creación de las Tecnologías de la Información y la Comunicación que a criterio de **Machuca et al. (2022)** "permite el desarrollo e interacción de nuevas formas, medios y tiempos de relaciones social, nuevas formas de relaciones de las empresas y sus clientes, nuevas formas de aprehensión personal y social" (p. 244). Este cambio social, genera que los datos personales trasciendan más allá del aspecto físico, a un espacio en el medio digital. En consecuencia, la identidad o forma de identificar a una persona pasa de un plano físico a uno virtual.

Teniendo presente este aspecto, **Llaneza (2021**) explica que la identidad personal responde a la pregunta ¿Quién soy? que engloba los aspectos esenciales de una persona. En esta misma línea Charles Taylor citado por Llaneza (2021) considera que ayuda a efectuar una distinción del individuo dentro de un grupo social y esto involucra la forma de vestir, hablar, comportarse, interactuar, etc. En cambio, la identidad digital es aquella información sobre una entidad utilizada por los sistemas informáticos, cuya finalidad es representar a un agente externo, sea este una persona, organización o dispositivo. En este sentido, se habla de un traspaso de una identidad legal al mundo online. En el cual un individuo puede representarse socialmente en un contexto virtual a través del uso de medios tecnológicos. Esta identidad puede incluir datos personales como, nombre, fotos, entre otros. Esto debido a que la información se trasmite en las redes y los datos son captados, almacenados y tratados desde ese espacio virtual, imposibilitando localizaros y controlarlos.

Además, la Declaración Internacional sobre los Datos Genéticos Humanos estatuye que la identidad de una persona no se reduce a sus rasgos genéticos, sino que abarca factores educativos, ambientales personales, lazos afectivos, sociales, espirituales y culturales, esto conlleva a la dimensión de libertad (Art. 3). Dicho de otra manera, la identidad es el conjunto de aspectos individuales o sociales que forman parte de la individualidad del ser humano.

Bajo esta línea, el Diccionario panhispánico del español jurídico incorpora la definición de datos personales de una forma más amplia e incluye "cualquier información numérica, alfabética, gráfica, fotográfica, acústica o de cualquier otro tipo que refiere a personas físicas identificadas o identificables". Además, el Reglamento (UE) 2016/679 del parlamento europeo y del Consejo de la Unión europea señala que la identidad de una persona puede determinarse de forma directa o indirectamente a través de un indicador como "un número de identificación, datos de localización, un identificador en línea o uno o varios elementos propios de la identidad física, fisiológica, genética, psíquica, económica, cultural o social de dicha persona" (Art. 4.1).

Ahora bien, es importante tener en cuenta que el reconocimiento de los datos personales a nivel doctrinario, legal y jurisprudencial evoluciona conforme el avance tecnológico. Es así que el **Tribunal de Justicia de la Unión Europea (TJUE)** en el caso Peter Nowak contra Data Protection Commissioner demuestra que el alcance de los datos personales va más allá del conjunto de presupuestos como nombres, apellidos, entre otros. Manifiesta en su sentencia sobre el asunto C-434/16 que, cuando se refiere a que un dato personal es toda información, que incluye más que aquella que es confidencial o relacionada con la intimidad, pues alcanza

un nivel mucho más amplio que integra a "todo género de información, tanto objetiva como subjetiva, en forma de opiniones o apreciaciones, siempre que sean «sobre» la persona en cuestión" (párr. 31).

Roca (2020) sostiene que:

> Según el TJUE, por otro lado, el concepto de dato personal es muy amplio, son datos personales, entre otros: nombre y número de teléfono o información sobre condiciones de trabajo y/o aficiones, datos bancarios (ingresos, etc), datos personales que obran en poder del municipio, perfiles de usuarios de redes sociales, datos conseguidos por un detective privado, datos de registro de trabajo (periodos de trabajo, descanso, etc), la imagen de una persona grabada por una cámara, los daos fiscales, las respuestas escritas de un examen y las anotaciones del examinador, los que figuran en una minuta (nombre, fecha de nacimiento, nacionalidad, sexo, étnica, religión e idioma, etc. También, según el TEDH, las comunicaciones escritas o habladas e imágenes, las filmaciones o sonidos de circuido cerrado de televisión. (pp. 181-182)

Entonces vale decir que, los datos personales son como un bien inmueble inscrito a nombre del titular, que puede disponer a su conveniencia libre y voluntariamente, sin intromisiones ajenas. Esta metáfora cobra sentido toda vez que cualquier individuo puede usar sus datos personales en el sentido que este disponga. Toda apropiación o tratamiento ilegal de los datos personales constituiría un delito, puesto que se está atentando contra la intimidad de los individuos. La fuerza informática que se vive en la actualidad hace que mediante los datos digitales se establezcan ciertos perfiles de una misma persona, que afecta a la intimidad o que generan actitudes discriminatorias e intolerantes.

En la jurisprudencia ecuatoriana la Corte Constitucional (CC) a través de la Sentencia No. 2064-14- EP/21 a considerado que el concepto de dato personal, así como el hábeas data es amplio, dado que incorpora cualquier tipo de dato que se relaciona a una persona identificándola o haciéndola identificable. De manera que, la CC afirma que

> La imagen puede revelar la identidad de la persona (es decir que la identifica), por ejemplo, cuando contenga su rostro, aunque también podría ser que cuente con algún otro elemento que inmediatamente permita reconocer la identidad del titular de ese dato, tal como su número de cédula, identificación o nombre. A su vez, también se constituye en dato personal aquella fotografía que, si bien no contiene el rostro de esta o algún otro

> elemento que la identifique de manera inmediata, permitiría el reconocimiento de aquella de manera mediata (es decir que la hace identificable). (párr. 78)

La constante evolución social provoca el surgimiento de nuevas formas de interactuar, convivir y desarrollarse. En el contexto de la sociedad digital, los individuos empiezan a crear nuevas formas de identificarse en el mundo digital, de ahí que los datos personales actualmente han adquirido una importancia creciente como bienes jurídicos protegidos, dado su valor no solo para la identidad y privacidad de los individuos, sino también para el correcto funcionamiento de las interacciones sociales. Ya que el origen de la protección de los datos personales radica en el derecho a la intimidad, entendida como el derecho a estar solo y sin injerencias.

Según **Pizarro (2022)** el derecho a la intimidad involucra que el individuo goza de la plena protección de su persona y en su propiedad. Está ligado con el derecho a la vida y el hecho de disfrutarla (p. 32). Por lo tanto, con el reconocimiento del valor legal de los sentimientos, la protección contra lesiones corporales reales se extendió hasta prohibir las simples amenazas o tentativas; es decir, poner a otro en la eventualidad de lesionar o ser lesionado. Conlleva un respeto de la reputación y posición del individuo frente a sus semejantes. Por ello se puede considerar que constituye garantía fundamental que protege la esfera privada de las personas contra intervenciones no deseadas, ya sean del Estado, de individuos u organizaciones.

Es importante tener claro que este derecho abarca varios aspectos de la vida personal, incluyendo la protección de datos personales, la privacidad en el hogar, la correspondencia, las comunicaciones y la información personal. Su objetivo es asegurar que cada individuo tenga control sobre su información personal y su vida privada, evitando intromisiones y divulgaciones no autorizadas. El derecho a la intimidad es reconocido y protegido por diversas legislaciones nacionales e internacionales como la Declaración Universal de Derechos Humanos y el Pacto Internacional de Derechos Civiles y Políticos. En la era digital, la protección de este derecho se ha vuelto aún más crucial debido a los avances tecnológicos que facilitan la recopilación, almacenamiento y distribución de datos personales.

Ahora bien, en la sentencia No. 2064-14-EP de la Corte Constitucional, los jueces mencionan que en la jurisprudencia constitucional de Colombia se fija que este derecho tiene dos dimensiones, la primera tiene que ver con el secreto que limita la divulgación de hechos o documentos privados, la segunda dimensión versa sobre la libertad, es decir la capacidad de todos los individuos para tomar decisiones propias en su vida. Por ende, el Estado a través de su ordenamiento jurídico debe garantizar la protección de este derecho.

Características de los datos personales

- **Gozan de regulación especial:** Según Jara (2021) los datos personales se diferencian de aquellos "impersonales" puesto que al identificar o permitir identificar a una persona natural, adquieren un valor inherente mayor y se regulan legalmente en varias jurisdicciones del mundo.
- **Se vincula a una persona natural viva:** Los datos personales identifican o hacen identificable a una persona natural, pues según Jara (2021), la información de las personas jurídicas es recopilada en un proceso industrial, macroeconómicos o financieros. Por ello, el titular de los datos personales es el individuo al que identifican los indicadores como nombres, apellidos, imágenes, etc. De tal manera, no constituyen datos de carácter personal la información de personas jurídicas, siempre y cuando no identifiquen a propietarios, empleados, directores, socios, etc., y la información de las personas fallecidas.
- **Son personalísimos y extrapatrimoniales: Argüello (2022)** considera que los datos personales son derechos subjetivos inherentes al ser humano, debido a que es información representada simbólicamente, además, se relacionan con el derecho a la intimidad, a la imagen y a la identidad. Sumado a aquello, adquieren la característica de ser extrapatrimoniales, es decir son intrasmisibles e inembargables. Al ser personalísimos, permite que los titulares gocen de la capacidad independiente de disponer de forma total y absoluta de sus datos personales, con la finalidad de impedir el tráfico ilícito o mal uso que afecten a su dignidad, intimidad, buen nombre.

Alcance de los datos personales

En el contexto digital actual, la recopilación, almacenamiento y procesamiento de datos personales ha adquirido una importancia central, generando debates sobre la privacidad, la seguridad y los derechos individuales. El acceso y uso de la información personal en línea plantea desafíos significativos en cuanto a la protección de los datos sensibles, especialmente en un entorno donde las interacciones digitales proliferan y las tecnologías avanzadas permiten el seguimiento y análisis exhaustivo de los comportamientos de los usuarios. Por ello, es esencial determinar el alcance y las implicaciones de la gestión de los datos personales en el ámbito digital.

Como se ha venido mencionando en esta investigación, los datos personales están integrados por indicadores específicos que permiten identificar a una persona. Sin embargo, el alcance de los datos personales va más allá de la información que aporte un indicador. Pues, los datos

considerados como “no personales” y obtenidos a través de la base de datos de registros electrónicos también pueden identificar a una persona cuando se vincula con otro dato.

En este sentido, Roca (2021) explica sobre los datos personales compuestos que tienen carácter personal, pero que se integra de datos no personales y sobre los metadatos (p. 223). El primero, permite identificar a una persona cuando este se vincula con otro que permite establecer la identidad del individuo. Por otro lado, los metadatos entendidos como aquellos que rodean un registro de actividad, por ejemplo, en una llamada, en una fotografía, en la publicación de tweet, los metadatos llegan a ser los registros de hora, fecha, duración, destinatario, cantidad de caracteres, etc. Estos registros de una comunicación electrónica como la navegación en la web y la transferencia al servidor tienen como consecuencia conformar un perfil completo de una persona física e identificarla, ofreciendo detalles íntimos sobre la vida privada sobre la persona física.

En resumen, los datos que son considerados como no personales, no están contemplados en la protección jurídica de los instrumentos normativos. Sin embargo, se debe considerar a estos datos en su conjunto para que constituyan datos de carácter personal. De modo que la información que aportan los datos no personales tiene un inmenso valor, pese a que en el ámbito jurídico no puedan ser considerados como personal. La combinación de estos datos no solo permite identificar a las personas a través de los rastros de registro, sino que construye datos personales y detalles íntimos de una persona.

Bajo este argumento, el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016 en su considerando 30 establece:

> Las personas físicas pueden ser asociadas a identificadores en línea facilitados por sus dispositivos, aplicaciones, herramientas y protocolos, como direcciones de los protocolos de internet, identificadores de sesión en forma de «cookies» u otros identificadores, como etiquetas de identificación por radiofrecuencia. Esto puede dejar huellas que, en particular, al ser combinadas con identificadores únicos y otros datos recibidos por los servidores, pueden ser utilizadas para elaborar perfiles de las personas físicas e identificarlas. (p.6)

Componentes de los datos personales

Los datos personales como se ha mencionado *ut supra* se componen por indicadores generales como nombres, apellidos, DNI, entre otros. Sin embargo, estos indicadores se categorizan

conforme a la información que integran sobre el individuo. La Corte Constitucional ecuatoriana en la sentencia No. 1868-13-EP determina que

> como primer componente del concepto de dato personal, que es todo tipo de información objetiva o subjetiva –independientemente de su veracidad o no– respecto de una persona. Los datos personales comprenden información relativa a la vida privada de una persona, así como a la vida pública. El segundo componente de la definición de datos personales es información que versa "sobre" una persona, cuando se refiere a ella. (párr. 22)

De modo que, los datos personales incluyen datos relativos a la vida privada y familiar, así como información sobre actividades desarrolladas en las diferentes relaciones sociales, laborales, económicas o sociales. La normativa, jurisprudencia y doctrina, han categorizado los datos personales conforme a la información que aportan para establecer la identidad de las personas. Así, se puede señalar:

Datos personales sensibles: También son denominados datos merecedores de "especial protección" o datos de "carácter especial", en vista de que reflejan situaciones que incluyen ideología, religión, creencias, origen racial, salud, vida sexual, entre otros. Conforme Peyrano (2002) la especial protección por parte de la normativa jurídica radica en que estos datos afectan a la esfera más íntima de las personas y por "motivaciones de orden político, social, histórico y cultural, no necesariamente relacionadas con razones personales" (514). Estas últimas se enfocan a evitar situaciones de discriminación social por prejuicios históricos, culturales y sociales que debido al comportamiento social se han demostrado a lo largo de la historia de la humanidad. Pues información referente a etnia, raza, ideología, políticas, inclinaciones sexuales, situaciones socioeconómicas, estado de salud, entre otros, ha categorizado a los individuos, produciendo efectos discriminatorios y desigualitarios.

Los datos de carácter personal considerados sensibles gozan de una voluntad de reserva, es decir que se necesita irrestrictamente el consentimiento de su titular para ser difundido o efectuar cualquier tratamiento sobre estos, dado que representan realidades sociales capaces de provocar actitudes discriminatorias a sus titulares y atentar contra la intimidad y privacidad. Peyrano (2002) considera que para ser datos sensibles es necesario el análisis del caso concreto, es decir la aptitud de generar conductas o actos de discriminación (p. 517). Así por ejemplo, se puede mencionar que la estatura por sí sola no constituye un dato personal sensible, pero puede llegar a serlo cuando en la convivencia social genera discriminación a su titular y por ende

merece una protección especial. La utilización indebida de este tipo de datos da origen a una discriminación ilegal o arbitraria o conlleva a generar un riesgo grave a su titular. Esto debido a que esta categoría de datos personales por su naturaleza podría generar riesgos a los derechos y libertades fundamentales.

De tal forma que el RGPD dispone que los daos sensibles que se relacionan con derechos y libertades fundamentales deben tener una protección especial. Esto toda vez que no todos los datos personales sobre una persona física tienen el mismo impacto y su divulgación o tratamiento indebido provocaría afectaciones a derechos reconocidos a nivel interno e internacional. Para Jove (2021) identificar los datos que adquieren esta calidad de sensibles es una tarea altamente complicada, debido a que a nivel global no existe un consenso sobre la información que debe ser considerada como tal (p.347).

Los datos sensibles son categorizados por diferentes autores. Por ejemplo, Cristea (2018) señala que los datos sensibles deben ser analizados desde dos aristas uno material y otra formal. En el punto material, revelan cualidades de las personas que se relacionan con su dignidad, personalidad, forma de ser o comportarse; desde la perspectiva formal los datos son susceptibles de especiales y reforzadas garantías de uso, tratamiento y voluntad de la persona. Herrán (1998) por su parte considera que estos datos deben ser distinguidos de acuerdo con el contenido, así, en primera instancia se agrupan información referida a la libertad ideológica o creencias religiosas, mientras que en el segundo grupo se integran aquellos sobre el origen racial, comportamiento sexual y salud (p. 263). Entonces, los datos de carácter sensible pueden dividirse en tres bloques, en el primero se integran aquellos datos que reflejan ideología, afiliación sindical, religión y creencias, en el segundo bloque se incluyen datos sobre el origen racial, la salud y la vida sexual, mientras que el último abarca datos sobre infracciones penales o administrativas.

En Ecuador, la Ley Orgánica de Protección de Datos Personales reconoce que los datos sensibles son:

> 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. (Art. 4)

El tratamiento de estos datos es de carácter especial, razón por la cual, es necesario el consentimiento expreso de su titular, pues estos datos afectan a la esfera más íntima y privada del individuo. En este contexto, la Sentencia No. 2064-14-EP/21 de la Corte Constitucional del Ecuador (CCE) menciona que las fotografías que reflejan la vida sexual de su titular son muy personales y por sus características constituyen datos de carácter sensible puesto que afectan a la esfera íntima.

En esta misma línea, vale señalar el criterio de la CCE contenido en la Sentencia No. 77-16-IN/22 sobre los aspectos que integran la intimidad. Este ente constitucional refiere que "En la intimidad, una persona es libre de desarrollar su personalidad, formar su pensamiento, explorar su creatividad, sexualidad, su ideología, etc." (Párr. 42). Es decir, que este derecho permite que el individuo tenga libertad personal, de manera que pueda desenvolverse en la sociedad sin injerencias y pueda gobernarse a sí mismo. Cuando terceros tienen acceso a información privada esto podría afectar a la convivencia social y atentar contra la dignidad de las personas. La Corte establece que la información privada permite un control del titular; esta información como mensajes enviados a familiares, chats de grupos de trabajos, contraseñas de acceso, información de ahorros y finanzas, conversaciones y otros, son algunos ejemplos de acontecimientos que no son difundidos a la luz pública y por tanto, pertenecen a la esfera íntima y privada de las personas.

Corolario a este reconocimiento jurídico que hace la normativa ecuatoriana el Convenio 108 de la Unión Europea ha reconocido una categoría particular de datos en la que se incluyen datos personales sobre origen racial, opiniones políticas, convicciones religiosas u otras convicciones, datos sobre la salud o la vida sexual, datos referentes a condenas penales. El Reglamento de la Unión Europea (UE) 2016/679 del Parlamento Europeo y del Consejo añade a esta categoría, datos sobre la afiliación sindical, datos genéticos, datos biométricos dirigidos a identificar de manera unívoca a una persona física, datos sobre la salud, orientación sexual de una persona física (Art. 9).

Datos biométricos: Los datos biométricos ha emergido como un campo clave en la intersección entre tecnología, seguridad y derechos individuales. Estos incluyen características físicas y conductuales como huellas dactilares, reconocimiento facial, patrones de voz y escaneo del iris, se han convertido en herramientas fundamentales para la identificación y autenticación de personas en diversos sectores. Burzaco (2020) describe a los datos biométricos como la información obtenida mediante un tratamiento técnico específico, señala aspectos

relativos a las características físicas que hagan o confirmen la identificación única de la persona, entre algunos ejemplos están, las imágenes faciales o datos dactiloscópicos (p. 22).

Similar definición está contenida en el Art. 4 de la Ley Orgánica de Protección de Datos Personales del Ecuador, "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" (Art. 4). En el ámbito legal internacional el Reglamento (UE) 2016/679 de la Unión Europea recoge la misma conceptualización sobre estos datos. Por su parte la Ley 1581 de 2012 de Colombia reconoce a los datos biométricos como parte de los datos sensibles (Art.5). La legislación española señala la misma definición, sin embargo, en su preámbulo añade que los datos biométricos se incluyen en la categoría especial de datos, siempre que su tratamiento esté dirigido a identificar de manera unívoca a una persona física. Este hecho se visibiliza en materia penal, cuando parte de las investigaciones es determinar a través de estos datos la comisión de algún delito, a través de sus huellas dactilares o imágenes faciales.

Datos genéticos: Según la Declaración Internacional sobre los Datos Genéticos Humanos estos datos constituyen la información que reflejan características hereditarias de las personas y que son obtenidas mediante el análisis de Ácido Nucleico u otros científicos vinculados con este (Art. 2). Por su condición, estos forman parte de los datos sensibles, ya que indican predisposiciones genéticas de los individuos, pueden incluir información familiar cuya relevancia no se conozca públicamente y desde el punto de vista social y cultural traigan consigo actos discriminatorios. Se habla de una esfera íntima individual y familiar. De ahí nace la necesidad de que su tratamiento sea con el consentimiento de su titular y su divulgación no implique vulneraciones a sus derechos.

Liceda (2011) estima que los datos biológicos forman parte de la condición del ser humano como ser vivo e integran componentes como el ADN, sexo, sangre, cuestiones referentes a enfermedades (p. 298). Este reconocimiento permite que la legislación se regule conforme las necesidades de su protección.

Datos personales en la legislación española, europea, colombiana, y ecuatoriana.

Tabla 3*: Reconocimiento jurídico de datos personales en la legislación española, europea, colombiana y ecuatoriana.*

	Legislación	**Datos personales**	**Datos sensibles**
E S P A	Ley Orgánica 7/2021, de 26 de mayo, de protección de datos personales tratados para fines de prevención, detención, investigación y enjuiciamiento de infracciones penales y de ejecución de sanciones penales.	Toda información sobre una persona física identificada o identificable (el interesado); se considerará persona física identificable a toda persona cuya identidad pueda determinarse, directa o indirectamente, en particular mediante un identificador, como por ejemplo un nombre, un número de identificación, unos datos de localización, un identificador en línea, uno o varios elementos propios de la identidad física, fisiológica, genética, psíquica, económica, cultural o social de dichas personas. (Art. 5)	Son considerados como categorías de datos especiales y establece en su artículo 13 que el tratamiento de datos personales que revelen el origen étnico o racial, las opiniones políticas, las convicciones religiosas o filosóficas o la afiliación sindical, así como el tratamiento de datos genéticos, datos biométricos dirigidos a identificar de manera univoca a una persona física, los datos relativos a la salud o a la vida sexual o a la orientación sexual de una persona física, se permite con sujeción a las garantías, principios y derechos establecidos en el ordenamiento jurídico.
	Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales.	Adopta los efectos previstos en el artículo 4.1 del Reglamento (UE) 2016/679.	Contempla lo determinado en el Reglamento (UE) 2016/679. Los datos que puedan generar situaciones discriminatorias como la ideología, afiliación sindical,

ÑA			religión, orientación sexual, creencias u origen racial o ético, son considerados categorías especiales.
	Ley 11/2022, de 28 de junio, General de Telecomunicaciones.	Reconoce y protege los datos personales de los usuarios en el contexto de las comunicaciones electrónicas. Establece parámetros como la prohibición de recibir llamadas automáticas sin intervención humana ni mensajes de faz con fines comerciales a menos que haya otorgado el consentimiento previo. Esta normativa refuerza la privacidad de los ciudadanos y establece medidas para garantizar que solo personal autorizado tenga acceso a los datos personales.	Enfatiza que el tratamiento de datos personales debe ser realizado conforme a lo establecido en el Reglamento (UE) 2016/679, que incluye disposiciones específicas sobre datos sensibles.
	Ley 34/2002, de 11 de julio, de Servicios de la Sociedad de la Información y de Comercio Electrónico	Establece un marco normativo que protege a los datos personales de los usuarios en el ámbito legal, busca garantizar la privacidad y seguridad en transacciones electrónicas. La ley impone a los prestadores de servicio la obligación de obtener el consentimiento expreso de los usuarios para el tratamiento de sus datos personales, especialmente en el contexto de comunicaciones comerciales electrónicas.	No establece un ámbito de protección específica para esta categoría de datos, sin embargo, contempla la aplicación de los presupuestos contenidos en la normativa de la Unión Europea.

		Se establece una pena de prisión de uno a cuatro años y una multa de 12 a 24 meses a la persona que, sin tener la autorización, se apodere, utilice o modifique, en perjuicio de tercero, datos reservados de carácter personal o familiar de otro que se hallen registrados en ficheros o soportes informáticos, electrónicos o telemáticos, o en cualquier otro tipo de archivo o registro público o privado. (Art. 197.2)	La utilización de datos personales sensibles en la legislación penal española contempla una sanción superior. Es así como expresamente menciona que cuando los hechos de apodarse, utilizar o modificar datos reservados de carácter personal o familiar "afecten a datos de carácter personal que revelen la ideología, religión, creencias, salud, origen racial o vida sexual, o la víctima fuere un menor de edad o una persona con discapacidad necesitada de especial protección" (Art. 197. 5). Se castiga con una pena en su mitad superior de prisión de uno a cuatro años.
	Agencia Española de Protección de Datos (AEPD):	Este organismo es responsable de supervisar y garantizar el cumplimiento de la normativa sobre protección de datos en España. Proporciona directrices, resuelve reclamaciones y actúa como punto de contacto para los ciudadanos que deseen ejercer sus derechos relacionados con sus datos personales. Es una autoridad administrativa independiente del ámbito estatal.	
	Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación	La normativa contempla que datos personales es: Toda información sobre una persona física identificada o identificable (el interesado); se considerará persona física identificable a toda persona cuya identidad pueda determinarse, directa o indirectamente, en particular mediante un identificador,	Los datos personales considerados dentro de las categorías especiales según el Reglamento son aquellos que revelen el origen étnico o racial, las opiniones políticas, las convicciones religiosas o filosóficas, o la afiliación sindical, y el tratamiento de datos genéticos, datos biométricos dirigidos a identificar de manera unívoca a una persona física, datos

UNIÓN EUROPEA	de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos).	como por ejemplo un nombre, un número de identificación, unos datos de localización, un identificador en línea, uno o varios elementos propios de la identidad física, fisiológica, genética, psíquica, económica, cultural o social de dichas personas. (Art. 4.1)	relativos a la salud o datos relativos a la vida sexual o las orientación sexuales de una persona física. (Art. 9.1)
	DIRECTIVA (UE) 2016/680 DEL PARLAMENTO EUROPEO Y DEL CONSEJO de 27 de abril de 2016 relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por parte de las autoridades competentes para fines de prevención, investigación, detección o enjuiciamiento de infracciones penales o de ejecución de sanciones penales, y	Contempla la definición establecida por el Reglamento (UE) 2016/679.	Adopta lo establecido en el Reglamento (UE) 2016/679.

	a la libre circulación de dichos datos y por la que se deroga la Decisión Marco 2008/977/JAI del Consejo.		
	Comité Europeo de Protección de Datos (CEPD).	Conforme el Reglamento (UE) 2016/679, El CEPD es un organismo independiente de la Unión Europea, encargado de la aplicación del Reglamento General de protección de dato, sustituye al Grupo de protección de las personas en lo que respecta al tratamiento de datos personales.	
	Supervisor Europeo de Protección de Datos (SEPD).	Según la Unión Europea, este organismo tiene como función garantizar que las instituciones y organismos de la UE respeten el derecho a la intimidad de los ciudadanos a la hora de efectuar un tratamiento sobre los datos personales. Además, supervisa el tratamiento de datos personales, asesora a las instituciones y organismos de la UE, atiende reclamaciones y realiza investigaciones, colabora con autoridades nacionales en relación a la protección de datos personales y realiza un seguimiento a las nuevas tecnologías que generen incidencia en la protección de los datos personales.	
	Ley 1581 de 2012	Cualquier información vinculada o que pueda asociarse a una o varias personas naturales determinadas o determinables.	Aquellos que afectan la intimidad del Titular o cuyo uso indebido puede generar su discriminación, tales como aquellos que revelen el origen racial o étnico, la orientación política, las convicciones religiosas o fisiológicas, la pertenencia a sindicatos, organizaciones sociales, de derechos humanos o que promuevan intereses de cualquier partido político o que garantice los derechos y garantías de

			partidos políticos de oposición así como datos relativos a la salud, a la vida sexual y los datos biométricos.
COLOMBIA	Ley 1266 de 2008	La normativa colombiana contempla que dato personal es: cualquier pieza de información vinculada a una o varias personas determinadas o determinables o que puedan asociarse con una persona natural o jurídica. Los datos impersonales no se sujetan al régimen de protección de datos de la presente ley. Cuando en la presente ley se haga referencia a un dato, se presume que se trata de uso personal. Los datos personales pueden ser públicos, semiprivados o privados; (Art. 3. e) Además, contempla la protección de estos datos y menciona que, salvo la información pública, no pueden ser accesibles los datos personales, por internet o por otros medios de divulgación masiva, salvo las predicciones de la ley.	No contempla una definición sobre datos personales sensible, pero reconoce la existencia de los datos privados, menciona que "Es el dato que por su naturaleza íntima o reservada sólo es relevante para el titular" (Art. 3. h).

	Ley 599 de 2000	El Código penal colombiano establece el delito de violación de datos personales y específicamente sostiene que: El que, sin estar facultado para ello, con provecho propio o de un tercero, obtenga, compile, sustraiga, ofrezca, venda, intercambie, envíe, compre, intercepte, divulgue, modifique o emplee códigos personales, datos personales contenidos en ficheros, archivos, bases de datos o medios semejantes, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1000 salarios mínimos legales mensuales vigentes. (Art. 269F)	No establece una conducta que ataña al uso de datos personales de carácter sensible, pero al igual que otras legislaciones contempla el delito de violación a la intimidad, imponiendo una sanción privativa de libertad de uno a tres años cuando la persona ilícitamente sustraiga, oculte, extravié, destruya, intercepte, controle o impida una comunicación privada dirigida a otra persona, o se entere indebidamente de su contenido, además contempla como agravante la revelación del contenido de la comunicación o empleo en provecho propio o ajeno o con perjuicio de otro e impone una pena de prisión de dos a cuatro años. (Ar. 192).
	Superintendencia de Industria y Comercio.	Este organismo actúa como la autoridad nacional de protección de datos, supervisando y garantizando el cumplimiento de la legislación relacionada con el tratamiento de datos personales, protege los derechos de los consumidores y administra el Sistema Nacional de Propiedad Industrial.	
	Ley Orgánica de protección de datos personales.	Dato que identifica o hace identificable a una persona natural, directa o indirectamente.	Datos relativos a etnia, identidad de género, identidad cultural, religión, ideología, filiación política, pasado judicial, condición migratoria, orientación sexual, salud,

E C U A D O R			datos biométricos, datos genéticos, y aquellos cuyo tratamiento indebido pueda dar origen a discriminación, atenten o puedan atentar contra los derechos y libertades fundamentales.
	Sentencia No. 2064-14-EP/21 de la Corte Constitucional del Ecuador	El concepto de dato personal es amplio ya que comprende cualquier tipo de dato que atañe a una persona, identificándola o, en su defecto, haciéndola identificable.	Engloba un análisis más amplio y menciona que las fotografías que revelan el ejercicio de la sexualidad pertenecen a la esfera más íntima del individuo, por ende son consideradas como datos personales de carácter sensible.
	Código Orgánico Integral Penal	Contempla como delito de violación a la intimidad a la conducta de acceder, interceptar, examinar, retener, grabar, reproducir, difundir o publicar sin el consentimiento del titular los datos personales, la sanción es pena privativa de libertad de uno a tres años (Art. 178).	No contempla la conducta del uso de datos personales de carácter sensible, tampoco incorpora como agravante en el delito de violación a la intimidad.
	Reglamento a la Ley Orgánica de Protección de Datos Personales.	Contempla cuestiones establecidas en la LOPDP y establece procedimientos específicos para el ejercicio de derechos como el acceso, rectificación, eliminación y oposición al tratamiento de datos personales, involucra conceptualizaciones más amplias sobre el tratamiento de datos personales, incluyendo la esfera doméstica. Se refiere a la protección de datos personales sin incluir definiciones sobre los mismos.	
	Ley Orgánica de Telecomunicaciones	Su enfoque principal es regular el sector de las telecomunicaciones, empero incluye disposiciones sobre la protección de datos personales en el contexto de las comunicaciones electrónicas, asegurando que los usuarios tengan derechos sobre sus datos en este ámbito.	

	Superintendencia de Protección de Datos Personales.	Es una entidad que regula y supervisa el adecuado tratamiento de los datos personales. Su objetivo es velar por el cumplimiento de los derechos fundamentales de conformidad con la legislación vigente.

Nota: Información extraída del ordenamiento jurídico de cada país.

Tratamiento de datos personales

El constante desarrollo tecnológico coloca al derecho en una utopía que no satisface las necesidades sociales frente al advenimiento de nuevas formas de comunicar e interactuar. Actualmente, las redes digitales almacenan un sin número de datos personales que provienen de usuarios que expresamente han dado su consentimiento para posteriores situaciones. Los datos personales al formar parte del derecho a la intimidad merecen una tutela judicial eficaz que soslaye aquellos preceptos ambiguos que no determinan lo esencial del derecho a la protección de estos datos. Puesto que con este avance surge la posibilidad de crear y recoger una gran cantidad de datos. Frente a esto, las normas jurídicas que se refieren a la protección y privacidad quedan desactualizadas.

La navegación en internet hace que los usuarios dejen rastros personales a la vanguardia de la red. Según Sánchez (2023) las redes sociales y aplicaciones solicitan el ingreso de datos personales como el rostro para un fin de entretenimiento, sin embargo, no existe la certeza del modo de tratamiento que le darán, la finalidad o el tiempo de resguardo (p. 3). Las instituciones públicas, privadas e individuos particulares de la sociedad civil pueden ejecutar un tratamiento a estos datos personales que se encuentran en sistemas informáticos y redes digitales. De la misma manera, Gil (2022) menciona que las organizaciones a través del uso de las tecnologías de la información recopilan, acceden, utilizan e intercambian datos personales con el objetivo de tomar decisiones y obtener beneficios empresariales y sociales (p. 25). Mediante la información obtenida en los sistemas informáticos las organizaciones pueden llegar a predecir el comportamiento e influir en él, situación que generalmente sucede de una manera no autorizada, unilateral y secreta.

El tratamiento es entendido como el conjunto de operaciones que conllevan a un procesamiento, conservación, registro o alteración de datos, que en la actualidad ha experimentado un crecimiento significativo, pues las nuevas tecnologías permiten la recogida e intercambio de datos en una gran escala. Las empresas públicas y privadas necesitan tratar la información personal de los individuos para la prestación de servicios. En este contexto se precisa que el tratamiento de datos personales a la luz de la Ley Orgánica de Protección de Datos Personales es:

> Cualquier operación o conjunto de operaciones realizadas sobre datos personales, ya sea por procedimientos técnicos de carácter automatizado, parcialmente automatizado o no automatizado, tales como: la recogida, recopilación, obtención, registro,

> organización, estructuración, conservación, custodia, adaptación, modificación, eliminación, indexación, extracción, consulta, elaboración, utilización, posesión, aprovechamiento, distribución, cesión, comunicación o transferencia, o cualquier otra forma de habilitación de acceso, cotejo, interconexión, limitación, supresión, destrucción y, en general, cualquier uso de datos personales. (Art. 4)

Esto quiere decir que implica una serie de actos como obtención, uso, divulgación, acceso, manejo, aprovechamiento, disposición, almacenamiento de datos personales. Engloba una gama de operaciones efectuadas sobre datos vinculados a una persona. Además, este tratamiento puede ser automatizado o no automatizado y esto depende de la fuente de la que se obtienen los datos.

Por ejemplo, en la actualidad se entiende que algunos datos se encuentran digitalizados, es decir, han sido cargados en los sistemas de información. En este caso, se estaría frente a un tratamiento automatizado de datos. Bajo este precepto, el Gobierno Neerlandés en la sentencia 6.11.2003 Asunto C-101/01 señala que

> la inclusión de datos personales en una página web se realiza con ayuda de un ordenador y de un servidor, lo que constituye una característica importante de la automatización, de modo que debe estimarse que dichos datos son objeto de un tratamiento automatizado. (párr. 22)

Además, el Tribunal de Justicia de la Unión Europea sostiene que hacer referencia en una página web a diversas personas e identificarlas a través de datos personales es considerado un tratamiento total o parcialmente automatizado de datos personales (párr. 27). En este sentido, el objeto del tratamiento de datos personales puede variar dependiendo del contexto en el que se lo realiza, medio que se utiliza y la persona o personas que lo ejecutan. Se debe aclarar que para Nieves y Ponjuan (2021) lo esencial del tratamiento de datos es que éste cumpla con las normas establecida y que contribuya a la alfabetización digital de los individuos, de manera que se les informe los derechos que el titular tiene sobre sus datos y se mantenga la calidad de éstos.

Gil (2022) señala que el tratamiento de los datos personales que se aplican en las tecnologías big data es un proceso que se refleja en tres fases:

1. **Recolección de datos**: El origen de los datos es muy variado, y éstos pueden ser estructurados y no estructurados, los primeros se refieren a aquellos que son ordenados y

fácilmente analizables de forma automatizada, mientras que los no estructurados son los que no cuentan con un formato definido y son difícilmente analizables. Los datos provienen sea directamente de la persona a través de formularios, o mediante sensores que recogen datos como el ritmo cardiaco, información de procesos, localización, etc. Así también, los datos son recogidos de transacciones de una compañía con cada cliente. Por otro lado, la fuente de la que pueden ser extraídos los datos son las **redes sociales e internet,** que en la actualidad son las herramientas más utilizadas por la sociedad que provoca el acceso incalculable a los datos personales.

2. **Análisis de los datos:** Se realiza la búsqueda de correlaciones y patrones, diseño de nuevo conocimiento y de un modelo algorítmico.

3. **Aplicación del modelo:** Se aplica el modelo sobre los datos de una persona concreta. Este tratamiento permite la elaboración de perfiles del titular de los datos y por ende la personalización de servicios. Esta fase conlleva a poner en riesgo la protección de datos personales.

El responsable del tratamiento según la legislación colombiana es toda persona sea natural o jurídica, pública o privada que a través de sí mismo o en asociación con otros decida sobre la base de datos o el tratamiento. La legislación ecuatoriana engloba el mismo precepto jurídico respecto del responsable. Es importante mencionar que el manejo de datos personales debe ajustarse a los presupuestos establecidos en la normativa. Por ende, los datos deben ser tratados de una manera lícita, leal y transparente en relación con el titular.

En concordancia con esto, es necesario el apego irrestricto a los principios establecidos jurisprudencial, legal y doctrinariamente. La legislación ecuatoriana a través de la Ley Orgánica de Protección de Datos Personales establece que los principios a los que debe regularse el tratamiento de datos personales son los contemplados en el artículo 10, sin que ello signifique la inobservancia de los reconocidos constitucionalmente.

- **Lealtad**: Permite que el titular de los datos tenga conocimiento sobre la recolección, utilización y la forma en que van a ser tratados los datos que les conciernen. Aclara también que bajo ningún precepto los datos pueden ser tratados por medios o para fines ilícitos o desleales. Por su parte, **Rodríguez (2019**) explica que el RGPD busca conceder al ciudadano el poder de supervisar y controlar las circunstancias que engloban el uso y tratamiento de sus datos personales, bajo el fundamento de que éste

es el principal actor como titular de los datos y por ello, este instrumento jurídico internacional reconoce los principios de licitud, lealtad y transparencia (pp.27-28).

- **Transparencia:** La información sobre lo concerniente al tratamiento de datos personales debe tener fácil acceso, comprensión y aplicando un lenguaje sencillo y claro. De manera que el responsable es el encargado de implementar las medidas necesarias para facilitar al titular las cuestiones que derivan del tratamiento. Por lo cual, el RGPD describe en su considerando 58 que la información concerniente al tratamiento debe facilitarse cuando el interesado lo solicite sea de forma verbal, electrónica o por cualquier otro medio. En este contexto, a través de este principio se garantiza que el interesado pueda consentir el tratamiento de sus datos con el conocimiento pleno
- **Finalidad:** En el ordenamiento jurídico europeo este principio también es denominado como limitación de la finalidad, que acorde con **Hernández (2023)** tiene por objeto que los datos personales sean recogidos con fines determinados, explícitos y legítimos (p. 264). Es importante que el titular tenga el pleno conocimiento de qué van a realizar con sus datos, saber y facultar para un fin determinado, sin que intermedie cuestiones de tratamiento ulteriores de manera incompatible con los fines iniciales. La importancia de este principio radica en el hecho de determinar la legitimidad del tratamiento de los datos personales. Es así como **Roldán (2021**) manifiesta que "Una finalidad legítima es la causa de justificación del tratamiento de datos personales, la cual se debe ajustar a los preceptos establecidos en cada ordenamiento jurídico" (p.185).
- **Pertinencia y minimización de datos personales:** Hernández (2023) explica que este principio atañe a que los datos deben ser adecuados, pertinentes y limitados a lo necesario (p.265). No puede el responsable del tratamiento de los datos solicitar información que nada tenga que ver con la finalidad a la que se pretende llegar, de ser así se estaría violando derechos como la privacidad e intimidad del individuo.
- **Proporcionalidad del tratamiento:** Surge debido a la necesidad de ponderar los intereses que devengan del tratamiento de los datos personales. En este sentido Cazurro (2020) piensa que es necesario la aplicación de una prueba de Proporcionalidad con la finalidad de determinar a existencia o no proporcionalidad entre los medios empleados en el tratamiento y el fin que se persigue (p. 79). Así también, se refiere a la proporcionalidad entre lo individual y el interés general, cuando el tratamiento de los datos personales debería ser necesario para satisfacer necesidades sociales.

- **Confidencialidad:** Se garantiza una seguridad eficaz a los datos personales, pretende evitar la pérdida, destrucción o daño accidental de los datos recogidos.
- **Calidad y exactitud:** Este principio busca garantizar que los datos hayan sido recopilados de manera precisa y establecer la responsabilidad a los encargados del tratamiento de datos personales en caso de inexactitud.
- **Conservación:** Incluye presupuestos temporales, es decir que los datos personales no pueden estar almacenados de manera indefinida, más bien que una vez cumplido el propósito estos deben ser eliminados o anonimizados.
- **Seguridad de datos personales:** López y Leal (2018) aluden que este principio busca brindar la certeza de que las entidades que tratan los datos personales doten medidas razonables para la seguridad física, técnica y organizacional y así salvaguardad la integridad de los datos (p. 107).
- **Responsabilidad proactiva y demostrada:** Es fundamental que los responsables del tratamiento de datos personales implementen medidas adecuadas y capacitaciones continuas y efectuar una auditoría para llevar el registro del manejo de datos.
- **Aplicación favorable al titular:** Tiene su fundamento en la CRE (2018), ya que prevé que los derechos deben aplicarse en el sentido que más favorezca su efectivo cumplimiento (Art. 11.5). De modo que, todo tratamiento debe garantizar el efectivo goce de los derechos del titular, respetar su autonomía y su autocontrol sobre sus datos personales.
- **Independencia del control:** Según la LOPDP (2021) este principio alude al efectivo ejercicio del derecho a la protección de los datos personales y la responsabilidad que tiene el Estado y la entidad correspondiente para ejercer un control independiente, imparcial y autónomo y efectuar acciones de prevención, investigación y sanción conforme lo establezca el ordenamiento jurídico (Art. 10. m)

Consentimiento del titular de los datos personales para el tratamiento.

El tratamiento de los datos personales conforme el RGPD de la Unión Europea se legitima a través de 6 mecanismos: consentimiento del titular; cuando el titular es parte de la relación contractual dentro de la cual es necesario procesar sus datos; por una obligación legal que se exige el responsable del tratamiento; bajo la necesidad de protección de intereses vitales del titular o terceros; por el interés público o ejercicio de poderes públicos; cuando existe intereses legítimos perseguidos por el responsable del tratamiento o terceros (Art.6). Sin embargo,

Trujillo citado por Roldán (2021) establece que, de estos presupuestos, el consentimiento constituye la regla general para el tratamiento de los datos (p. 187).

La protección de los datos personales surge debido a la necesidad de garantizar los derechos a la intimidad y privacidad de las personas. Por ello, el consentimiento ha sido considerado como el instrumento que permite legitimar el tratamiento de datos personales y evitar su uso y abuso. Conforme Roldán (2021) el consentimiento es la manifestación *libre*, sin coerción alguna y sin que intermedie vicios del consentimiento; *específica*, en cuanto al conocimiento sobre la finalidad concreta del tratamiento; *inequívoca*, sin tela de duda sobre la voluntad de consentir el tratamiento de sus datos; *e informada*, con respecto a conocer y entender los hechos e implicaciones que derivan de su prestación, este requisito se relaciona con la noción del control y autodeterminación; de la voluntad del titular de los datos (pp.184-185). Estos estándares deben cumplirse a fin de evitar una transgresión al derecho de protección de datos personales.

En esta misma línea de pensamiento Rebollo y Serrano (2019) sostienen que el consentimiento se traduce a la facultad de la libertad que posee el individuo para decidir respecto de sus datos (p. 237). En el mundo digital, esta libertad busca que el individuo extienda su capacidad de decisión para proteger sus derechos en el espacio virtual. El consentimiento debe ser dado por el titular mediante un acto afirmativo sea de forma escrita, verbal o a través de otros medios que se verifique la expresión de la voluntad del titular para el tratamiento de sus datos personales.

En el contexto actual del uso de las redes sociales el consentimiento para tratar los datos que se encuentran cargados en estas plataformas digitales debe entenderse de una forma más amplia. Puesto que en estas redes digitales se conocen personas de todo el mundo, se colabora y coopera, se crea y se comparte contenido, información, datos, entre otros. Además, mediante la utilización de este medio se logra efectuar una interacción con otros usuarios, amigos y familiares sin importar la distancia, se crean relaciones personales y comúnmente se comparten fotos, videos, música, libros, chateos, etc. De tal forma que, Barriuso (2009) deja sentada la idea de que existen grupos de interés o poder que atesoran la información contenida en las redes sociales, entre los cuales están los datos de carácter personal (p. 304).

Por ello, para establecer que un usuario de la red social ha otorgado el consentimiento expreso para que sus datos sean tratados De Miguel (2023) menciona que existen requisitos para determinar tal situación. Entre ellos destaca, por un lado, la exigencia de que los usuarios tengan la facultad de negarse individualmente a otorgar su consentimiento a operaciones

particulares de tratamiento de datos, sin que esto signifique la renuncia íntegra a la utilización del servicio ofrecido en la red social en línea y, por otro lado, la facultad para que el usuario pueda dar su consentimiento por separado, en relación con su comportamiento dentro de la red social y sus otros datos (p. 11). Es importante aclarar que este presupuesto jurídico engloba lo que respecta del tratamiento de datos personales por parte de la empresa que ofrece la red social, que sin embargo serviría como base para la regulación del tratamiento que deviene de los particulares.

Derecho a la protección de datos personales, privacidad e intimidad en el contexto digital.

Para comenzar es importante señalar que según Conde (2006) la doctrina ha señalado tres generaciones de derechos humanos.

- **Primera generación:** Aquellos derechos relacionados a las libertades individuales frente a los poderes públicos, que exigen una observancia y tutela a los derechos individuales.
- **Segunda generación:** Engloba a los derechos económicos, sociales y culturales que necesita de una política para su ejercicio eficaz.
- **Tercera generación:** Aparece la libertad informática como derecho que engloba la identidad informática en base a las garantías de acceso y control de las informaciones contenidas en los bancos de datos. Es aquí en dónde se sitúa la generación de las leyes sobre la protección de datos personales.

Debido a la revolución informática que ha sufrido la sociedad, los datos personales que eran considerados de una esfera privada se han colocado en escrutinio público como resultado del uso de redes sociales y buscadores digitales. En la actualidad, un dato considerado privado puede trascender fronteras con solo cargarlos en una página social, pues estas redes permiten la interacción social sin control de la difusión de información personal del usuario. A criterio de **Cornejo y Sánchez (2023)** las comunicaciones personales deben ser privadas y confidenciales con la finalidad de garantizar el pleno goce de los derechos a la dignidad, autonomía y libertad de las personas en un mundo cada vez más digitalizado (p. 999).

De esta manera, el tratamiento de los datos personales debe efectuarse en apego a lo que determina la normativa nacional e internacional y garantizar el efectivo goce de los derechos vinculados a la protección de datos personales. Es así que el RGPD estatuye en su considerando 85 que es necesario tomar las medidas adecuadas para evitar violaciones de la seguridad de los

datos personales que pueden desembocar en daños y perjuicios físicos, materiales o inmateriales para los individuos, entre los que detalla, la pérdida de control sobre sus datos personales, discriminación, usurpación de identidad, pérdida financiera, entre otros.

Tomando en cuenta que la privacidad se vincula con el derecho a la libertad y a la dignidad de las personas se puede mencionar que el uso indebido de los datos personales genera una transgresión a la dignidad humana, ya que coloca al titular en situaciones de riesgo dentro del cual no se puede establecer el daño que se genera a éstos. Según Sánchez (2023) la dignidad implica un derecho inherente a las personas y reconocido a nivel constitucional cuyo valor jurídico revela el hecho de que toda autoridad e incluso los particulares tienen que respetar (p. 3). Así también conforme la Constitución Política de los Estados Unidos Mexicanos este derecho implica el respeto a la persona a ser tratada como tal y no como objeto, a no ser humillada, degradada, envilecida o cosificada.

En la actualidad, el ordenamiento jurídico busca proteger la privacidad de los individuos frente a la constante difusión de sus datos, ya que este presupuesto favorece a la autonomía y al desarrollo integral del ser humano. La privacidad debe ser vista como un derecho que protege las múltiples dimensiones los individuos. En palabras de Hernández (2023) los derechos que configuran la privacidad son: Derecho a la intimidad personal y familiar; Derecho a la inviolabilidad del domicilio; Derecho al secreto de las comunicaciones; Derecho a la protección de datos personales; Derechos digitales de intimidad y protección de datos; Derecho al respeto a la vida privada y familiar (p. 236), mismos que se encuentran en constante evolución. Adquiere valor jurídico toda vez que es reconocida por los instrumentos jurídicos nacionales e internacionales. Es así como la Declaración Universal de los Derechos Humanos establece que:

> 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. (Art. 12)

En este sentido, Novoa Monreal citado por la Corte Constitucional de Colombia en la sentencia No. SU-089/95 reconoce que las actividades, situaciones y fenómenos que forman parte de la vida privada son:

- Ideas, creencias religiosas, filosóficas, mágicas políticas que el ser humano ha decidido adoptar del conocimiento externo.
- Situaciones que tienen que ver con su vida amorosa y sexual

- Aspectos que no son conocidos por extraños, configurados en una índole embarazosa para el individuo o el grupo.
- Defectos físicos o psíquicos.
- Comportamiento fuera de lo común que su conocimiento podría provocar críticas o descrédito a aquel.
- Afectaciones de salud.
- Cuestiones relacionadas con la vida pasada del sujeto que pueda ser sujeto de burlas.
- Orígenes familiares que provoquen discriminación.
- Cumplimiento de funciones fisiológicas de excreción y hechos que se relacionen al propio cuerpo.
- Momentos penosos para el individuo.
- En general todas las situaciones que en conocimiento de los demás provoquen cualquier acto de discriminación o rechazo del individuo.

Debido a esto, debe considerarse que la privacidad tiene una doble vertiente, jurídico y moral. El valor jurídico es vista desde la positivización de los derechos a la intimidad y protección de datos personales, es decir el reconocimiento jurídico en la normativa legal. Por su parte, el aspecto moral tiene una función crítica y de presión social sobre estos derechos. Estas dos vertientes deben configurarse de tal forma que contribuyan al pleno desarrollo social en lo que atañe a los datos personales y su difusión. Entonces, se habla de un consenso legal y social. Así también, se debe tener en cuenta al referirse a la vida privada hay que englobar dos aspectos sustanciales, por un lado, la vida interior que integran aquellos hechos de conciencia, pensamiento, fantasía, sentimiento y, por otro lado, aquella parte de la vida que se exterioriza al ámbito público, pero que no por ello deja de ser privado.

En este contexto, gracias a la creciente evolución tecnológica comienza la necesidad de proteger los datos personales del individuo de la sociedad civil que se difunden en espacios informáticos, razón por la cual este derecho es considerado relativamente moderno y se desarrolla a la par de la evolución tecnológica. El límite de este derecho depende del tipo de datos que se ha utilizado en el tratamiento Bajo este precepto Conde (2006) sostiene que “los bienes jurídicos más susceptibles de ser lesionados o puestos en peligro por el uso de las nuevas tecnologías es la intimidad” (p. 20). Esta protección jurídica implica establecer límites frente a la utilización de la informática y las comunicaciones para garantizar el ejercicio pleno de los derechos. El derecho a la intimidad inherente al ser humano busca el rechazo a la intromisión no consentida en la vida privada. La esfera íntima debe ser considerada como aquel ámbito

personal de cada individuo, que lejos del mundo exterior permite que su personalidad se desarrolle y evolucione bajo su ideal.

La intimidad es para Conde (2006) el conjunto de sentimientos, pensamientos e inclinaciones más internas del ser humano, tales como la ideología, religión o creencias, vida sexual, problemas de salud u otras cuestiones que se desea mantener en secreto (p. 25). Se refiere al ámbito propio y reservado del individuo frente a los demás sean estos públicos o privados, obligándolos a abstenerse y evitar la intromisión a la esfera íntima. Sin embargo, no todos los datos personales ni toda la vida puede ser considerada íntima, pero la vida íntima debe siempre ser privada. Para Hernández (2023) la intimidad es la dimensión más individual del ser humano (p. 242). Así, es importante considerar que este derecho es una dimensión que se enmarca en la privacidad.

La naturaleza de este derecho tiene una triple concepción, derecho fundamental, derecho de la personalidad y derecho a la privacidad y se vincula directamente con el respeto a la dignidad del ser humano. No se puede hablar de la intimidad sin dejar de lado los derechos conexos que integran la privacidad. Vale mencionar que en la CRE en su numeral 20 del artículo 66 se reconoce el derecho a la intimidad personal y familiar.

La intimidad ha evolucionado debido a dos factores recientes que han aparecido en la vida de los seres humanos. Las nuevas tecnologías que brindan la posibilidad de mantenerse conectados con otros individuos en tiempo real, y, por otro lado, el advenimiento de las redes sociales que abre la posibilidad de compartir información personal para conocer gente a través de este medio. En tal sentido, Bautista (2015) se refiere a las redes sociales como aquel mecanismo de información e interacción que ha cambiado el panorama del derecho a la intimidad personal (p. 16). Este pensamiento cobra sentido debido a que gran parte de la población que utiliza las redes sociales comprenden jóvenes, que con frecuencia agregan fotos propias de momentos íntimos, dejando así un rastro documental en la red. Estos datos pueden ser utilizados por terceros.

La Corte Constitucional de Colombia en la Sentencia SU-089 de 1995 estableció que los aspectos que integran este derecho son aquellos

> asuntos circunscritos a las relaciones familiares de la persona, sus costumbres y prácticas sexuales, su salud, su domicilio, sus comunicaciones personales, los espacios limitados y legales para la utilización de datos a nivel informático, las creencias religiosas, los secretos profesionales y en general todo comportamiento del sujeto que

no es conocido por los extraños y que de ser conocido originaría críticas o desmejoraría la apreciación que éstos tienen de aquel.

Se debe tomar en consideración que en las redes sociales mayormente se comparte imágenes propias como una representación externa del usuario. En consecuencia, del derecho a la intimidad se deriva el derecho a la propia imagen que le otorga a la persona la posibilidad de decisión sobre el modo de empleo de su imagen o la oposición a que sea utilizada con fines de lucro sin su consentimiento. Hernández (2009) alude que la persona es la única dueña de su fotografía o imagen, por ello su divulgación sin su consentimiento tiene consecuencias legales debido a que atenta contra derechos reconocidos a nivel constitucional e internacional (p. 90). Pese a aquello, es preciso resaltar que el autor menciona que este derecho tiene sus límites en distintos aspectos sociales.

1. **Notoriedad:** Constituida por aquellos actos o comportamientos del ser humano que no está en la esfera de lo común. Es decir, este presupuesto jurídico se refleja a través de los actos, bienes o acontecimientos extraordinarios en los que se ha desempeñado el individuo.

2. **Persona de carácter público:** Implica que las fotografías de una figura pública pueden ser utilizadas sin consecuencias jurídicas, pero se faculta una vida íntima cuyo objeto es mantener privado los aspectos más esenciales de su vida.

3. **Necesidad de justicia o de policía:** Un ejemplo que señala el autor es la inclusión de fotos en publicaciones en periódicos o en la televisión de personas buscadas para ser procesadas por un delito que hayan cometido.

4. **Interés público:** Faculta la posibilidad de la reproducción de las fotografías captadas en lugares públicos. El interés público deberá ser limitado a criterio del juzgador.

Ahora bien, cuando se refiere a la privacidad e intimidad surge la necesidad de hablar sobre el derecho a la protección de datos personales como un derecho autónomo. De acuerdo con Hernández (2023) este derecho si bien protege aquellos datos personales relativos a la vida privada y familiar del individuo, va más allá e incluye aquellos datos respecto de cualquier actividad desarrollada por el individuo. Es así como el autor explica que el tratamiento de datos personales no siempre llega afectar la vida privada (p.257). De tal forma que es necesario saber el alcance de la vida privada y los límites de la protección de datos a fin de establecer cuándo el tratamiento de datos personales constituye una afectación a la vida privada.

En la Guía sobre el artículo 8 del Convenio Europeo de Derechos Humanos se establece que la vida privada se agrupa en tres categorías:

- **Integridad física, psicológica y moral:** víctimas de violencia, derechos reproductivos desde la óptica de poder decidir la maternidad, tratamiento médico forzado y actos médicos obligatorios, enfermedades mentales, atención y tratamiento médico, aspectos sobre la forma de terminar la vida, discapacidad, orientación y vida sexual y actividades profesionales o comerciales.
- **Imagen y protección de fotografías:** Publicación de fotos, imágenes y artículos. Reputación, difamación, protección de datos, acceso a la información personal, información sobre el estado de salud, creación o recogida de datos por cuerpos de seguridad, vigilancia policial, vida privada en prisión.
- **Identidad y autonomía:** Desarrollo personal y autonomía, información sobre los propios orígenes, convicciones religiosas y filosóficas, apariencia, documento de identidad, identidad sexual y ética, situación marital y parental (pp. 19- 49).

En este punto, vale aclarar que todo lo íntimo termina siendo privado, empero no todo lo privado puede ser tratado desde la esfera de la intimidad. Sin embargo, todos los datos personales que formen parte de la esfera privada deben ser protegidos y se debe garantizar a las personas el control y disposición sobre su propia información. López y Leal (2018) establecen que el contenido del derecho a la protección de datos está compuesto por la posibilidad de acceder, rectificar, cancelar y oponerse a las bases de datos que se encuentran en posesión de particulares, cuando el tratamiento que se le otorgue sea diferente al de la finalidad inicial (p. 113).

En esta misma línea hay que señalar que este derecho surge como un mecanismo jurídico tendiente a proteger el derecho a la vida privada de las personas en la era digital. Por esta razón, los objetivos principales son, definir los datos personales, determinar el responsable del tratamiento, regular lo que respecta al tratamiento y la transferencia a nivel internacional. El surgimiento de este derecho se encamina a garantizar el efectivo cumplimiento del derecho a la seguridad jurídica comprendido en el artículo 82 de la Constitución ecuatoriana en el que prescribe que necesario la “existencia de normas jurídicas previas, claras, públicas y aplicadas por las autoridades competentes” (Art. 82).

Contenido sexual en redes digitales

López y Müller (2019) establecen que contenido sexual es aquel material erótico o pornográfico, se trata de fotos del cuerpo desnudo o de sus partes, pueden ser incluso videos de tipo sexual que filman los protagonistas y se los envían a sus pares, sean estos novios, amantes, amigos, conocidos o pareja (p. 68). Entonces, este contenido incluye representaciones explícitas o implícitas de actos sexuales, desnudez, comportamiento sugestivo o temas eróticos. Puede manifestarse en diversas formas, tales como textos, imágenes, videos, sonidos, o incluso a través de descripciones verbales. Se debe tomar en cuenta que este tipo de contenido en ocasiones puede generar un lucro para quien lo utilice, difunda o venda sin el consentimiento de su titular.

La difusión de este contenido es vista como una afectación del derecho a la intimidad de la persona, debido a que se expone públicamente una faceta muy privada del individuo. A criterio de Méndez y Cornejo (2023) los videos o imágenes de carácter sexual se comprende como una divulgación pública de hechos privados y es considerada una de las formas que más afecta a los derechos de protección de datos personales, intimidad y vida privada (p. 223). Toda vez que esa información expone públicamente a la persona, su vida privada y su vida sexual. Generalmente este suceso ocurre en los grupos adolescentes y es considerado como un delito de género, ya que en varias ocasiones esta acción es ejecutada por motivos misóginos y de interiorización de la mujer, podría entonces considerarse como una forma de violencia de género que sufren las mujeres.

Añadido a esto, la constante evolución social y tecnológica ha traído consigo la existencia de una manipulación en las fotografías, textos, audios o vídeos cuyo fin es variado. En este contexto la Inteligencia Artificial juega un papel fundamental para transformar las fotografías, imágenes, videos, audios, entre otros, que se encuentran cargados en una red digital. García (2021) expone que, herramientas como el denominado *deepfake* permiten recrear representaciones audiovisuales que simulan la apariencia y el habla de las personas, hecho que incrementa el riesgo de la suplantación de identidad (p. 105). Estas herramientas que ofrece la tecnología hacen que imágenes, video y audios falsos tengan una apariencia real. Esta manipulación tecnológica facilita la creación de videos o imágenes hiperrealistas, intercambios de rostros y otros actos que atentan contra la privacidad de la víctima y que dejan poco rastro.

Soler (2023) sostiene que la manipulación de fotografías, textos, audios o videos tiene múltiples finalidades y aunque no es considerado un fenómeno nuevo, su proceso de realización si lo es,

pues en la antigüedad para ejecutar este acto se necesitaba un ejercicio manual, que ahora se genera a través de las tecnologías (p. 495). Es decir, puede ser visto como una innovación del aprendizaje cuyo núcleo se lo encuentra en el engaño y la capacidad o intención de faltar a la verdad. Siendo indispensable en esta actividad el uso de un conjunto de datos faciales diversos y extensos para manipular en contenidos visuales o audiovisuales. Por ello, Heidari et al. (2023) manifiesta que es fundamental comprender que los atributos faciales, visuales o vocales distintivos que se utilizan constituyen información personal y, por tanto, datos personales que se refieren a un individuo que identificado o identificable. Dicho de otro modo, atenta contra la identidad de una persona al manipular sus datos con diferentes finalidades, así como también ejecuta un tratamiento sobre los datos personales del individuo. Es esencial considerar que conforme, O´Halloran (2021) citado por Ramos (2024) este avance tecnológico permite la creación de imágenes y videos alterados que representan a individuos en contextos inapropiados, pero que principalmente este atentado se dirige hacia las mujeres (p. 368). Esto debido a las cuestiones éticas que se derivan de la obscenidad sobre las mujeres.

Ramos (2024) destaca un hecho ocurrido en México, en dónde un estudiante de educación superior fue acusado por poseer material pornográfico con aproximadamente 160 000 imágenes íntimas, videos y fotos, tanto reales como manipuladas de alrededor de mil mujeres (p. 375). Este caso refleja el cometimiento de delitos a través de la utilización de la tecnología, en la que se deja de manifiesto que el grupo más vulnerable en este tipo de situaciones son las mujeres. Similar aspecto demuestra BBC News (2024) cuando detalla el acontecimiento ocurrido en España, en el cual expone que alrededor de 28 niñas se han convertido en víctimas de imágenes de desnudos generados por la IA y que son distribuidos entre sus pares, estas imágenes que fueron obtenidas de los perfiles de redes sociales fueron manipuladas y colocadas en situaciones explícitas, dejando varias afectaciones psicológicas a las víctimas.

El *deepfake* tiene diversas finalidades entre ellas Soler (2023) destaca el delito de suplantación de identidad desde una perspectiva de práctica de ciberacoso, que consiste en "falsificaciones fraudulentas de la identidad realizadas por hombres maltratadores tanto respecto a su propia imagen como a partir del reemplazo de la identidad de las mujeres" (p. 502). Además, Pérez y Reyes (2010) coinciden en este planteamiento y añaden que en lo que respecta a la suplantación de identidad de las mujeres sucede a través de la creación de perfiles o espacios falsos de las víctimas en el que se comparte videos íntimos y/o ofertas sexuales explícitas (p. 19). Con esto queda en evidencia que la suplantación de identidad con contenido sexual afecta

significativamente a las mujeres, quienes son más vulnerables en el contexto digital, uso y tratamiento de sus datos personales.

Suplantación de identidad

En un inicio es importante determinar que la identidad constituye un conjunto de datos o referencias que permiten diferenciar a un individuo de otro en un colectivo. Así, Hernández (2019) estima que las particularidades a tomar en cuenta para determinar la identidad son su nacionalidad, fecha de nacimiento, número de cedula de ciudadanía, etnia, tipo de sangre, datos informativos contenidos en instituciones públicas, características físicas, rasgos particulares, color de piel y ojos, huellas dactilares, idioma (p. 30). Cabe señalar que los aspectos de una persona son inherentes a esta, pero también existen aquellos que son objeto de una elección propia, como el estilo, orientación sexual, entre otros. Así también, debe entenderse que este presupuesto de identidad personal es un Derecho que da lugar a efectuar una serie de capacidades.

En el contexto actual, no se puede limitar el concepto de identidad únicamente a los aspectos físicos tradicionales, la tecnología ha permitido que aparezca una identidad digital que conforme lo menciona Llaneza (2021) es aquella información sobre una entidad utilizada por los sistemas informáticos, cuya finalidad es representar a un agente externo, sea este una persona, organización o dispositivo (p. 69). Dicho de otro modo, es un conjunto de datos o atributos asociados a un identificador. En este sentido, se habla de un traspaso de una identidad legal al mundo online en el cual un individuo puede representarse socialmente en un contexto virtual a través del uso de medios tecnológicos. Esta identidad puede incluir, nombre, fotos, entre otros.

El primer instrumento jurídico internacional en reconocer el derecho a la identidad fue la Convención sobre los Derechos del Niño (CDN). Para el año 1998 la Constitución política de la República del Ecuador en el artículo 49 reconocía que los niños y adolescentes tenía entre otros derechos, el de identidad que incluía nombre y ciudadanía. La actual Constitución ecuatoriana reconoce que las personas tienen derecho a la identidad personal o colectiva que incluye entre otros el tener nombre y apellido, debidamente registrados, entre otros aspectos, derecho que forma parte del catálogo de derechos de libertad (Art. 66. 28).

Ahora bien, la suplantación de identidad como delito informático es entendido para Arévalo (2022) como el engaño ejercido por una tercera persona con la finalidad de obtener información personal mediante el uso de correos electrónicos que pretenden ser legales y con el uso de

nombres afines (P. 15). El fin de este acto es robar información confidencial de los usuarios. En esta misma línea Parada y Errecaborde (2018) mencionan que el robo o usurpación de la identidad es el acto mediante el cual los delincuentes utilizan datos personales de terceros con la finalidad de hacerse pasar por el titular (p. 44). Este delito se caracteriza por la apropiación de la identidad de una persona, mediante la apropiación del DNI o el uso de datos personales obtenidos de diferentes fuentes (redes sociales).

Es esencial tener en cuenta que en la era digital este delito es ejecutado de diversas formas y a través de diferentes medios con la utilización de la ingeniería social. Es así como Fernández y Martínez (2020) mencionan que las diferentes formas de consecución de este delito son denominados de la siguiente manera: se conoce como smishing cuando se hace a través de SMS), linking (permite la utilización ilícita de hipervínculos), inlining (permite la utilización ilícita de imágenes), deep linking (permite ingresos por publicidad), framing (permite el acceso o reproducción en pantalla reducida), caching (permite la realización de una copia de una página web), mirroring (permite la creación de sitios idénticos a otros existentes), soliing (permite la copia en diferentes ordenadores de un mismo usuario, empresa o institución, de un soware del que se posee una sola licencia de uso), downloading (permite descargar en un ordenador una obra digitalizada), uploading (permite la puesta a disposición de terceros de los archivos digitales para la posterior descarga por otros usuarios), pygginbaking (permite el acceso a áreas restringidas dentro de los sistemas o dispositivos periféricos como consecuencia de puertas abiertas o dispositivos desconectados), data leakcage (permite la sustracción de información confidencial almacenada en un sistema desde un punto remoto), impersonation (permite la utilización de claves ajenas de acceso, llaves o tarjetas magnéticas), wiretapping (permite interferir las líneas de transmisión de datos, recuperando la información que circula por ella), carding (permite la manipulación de tarjetas de crédito pertenecientes a otras personas con la finalidad de cometer fraudes) (p. 19).

Esto quiere decir que la forma en la que se comete el delito depende de la finalidad a la que el ciberdelincuente quiere llegar en la red. Así también, los medios utilizados para extraer los datos personales son diferentes en cada caso. Sin embargo, todos llegan a apropiarse indebidamente de la identidad del sujeto y atentar contra su integridad. Es importante analizar este tipo penal bajo los presupuestos de la teoría del delito.

Teoría del delito

El delito constituye una conducta humana que reúne los elementos de tipicidad, antijuridicidad y culpabilidad, denominados por la doctrina como categorías dogmáticas del delito. Por ello, la teoría del delito se configura como la manifestación de la dogmática penal cuya finalidad es esquematizar estos elementos. Conforme Pedreira y Escudero (2023) busca generar certeza y seguridad jurídica a la hora de emplear el poder punitivo del Estado, evitando las posibles arbitrariedades de los operadores de justicia (p. 23). Es decir, cristaliza el principio de legalidad en el Derecho Penal, asegura el cumplimiento del ordenamiento jurídico y garantiza el principio de mínima intervención penal.

En este sentido, Graf (2018) sostiene que el delito es el incumplimiento de lo previsto en el ordenamiento jurídico que como consecuencia tiene una sanción penal. Así también, el Código Orgánico Integral Penal (COIP) establece que delito es la conducta típica, antijurídica y culpable (Art. 18). De tal forma que para Zaffaroni et al (1998) la teoría del delito se asemeja a un sistema de filtros que permite regular el poder punitivo del Estado. Se puede decir entonces que busca que el procesado no sea juzgado de forma intolerable e irracional, pues adquiere una función práctica para analizar el delito en toda su dimensión y caracteres. Es así que cuando una persona atenta significativamente sobre un bien jurídico tutelado por el Estado, es importante ejecutar el análisis bajo esta concepción, puesto que no toda acción debe ser juzgada de forma automática e igual. Cada acto delictivo se configura de forma diferente, y por ende se lo juzga conforme el respectivo análisis de las características propias del delito, esto es la tipicidad, antijuridicidad y culpabilidad.

En la misma línea de pensamiento Plascencia (2004) menciona que la teoría del delito tiene como objetivo analizar y estudiar los componentes jurídicos de la punibilidad como resultado de un comportamiento humano sea a través de una acción o una omisión que configure un delito (p. 15). Siendo así que todo aquello cuya consecuencia sea la aplicación de una pena o medida de seguridad es objeto de análisis de este sistema de filtros de la teoría del delito. También se analiza dentro de este presupuesto jurídico los comportamientos humanos que afecten bienes jurídicos protegidos por el ordenamiento jurídico pero que su conducta sea justificada o no reprochable y, por tanto, no punible.

A criterio de D. Juan Bustos Ramírez citado por **Zambrano (2023),** las categorías dogmáticas del delito son:

> tipicidad (como) adecuación de un hecho determinado con la descripción que de él hace un tipo legal; la antijuridicidad, la contravención de ese típico con todo el ordenamiento jurídico, y, la culpabilidad, el reproche porque el sujeto pudo actuar de otro modo, es decir, conforme al orden jurídico. (p. 22)

Conducta

El primer elemento del delito es la acción, que según Benavente (2023) se considera como la actividad voluntaria que ejerce el individuo, es decir es el resultado expresado en el mundo exterior (p. 47). Para Mila (2023) la acción como primer filtro de la teoría del delito está relacionado con los principios de; acto, por cuanto se prevé que se le puede perseguir penalmente a los individuos que han ejecutado actos exteriorizados, que dejan de lado meras suposiciones o pensamientos; legalidad, ya que estas conductas deben encontrarse prescritas en el ordenamiento jurídico como delito; culpabilidad, que considera los aspectos subjetivos y; voluntariedad con la que ha efectuado dicha acción.

Es importante mencionar que, la acción por sí sola no se configura como delito, sino que este comportamiento debe ser relevante para el Derecho Penal, debe modificar el mundo exterior y afectar significativamente a un bien jurídico protegido por la normativa legal del Estado. Siendo así que el legislador a previsto en el COIP que, las conductas penalmente relevantes son acciones u omisiones que tienen como resultado daños lesivos, descriptibles y demostrables (Art. 22). Por ello, en materia penal el hacer (acción) y el dejar de hacer (omisión) que genere consecuencias jurídicas puede ser sancionada penalmente. En este punto es fundamental diferencia la acción de la omisión, la primera está caracterizada por la intención que tienen el sujeto de cometer el delito, mientras que la omisión se deriva de aspectos involuntarios como la negligencia, imprudencia o la ignorancia.

En relación con esto, hay que tener en cuenta que la acción es la manifestación de la voluntad manifestada en el mundo exterior, resultando la voluntariedad y exterioridad requisitos fundamentales. Por ello, la acción debe ser un ataque contra un bien jurídico y necesariamente debe interferir en el sujeto y resultar la materialidad del mismo. Similar acepción sostiene Zambrano (2023) al establecer que la acción es un simple movimiento corporal provocado por un acto voluntario, sin presión mecánica o psicológica (p.28). También menciona el autor que los elementos de la acción son:

Elementos de la fase interna: objetivo, medios empleados para la consecución, posibles consecuencias.

Elementos de la fase externa: puesta en marcha, dinámica para ejecutar el objetivo, resultado previsto o concomitantes y el nexo causal (p.40).

En el Derecho Penal, la acción que verdaderamente importa es aquella cuyo fin se materializa y afecta a un bien jurídico tutelado, así es importante hacer un análisis de cada caso en concreto a fin de demostrar que la acción constituye delito y que no ha intermediado ninguna causa de exclusión de la antijuridicidad o si el sujeto que la cometió no es considerado por la normativa penal como inimputable.

Parada y Errecaborde (2018) consideran que la suplantación de identidad en redes sociales es el robo o usurpación de datos personales sustraídos a través de la utilización de técnicas de la ingeniería social. Por consiguiente, llega a ser una acción ejercida por un individuo en donde intermedia la voluntad de este para apropiarse la identidad de una persona y hacerse pasar por ella (p. 44). Hay que considerar que no puede catalogarse como omisión, ya que este presupuesto es entendido como la inacción del sujeto, el dejar de hacer algo y en el caso *in examine* se efectúa obligatoriamente la actividad de sustituir, suplir, reemplazar fraudulentamente a otra persona.

Tipicidad

En líneas anteriores se mencionó que no toda acción u omisión son consideradas como delitos, pues deben ser valoradas por el sistema de filtros de la teoría del delito. En este aspecto, la tipicidad viene a ser uno de estos filtros que ayuda a determinar si existe o no una responsabilidad penal. Cornejo y Maza (2023**)** mencionan que es esencial discernir entre lo que es el tipo y la tipicidad, el primero es la descripción legal y la tipicidad es la descripción del tipo penal en la normativa, es la subsunción de la conducta al tipo. Bajo esta línea, la tipicidad está relacionada con el principio de legalidad y el de mínima intervención del poder punitivo. La intervención penal es legítima siempre y cuando los bienes jurídicos penales afectados sean relevantes para la sociedad.

El principio de legalidad conocido por el aforismo jurídico *nullun crimen sine lege,* y se consagra en la norma suprema del Estado, en la Constitución de la República del Ecuador en el que expresamente se señala “Nadie podrá ser juzgado ni sancionado por un acto u omisión que, al momento de cometerse, no esté tipificado en la ley como infracción penal” (Art. 76.3). En tanto que el COIP establece “los tipos penales describen los elementos de las conductas penalmente relevantes” (Art. 25). Este principio busca regular el accionar de los operadores de

justicia para evitar posibles arbitrariedades e inseguridad jurídica a los procesados por la comisión de una infracción penal.

La tipicidad es la descripción objetiva y material de la acción prohibida en el ordenamiento jurídico. El tratadista sostiene que el tipo penal es de carácter objetivo y subjetivo, así los elementos que forman parte del tipo penal objetivo son:

Elementos descriptivos: No requieren de alguna valoración, se establecen referencias sobre tiempo, lugar, modo, ocasión, medios.

Elementos normativos: Contienen connotaciones jurídicas y éticas.

Resultado o mutación física: Establece la finalidad que tuvo la acción antijurídica.

Nexo de causalidad: Causa y efecto entre la conducta del autor y el resultado que provoca.

Sujeto activo: Persona que ejecuta la conducta penalmente relevante.

Sujeto pasivo: Persona natural o jurídica que sufre la afectación como resultado de la acción delictiva del sujeto activo.

Por otro lado, en el tipo subjetivo se estudia el dolo que es la voluntad de hacer, prevé un conocimiento sobre los elementos descriptivos, normativos, causalidad y previsión del resultado (p. 20), así también en el tipo subjetivo se puede encasillar la imputabilidad, voluntad dolosa, voluntad culposa. El tipo penal describe la conducta reprochable penalmente y es efectuada por los legisladores, cuyo fin es garantizar la existencia de normas previas y claras para cumplir con el principio de legalidad y seguridad jurídica. Es importante que el tipo penal se configure con todos los elementos que exponen los autores a fin de una comprensión clara y efectiva de la infracción penal.

De la misma manera, Plascencia (2004) sostienen que el tipo requiere de elementos como, las cualidades del sujeto activo u pasivo, el resultado y la atribución a la acción u omisión, el objeto material, medios, circunstancias, tiempo, lugar, modo, ocasión, elementos normativos, elementos subjetivos y demás que la ley en cada caso prevé (p. 19). En el caso ecuatoriano, la normativa penal bajo una percepción finalista considera a la acción y omisión en el tipo penal, además incluye el dolo y la culpa como elementos de la acción. Además, el COIP reconoce en la categoría de la tipicidad la existencia del error de tipo vencible e invencible como una causa de exclusión de la tipicidad. El error de tipo sucede cuando por ignorancia debidamente comprobado se desconoce uno o varios de los elementos objetivos del tipo penal, cuando el

error es invencible no existe infracción penal, pero cuando el vencible se sanciona por la modalidad culposa (Art. 28.1).

Se debe tener en consideración que en esta categoría se involucra el dolo y la culpa. Según lo prescrito en el COIP una persona actúa con dolo cuando voluntariamente ejerce la conducta (Art. 26). En cambio, la culpa surge cuando se infringe el deber objetivo de cuidado. El deber objetivo de cuidado son los preceptos jurídicos a los cuales las personas se obligan a observarlas en determinadas circunstancias (Art. 27). En esta misma línea de pensamiento Jiménez de Asúa citado por Bustamante (2020) considera que el dolo es la actividad volitiva de querer hacer algo, es por ello que se habla de voluntad y conciencia al momento de ejecutar una acción, mientras que la culpa es efectuar una acción que afecta a un bien jurídico sin intensión (p. 39). Dentro del caso en cuestión, la suplantación de identidad con contenido sexual es una acción típica puesto que en el COIP se tipifica que "La persona que de cualquier forma suplante la identidad de otra para obtener un beneficio para sí o para un tercero, en perjuicio de una persona, será sancionada con pena privativa de libertad de uno a tres años." (Art. 212). La persona que suplanta la identidad de otro, lo hace dolosamente, conoce y estudia a la víctima y a sus datos personales que se encuentran en las redes digitales.

Antijuridicidad

La antijuridicidad según Creus (s.f) aparece como "una proyección del tipo que se consustancia con él" (p. 16). De esta premisa se desprende que la conducta típica es caracterizada como antijurídica, excepto que en su ejecución haya mediado una causa de justificación o cualquier aspecto permisivo establecido en el artículo 30 y siguientes del COIP. Para el autor la antijuricidad aparece incluso antes de la tipicidad, pues en dónde no existe antijuridicidad no puede existir tipo penal. En resumen, una acción es antijurídica cuando se menoscaba o se pone en peligro un bien jurídico. Por su parte, Zambrano (2023) explica que la antijuridicidad es un juicio de valor objetivo realizada sobre la acción que expresa la desarmonía que existe entre la acción efectuada y el orden jurídico definido. Se denota entonces que es una característica propia de la acción (p.19). Vale decir que, esta categoría simboliza la contradicción de un acto con el ordenamiento jurídico.

Plascencia (2004) distingue dos aspectos en la antijuridicidad, uno material y otro formal (p. 44). El aspecto material engloba al comportamiento que es contrario al ordenamiento jurídico penal, mientras que el aspecto material hace alusión a la lesión o peligro a un determinado bien jurídico. Tarrío (2008) sostiene que lo fundamental en la antijuridicidad es el análisis de las

causas de justificación (p. 37). De esta manera aparece el concepto del injusto penal como consecuencia de la verificación de un comportamiento considerado típico, es decir que se encuentra descrito en la normativa penal y la inexistencia de las causas que justifiquen el acto.

Por su parte, Binding citado por Plascencia (2004) configura una definición con carácter autónomo a la antijuridicidad y establece que la acción punible no tiende a vulnerar directamente la ley penal, más bien atenta contra la norma inmersa en la misma, es decir vulnera mandatos, prohibiciones contenidas en la normativa. Este filtro penal tiene como finalidad determinar la calificación o no de un acto como infracción penal, a través del análisis permite determinar la vulneración sin justa causa a un bien jurídico protegido por el ordenamiento jurídico.

En el caso de la suplantación de identidad se puede mencionar que el bien jurídico tutelado es el derecho a la identidad. Presupuesto jurídico reconocido en la Constitución de la República del Ecuador del año 2008 en su artículo 66 numeral 28 en donde establece que las personas tienen derecho a la identidad personal o colectiva que incluye entre otros el tener nombre y apellido, debidamente registrados, entre otros aspectos. Sin embargo, cabe destacar que conforme evoluciona la sociedad el derecho cambia y debe ajustarse a las nuevas necesidades. Es por ello que ahora la identidad no solo puede ser considerada aquel derecho que incluye un nombre y apellido debidamente registrados, pues en la sentencia No. 2064-14-EP/21 emitida por la Corte Constitucional el 27 de enero de 2021 se determina que la imagen puede revelar la identidad de la persona, esto porque con el nuevo avance tecnológico la forma de interacción social se traspasó de un plano físico a uno virtual.

En este sentido, una conducta típica es presumiblemente antijurídica, es decir va en contra de lo que establece el ordenamiento jurídico. En relación con esto, el COIP establece que “Para que la conducta penalmente relevante sea antijurídica deberá amenazar o lesionar, sin justa causa, un bien jurídico protegido por este código” (Art. 29). Se refiere a justa causa cuando surge en el cometimiento del delito circunstancia de, estado de necesidad, legítima defensa, cumplimiento del deber legal de la o el servidor de la Policía Nacional, Fuerzas Armadas y del Cuerpo de Seguridad y Vigilancia Penitenciaria, actos de servicio, cumplimiento de su misión constitucional o legal, cuando exista amenaza o peligro inminente de muerte o lesiones graves sea para sí o para terceros, entre otros (Art. 30.1). Para el caso concreto, en la suplantación de identidad, no se puede referir a una justa causa.

Culpabilidad

Constituye un juicio de reproche hacia un determinado acto que afecta a un bien jurídico protegido por la normativa. En la culpabilidad se estudia la posibilidad de que el autor adecúe su comportamiento a la exigencia del deber, es decir la posibilidad de que su decisión de efectuar o no el acto sea responsable. Tarrío (2008) menciona que los requisitos que configura la culpabilidad son: la capacidad del autor al momento de efectuar el ilícito, la comprensión de la antijuridicidad de su comportamiento, capacidad de culpabilidad, que el hecho no haya sido cometido bajo circunstancias que adquieran carácter no reprochable (p.37). En este contexto, el COIP establece que "Para que una persona sea considerada responsable penalmente deberá ser imputable y actuar con conocimiento de la antijuridicidad de su conducta" (Art. 34).

Cuando se habla de un juicio de reproche se hace alusión a lo que menciona Zambrano (2023) sobre el juicio de disvalor o reproche que se dirige a la persona que cometió el acto típico y antijurídico, de quien se presume que tiene la capacidad de comprender la antijuridicidad de su acto y que no se encuentra en situación de error de prohibición o inimputabilidad (p. 22). La culpabilidad es el medio que sirve como fundamento para la imposición de una pena. En el análisis para determinar si una determinada conducta debe ser considerada un delito, la culpabilidad dirige su atención no con la relación de la situación que ataca al orden jurídico, sino que estudia la relación del sujeto con la situación.

De este presupuesto jurídico se desprende dos momentos, el primero debido a la imputabilidad, es decir una persona capaz de recibir una sanción penal, así se habla de las personas consideradas inimputables como aquellas que tienen algún trastorno mental, personas menores de dieciocho años, así también se señala la responsabilidad en embriaguez o intoxicación. Ahora bien, sobre el conocimiento, la norma y la doctrina prevé el error de prohibición que surge cuando una persona por error o ignorancia desconoce la ilicitud de su conducta, es decir, este presupuesto jurídico recae sobre la comprensión de la ilicitud del acto que comete. Se habla de un error de prohibición vencible cuando el efecto que produce es el de disminuir la reprochabilidad, la cuantía de la pena según lo establezca la normativa jurídica; por otro lado, el error de prohibición invencible no permite un juicio de reproche debido a que el sujeto a través de la debida diligencia para comprender la antijuricidad del acto no lo ha logrado, evitando la imputabilidad de una pena.

En resumen y de acuerdo con Frister citado por Zambrano (2023) el análisis de la culpabilidad se enfoca en saber si al autor del delito se le puede hacer un reproche personal por un ilícito

que fue comprobado con anterioridad, considerando así que la reprochabilidad personal del ilícito se fundamenta en la culpabilidad que tienen el autor (p. 24). Entonces, se infiere que la culpabilidad es del autor y no del acto, es decir una persona que es considerada inimputable sí comete un delito, pero no es posible la imposición de una pena por su condición y no por el acto.

El juicio de reproche que se efectúa al acto de suplantar la identidad se dirige hacia el bien jurídico protegido, en este caso es la identidad personal. La conducta del infractor se evalúa en la medida del acto y de la capacidad para comprender la antijuricidad de su comportamiento. Además, para que una persona sea considerada culpable de este delito debe ser imputable, es decir, debe tener el conocimiento de la antijuridicidad de su conducta. Así, si el autor actúo bajo un error de prohibición desconocimiento la ilicitud del acto, esto podría disminuir la reprochabilidad. Sin embargo, en los casos de suplantación de identidad se presupone que el autor actúo bajo plena conciencia del engaño y por ende refuerza su culpabilidad.

Corte Constitucional del Ecuador: Acción extraordinaria de protección y análisis de mérito

La Constitución ecuatoriana es la norma suprema del Estado, por lo que todo el ordenamiento jurídico debe estar ajustado a los preceptos constitucionales. Para su efectivo cumplimiento aparece la Corte Constitucional del Ecuador (CCE) como "el máximo órgano de control, interpretación constitucional y de administración de justicia en esta materia". (Art. 429)

En este sentido, la CCE (2019) menciona que ejerce sus atribuciones y competencias en el ámbito jurisdiccional, garantizando la supremacía de las normas y de los derechos constitucionales bajo independencia, imparcialidad y transparencia (p. 4). Este órgano constitucional tiene la finalidad de adecuar el ordenamiento jurídico y las actuaciones del poder público a la Constitución en relación con el principio de supremacía Constitucional. En este sentido, Villigua (2022) estima que los fallos y dictámenes emitidos por este órgano va más allá de la interpretación constitucional de un problema en particular, sino que trasciende en la sociedad en general (p. 3). De tal manera que la importancia radica en los criterios jurídicos que emite y en la aplicación vinculante a otros casos similares.

La Constitución establece una serie de atribuciones como: interpretación constitucional, resolver acciones de inconstitucionalidad de actos normativos. Normas, actos administrativos, resolver acciones por incumplimiento, expedir sentencias con carácter vinculante respecto de acciones de protección, cumplimiento, habeas corpus, hábeas data, acceso a la información

pública y demás procesos constitucionales, dirimir conflictos de competencia, efectuar control de constitucionalidad, sancionar incumplimiento de sentencias y dictámenes constitucionales, entre otros (Art. 436).

En virtud de lo cual, a partir de la constituyente del año 2008 la Corte analiza y resuelve acciones extraordinarias de protección. Según Oyarte (2020) esto implicó una modificación sustancial al sistema de garantías que se establecían en la Constitución de 1998, instrumento jurídico que prohibían el acceso a la justicia constitucional para impugnar las decisiones emitidas por autoridades judiciales (p. 16). En ese entonces a esta garantía se la denominaba acción de amparo constitucional y prohibía expresamente que el Tribunal Constitucional se pronuncie sobre resoluciones judiciales. Es decir que el Ecuador a partir de la nueva Constitución del año 2008 se convierte un Estado de garantismo, en el que prevalecen los derechos reconocidos en la Constitución y en instrumentos internacionales de Derechos Humanos. La nueva constitución permite que la jurisdicción constitucional sea veedora en las decisiones judiciales, evitando que se cometan arbitrariedades y que se transgredan derechos.

La acción extraordinaria de protección (EP) es un mecanismo constitucional que permite ejercer un control de constitucionalidad a los actos que emiten los operadores de justicia. Toda vez que las decisiones judiciales no deben vulnerar los derechos reconocidos en la CRE. Este mecanismo constitucional se encuentra regulado en la Ley Orgánica de Garantías Jurisdiccionales y Control Constitucional y establece que:

> La acción extraordinaria de protección tiene por objeto la protección de los derechos constitucionales y debido proceso en sentencias, autos definitivos, resoluciones con fuerza de sentencia, en los que se hayan violado por acción u omisión derechos reconocidos en la Constitución. (Art. 58)

Es importante aclarar que, pese a que la acción extraordinaria de protección tiene como fin ejercer un control de actividad a las decisiones judiciales para verificar la existencia o no de vulneración de derechos, esta no constituye una nueva instancia. Por ello, Oyarte (2022) dice que mediante la acción extraordinaria de protección se conforma un nuevo proceso autónomo que surge posterior a la decisión impugnada, entonces no sería una instancia ya que, en caso de aceptar la demanda, la Corte se limitaría a ordenar que se corrijan errores que incurre en el fallo materia de la garantía (p. 25). En cambio, el recurso es un mecanismo de impugnación intraprocesal, debido a que en el mismo proceso surgen como una etapa o instancia.

Ahora bien, este mecanismo constitucional conforme la CRE procede contra sentencias o autos definitivos en los que por acción u omisión se consideran violados derechos constitucionales; una vez agotado los recursos ordinarios y extraordinarios en el término legal (Art. 94). Como se ha mencionado en líneas *supra* el órgano competente para conocer y resolver la EP es la Corte Constitucional, para lo cual la Corte hace un examen de admisibilidad.

Siguiendo esta línea, la Corte Constitucional a través de su jurisprudencia a mencionado que las decisiones jurisdiccionales son objeto de demanda de protección extraordinaria, sin embargo, aclara que la Corte tiene la facultad para realizar un **control de mérito** (la negrita me corresponde). Este control, permite efectuar un análisis integral del fondo de la causa. Cisneros (2020) verifica que la jurisprudencia constitucional del Ecuador ha establecido tres razonamientos para que se legitime el análisis de fondo: la protección de derechos, el principio *iura novit curia*, la dimensión objetiva de la EP (p. 214). Sin embargo, la CCE a partir del año 2019 ha establecido nuevas líneas jurisprudenciales en torno al análisis de mérito.

En esta misma línea, en la Sentencia No. 1162-12-EP/19 se explica que de forma excepcional la Corte podrá ampliar su actuación y analizar los hechos o procedimientos administrativos a los que se refiera las decisiones jurisdiccionales (párr.61). Esta posibilidad de analizar más allá de las posibles vulneraciones a los derechos en las que han incurrido las autoridades judiciales en sus decisiones tiene su fundamento en carácter de máximo órgano de control, interpretación y administración de justicia constitucional que tienen la Corte. Cisneros (2020) enfatiza en que el control de mérito procede únicamente sobre sentencias dictadas por la justicia constitucional. Así mismo, Dávila (2022) explica que este control extiende la capacidad de la corte y no se limita a verificar los vicios de la decisión impugnada, más bien su análisis se extiende a los hechos de origen.

En la Sentencia 176-14-EP/19 de la CC del Ecuador se estableció que de manera excepcional y de oficio la Corte podrá realizar un análisis de mérito cuando incurran los siguientes presupuestos (párr. 55):

- La autoridad judicial inferior haya violado el debido proceso u otros derechos de las partes.
- Cuando la autoridad judicial inferior no haya tutelado derechos en el proceso de origen y constituyan una vulneración.
- Que el caso no haya sido seleccionado para revisión.

Sentencia No. 2064- 14- EP de la Corte Constitucional

Antecedentes

El 19 de agosto de 2014, una mujer (NN) cuyo nombre es reservado para salvaguardar el derecho a la intimidad y privacidad, presentó una acción de hábeas data en contra de DD (nombre reservado) con la finalidad de determinar el modo en que la demandada llegó a poseer fotografías personales e íntimas de la actora, solicitó se determiné desde cuándo las tiene, cómo las ha utilizado, a quiénes a difundido y qué tecnología empleó para el acceso y almacenamiento de las fotografías. Además, pidió reparación integral y como medidas cautelares solicitó que el juez dicte la prohibición para que dichas fotografías sean difundidas o reproducidas por cualquier medio.

En sentencia de 26 de agosto de 2014 la jueza competente resolvió aceptar la acción de hábeas data y dispuso la eliminación de forma inmediata de las fotografías de la actora que se encuentre contenidas en cualquier soporte informático o material, la presentación de una declaración juramentada en la que la demandada afirme no poseer ningún archivo relativo a las fotografías y consecuentemente que no puede hacer uso de estas. En esta misma línea, el 27 de agosto del 2014 la actora solicitó ampliación de la sentencia en lo que respecta la reparación integral. Sin embargo, el 01 de septiembre del mismo año la jueza resolvió negar el recurso de aclaración.

En la misma fecha la parte actora apeló la sentencia en la parte que niega la reparación integral. Es así como el 13 de octubre de 2014 la Sala rechaza el recurso de apelación y revoca la sentencia de primera instancia declarando sin lugar la acción de hábeas data toda vez que al analizar no se encontró vulneración de derechos de la actora. La argumentación de la Sala radicó en el hecho de que la actora fue quien libremente puso en circulación sus datos al enviárselo a un tercero. Frente a esta situación, el 02 de diciembre de 2014 la procuradora judicial de la actora presentó acción extraordinaria de protección en contra de la sentencia dictada en segundo nivel.

Alegaciones de las partes

Accionante: Señala que la Sala vulneró los siguientes derechos:

- *Debido proceso en la garantía de recurrir el fallo* por cuanto presentó la apelación exclusivamente en lo que atañe al derecho a la reparación integral, situación que limita e impide a los jueces a pronunciarse respecto de alegaciones no invocadas.
- *Debido proceso en la garantía non reformatium in peius,* sostiene que la Sala no debía colocar a la parte recurrente en situación jurídica peor de la que partió.

- *Defensa,* alega que la Sala colocó a la parte accionante en la disyuntiva de aceptar una declaración parcial del derecho o la posibilidad de que con la apelación pueda perder aquello que ya conseguido.
- *Tutela judicial efectiva,* ya que la Sala no ha dado respuesta a la pretensión formulada en la apelación.
- *Debido proceso en la garantía de motivación,* aduciendo que la Sala enuncia normas constitucionales aplicables a procesos penales.

Accionados: Los jueces de la Sala presentaron su informe de descargo bajo los siguientes términos:

En lo principal, los jueces de la Sala sostienen que no existe violación de derechos, puesto que éstos tienen la competencia para poder modificar los alcances de la sentencia, sin que sea necesarios que las dos partes apelen, esto con el fin de proteger los derechos constitucionales. Además, mencionan que la sentencia emitida goza de motivación, no se afectó a la tutela judicial efectiva. Finalmente, señala la jueza que no existe vulneración a derechos constitucionales, ya que en las pretensiones del caso de origen la accionante solicita una investigación de supuestas infracciones contempladas en la legislación penal.

Análisis constitucional

Frente a los hechos expuestos, la CC realiza su análisis para determinar las supuestas vulneraciones de los derechos constitucionales invocados por la parte actora.

- ***Debido proceso en la garantía de recurrir al fallo:*** La Corte estima que no existió vulneración a este derecho, puesto que el accionante ejerció plenamente este derecho al presentar el recurso de apelación. Así también, deja claro que este derecho tiene carácter instrumental y permite el acceso a los medios de impugnación establecidos en la ley, tiene como fin encausar un nuevo debate sobre la controversia, sin que ello signifique una decisión favorable para el recurrente.
- ***Debido proceso en la garantía non reformatium in peius:*** Señala que este derecho es aplicado en materia penal, y por ende no considera pertinente una pronunciación al respecto.
- ***Derecho a la defensa y Tutela Judicial Efectiva:*** Bajo el análisis efectuado por la Corte, esta considera que no se vulneraron estos derechos, debido a que la accionante ha accedido a la justicia y ha recibido un pronunciamiento de fondo, además que ejerció

su derecho a la defensa en la audiencia pública en la que pudo presentar las pruebas de las que se creyó asistida.

- ***Debido proceso en la garantía de motivación y Tutela Judicial Efectiva:*** La Corte estima que existió vulneración del derecho al debido proceso en la garantía de la motivación, pues la Sala en su sentencia se limitó a realizar una simple enunciación de que no se podía proteger el derecho a la imagen e intimidad de la accionante sin que ello implique el menoscabo de los derechos constitucionales de la accionada, cuestión que quedó en una mera enunciación puesto que no explicó de qué manera se conlleva a dichas vulneraciones dentro del ámbito constitucional o legal. La CC estableció que la sentencia emitida por la Sala adolece de incongruencia. Finaliza su análisis entendiendo que la obtención de una respuesta motivada forma parte de la tutela judicial efectiva y al no existir la misma se vulnera este último.

Análisis de Mérito

En líneas anteriores ya se refirió respecto del análisis de mérito y sus implicaciones, por ello, a continuación, se efectuará un análisis respecto de lo esgrimido por la Corte Constitucional en el presente caso. Los argumentos esgrimidos versan en los siguientes puntos:

Alcance del concepto de dato personal: La Corte estima que el concepto de dato personal debe ser entendido de la forma más amplia, en el sentido de todo el conjunto de información que haga referencia sea de forma directa o indirecta a cualquier aspecto relativo a una persona, sus bienes o diferentes esferas y dimensiones. Llega a la conclusión que una fotografía de una persona constituye un dato personal, pues la imagen puede revelar la identidad de una persona cuando contenga su rostro u otro elemento que permita reconocer la identidad del titular (número de cédula, nombre). También constituye un dato personal la fotografía que sin necesidad de contener el rostro del titular permite el reconocimiento de esta.

Tratamiento de datos personales: Considera que el tratamiento de datos personales es un concepto técnico que no está desarrollado adecuadamente en la normativa nacional. Recogiendo la doctrina, jurisprudencia y leyes de otras jurisdicciones determina que comprende un amplio espectro de actuaciones y deja a criterio de los jueces el establecer cuando se está frente a un tratamiento de datos personales, establece en la sentencia los parámetros a considerar.

Tratamiento de datos personales en la esfera personal o doméstica y sus efectos: La CC considera que el tratamiento de datos personales que se lleva a cabo en una esfera doméstica o

personal no activa la protección constitucional del dato, pero siempre que el dato se encuentre en el poder de una tercera persona su titular puede solicitar la anulación, modificación, acceso o eliminación, salvo las excepciones previstas en la ley. Concomitante a esto establece que es considerado tratamiento con connotación legal cuando el acceso produce daño subjetivo u objetivo en la privacidad de la persona, contrario *sensu* si no es susceptible de producir daño en cualquier dimensión del individuo este no puede ser considerado capaz de producir efectos jurídicos. Resalta que el tratamiento de datos personales es lícito siempre que se verifique el consentimiento del titular para el efecto.

Consentimiento del titular: Para cualquier tipo de tratamiento de datos personales es necesaria la autorización de titular o el mandato de la ley, sin que esto signifique la renuncia de derechos. El consentimiento es definido por la Corte como la manifestación de la voluntad libre, específica, informada e inequívoca. Por otro lado, cita jurisprudencia de la Corte Constitucional de Colombia y en la que enmarca que la autorización que otorga el titular del dato personal no significa una renuncia al derecho fundamental.

Derecho a la intimidad: El criterio de la Corte se apega a lo establecido en la doctrina y en la jurisprudencia, toda vez que esgrime que este derecho implica la existencia, goce y disposición de una esfera reservada para el individuo, capaz de otorgarle al individuo la libertad para su desarrollo, sin injerencias externas, ni arbitrarias en los distintos ámbitos que componen su vida. Resalta que el derecho a la intimidad se da en diferentes ámbitos, relaciones familiares, costumbres, prácticas sexuales, creencias religiosas, salud, domicilio, nivel informático, secretos profesionales de una persona y espacio físico. La intimidad dentro del espacio virtual se delimita el marco de protección determinando si aquel espacio es cerrado o abierto.

Privacidad: Establece lineamientos para que el juez pueda determinar cuándo opera el derecho a la privacidad. Es importante que los operadores de justicia realicen un examen de cada caso en particular para verificar si concurren los elementos subjetivos y objetivos para considerar que una persona tiene una expectativa razonable de privacidad. Es así que aclara que el elemento subjetivo consiste en que quien alegue violación a la intimidad, considere que su actividad o esfera está protegida de posibles injerencias. Por otro lado, el elemento objetivo consiste en que la sociedad tenga la capacidad para asumir que la actividad o esfera es oponible a terceros. Además, en cada caso particular el juez deberá analizar y determinar: el tipo de información que se discute, el espacio, el conocimiento o autorización del titular, la condición

de la persona, la relación del titular de los datos y el individuo que pretende su acceso o tratamiento.

Procedencia del habeas data cuando existe elementos inherentes a justicia ordinaria: En principio la Corte ha determinado que la acción de hábeas data como un mecanismo constitucional tiene por objeto garantizar el acceso, autodeterminación informativa, conocimiento del uso, finalidad, origen, destino, recolección y tiempo de videncia del dato personal. Por su parte, el ámbito penal está orientado a constatar la existencia objetiva y subjetiva de una infracción penal, la responsabilidad y la imputación de una sanción. En definitiva, la esfera constitucional no es subsidiaria de la penal y viceversa, por lo tanto, un proceso con identidad subjetiva que se litigue en vía penal o civil no es causa para que no sea ventilado por la esfera constitucional.

Resolución del problema jurídico.
En el caso que examina la Corte establece como problema jurídico lo siguiente:

> ¿La parte demandada en el proceso de origen realizó un uso no autorizado de las fotografías íntima y personales de la actora? De ser así, ¿Dicho tratamiento además vulneró los derechos constitucionales de la actora a la protección de datos personales o autodeterminación informativa, así como el derecho a la imagen, honra, buen nombre e intimidad? Por consiguiente ¿Cuál es la reparación integral que corresponde en el presente caso? (Párr. 146)

Al respecto señala que la imagen objeto de la *litis* constituye un dato personal y al pertenecer a la esfera más íntima de la actora puesto que es una manifestación de su sexualidad tiene el carácter de dato sensible y goza de mayor protección. Así también, considera que la demandada efectúo un tratamiento de datos personales sensibles de la actora, al acceder, almacenar y difundirlas. En relación con lo manifestado, deja claro que el envío de fotografías a un tercero no equivale a otorgar el consentimiento o autorización para cualquier tipo de tratamiento, más aún cuando se tratan de datos personales altamente sensibles. Siendo así que, la Corte verificó que la demandada vulneró el derecho a la protección de datos personales o autodeterminación informativa.

Por otro lado, referente al derecho a la honra y buen nombre sostiene que estos derechos son inherentes a la dignidad humana y el hecho de que la demandada haya divulgado las imágenes intimas de la actora produce una afectación a estos derechos independientemente de la relación parento- filial que tenga. Respecto del derecho a la imagen la C.C. explica que involucra dos

facultades, la primera la de decidir qué información gráfica que contiene sus rasgos físicos pueden tener difusión pública y la impedir la captación, reproducción o publicación de la propia imagen y en el presente caso la demandada vulneró este derecho por cuanto limitó a la actora a manejar y disponer de su propia imagen. Así mismo, esgrime argumentos con relación a la intimidad, manifiesta que el haber divulgado las imágenes a los padres de la actora se atenta contra la esfera más íntima.

Finalmente, resalta que la sentencia constituye en sí mismo un medio idóneo para la reparación integral de la víctima.

Decisión

- Declara que la sentencia de fecha 13 de octubre de 2014 vulneró el derecho a la tutela judicial efectiva.
- Acepta la acción extraordinaria de protección.
- A través del análisis de mérito declara la vulneración de derechos constitucionales.
- Solicita formatear el *flash* que contiene las imágenes de la actora.
- Prohíbe el tratamiento de las fotografías.
- Declara la sentencia como reparación integral a la víctima.
- Dispone la difusión de la sentencia.
- Deja a salvo el derecho de la actora para accionar en otros ámbitos de la justicia ordinaria.

Influencia de la sentencia 2064-14-EP de la Corte Constitucional en la sanción de la conducta de suplantación de identidad en el contexto digital.

El ordenamiento jurídico ecuatoriano busca proteger los derechos constitucionales y garantizar una efectiva armonía en la convivencia social. En virtud de lo cual, el legislador ha establecido un marco jurídico específico para cada materia, destinado a regular los diferentes aspectos de la sociedad civil. En este sentido, el derecho penal regula las conductas penalmente relevantes y tiene como fin sancionar aquellas conductas punibles y mediante el proceso penal se busca la verdad y la reparación integral del bien jurídico afectado. En este contexto vale aclarar que, la Corte Constitucional de Colombia en la sentencia T-405/07 sostiene que la vía penal se orienta a "constatar la existencia objetiva y subjetiva de la infracción penal, la responsabilidad de la imputada, e imponer la sanción correspondiente"

Por esto, en la vía constitucional como se desprende del caso *in examine* únicamente se esgrimen cuestiones atenientes a la vulneración de derechos constitucionales, sin embargo, deja

a salvo el derecho de la parte actora para iniciar un proceso en vía ordinaria. Se debe considerar que la vía constitucional busca una protección eficaz, pronta y oportuna de todos los derechos. En el caso del uso no autorizado de datos personales, el habeas data tiene como fin permitir que las personas accedan a la información sobre sí mismas que se encuentra en bancos de datos públicos o privados, Además pueden exigir su rectificación, actualización, eliminación o anulación si es necesario. Mientras que la vía penal busca ejercer el poder punitivo del Estado. Considerando esto, si bien la vía constitucional es una respuesta inmediata para tutelar los derechos vulnerados, esto no quiere decir que se sanciona al infractor, *contrario sensu* para con la acción penal.

Ahora bien, refiriéndose únicamente a la vía penal, en esta el titular de la acción es el Estado, por ello a través de la fiscalía general del Estado (FGE) se recopilan los elementos de convicción necesarios para formular cargos o archivar el proceso. La CC en la sentencia 2064-14-EP/21 ha conceptualizado temas importantes para el análisis de la conducta de suplantar la identidad con contenido sexual en la era digital, esgrime cuestiones con relación a datos personales, derecho a la intimidad, privacidad, datos de carácter sensible, tratamiento de datos personales, imagen, etc.

En la investigación que atañe es esencial señalar que según el Equipo de comunicaciones y Escuelas de Seguridad Digital (2021) la suplantación de una identidad digital hace alusión a la apropiación indebida de otra para actuar en su nombre, entre sus consecuencias está, hacer bromas pesadas sin consecuencia jurídica alguna, dañar la reputación o realizar ciberataques aprovechando la confianza que se genera en el entorno digital. Actualmente es común observar la creación de perfiles falsos con información real de la víctima suplantada, este escenario no incide en la información personal de la víctima, pero si en su reputación, debido a la exposición de la imagen y datos personales de la víctima. Pues, para el Equipo de comunicaciones y Escuelas de Seguridad Digital (2021) el atacante crea un perfil a imagen y semejanza del titular de los datos.

Estas conductas son efectuadas a través del uso de medios tecnológicos, por lo que deberían ser considerados como ciberdelitos o delitos informáticos. La actual regulación jurídica penal ecuatoriana y la jurisprudencia relevante ha considerado necesario incluir tipos penales y hacer un análisis enfocado en las nuevas tecnologías y las conductas ilícitas que derivan de ellos. Así, en palabras de Castillo (2024)

> Desde que el Código Orgánico Integral Penal entró en vigor en 2014, incluye y penaliza los delitos informáticos, que abarcan acciones como la divulgación ilegal de bases de datos, la interceptación no autorizada de información, la transferencia electrónica de fondos obtenidos de manera ilícita, los ataques contra la integridad de sistemas informáticos, el acceso no autorizado a sistemas telemáticos o de telecomunicaciones, la producción y distribución de pornografía infantil y el acoso sexual. (p. 31)

En línea con lo manifestado, el desarrollo tecnológico deja abierta la posibilidad de conductas antisociales y delictivas que tienen impacto a nivel global. En palabras de Vásquez (2024) estas conductas tienen el objetivo de dañar o lesionar a la sociedad y son consideradas conductas de carácter doloso, en dónde el sujeto activo requiere un determinado conocimiento para el cometimiento del acto, teniendo como medio los aparatos electrónicos como computadoras (p. 42). En suma, se refiere a delito informático cuando el comportamiento criminógeno de un sujeto es llevado a cabo mediante aparatos electrónicos y con el uso de las tecnologías. Esta nueva forma de delinquir atenta contra el bien jurídico protegido por el ordenamiento jurídico que no siempre es el patrimonio, pese a que la mayoría de los ataques cibernéticos tengan como fin obtener un lucro. Una de las características de este tipo de delitos es que, los que lo cometen tienen la posibilidad de actuar bajo en anonimato, circunstancia que limita su rastreo y por ende la imposición de una sanción.

La penalización de los delitos informáticos permite garantizar una tutela judicial efectiva que responda a las necesidades actuales de la sociedad. En este sentido, la jurisprudencia constitucional involucra un medio idóneo para ampliar el contenido de los derechos reconocidos en la constitución en el ámbito tecnológico. Es decir, la Corte Constitucional engloba la protección a los derechos desde un enfoque digital. Dado que, en la actualidad los delitos cometidos en el mundo digital están asociadas con corrupción, destrucción de daos, apropiación de datos personales, entre otros. Sin embargo, como lo manifiesta Castillo (2024) las nuevas formas delictivas representan una amenaza difícil de controlar por el sistema de derecho penal convencional y el sistema de justicia ecuatoriana (p. 34).

Bien jurídico protegido en la suplantación de identidad en el contexto digital

Según el diccionario panhispánico del español jurídico, un bien jurídico consiste en objetos materiales e inmateriales, relaciones, intereses o derechos que socialmente pueden ser considerados valiosos y mantienen la calidad de estar protegidos jurídicamente. En el ámbito penal, este constituye la base de la antijuridicidad, toda vez que se configura la lesión al objeto

de protección cuyo titular sería el sujeto pasivo. En los casos de delitos informáticos, se sabe que el bien jurídico afectado no siempre es el patrimonio, pues en palabras de Vásquez (2024)

> la criminalidad mediante el uso de las TIC puede ir desde un fraude electrónico, hasta una usurpación de identidad o distribución de pornografía infantil, tráfico de personas, robo de datos personales, secuestro de información, lo cual vale la pena señalar, llega a ser en ocasiones más importante que el mismo daño patrimonial. (p. 44)

El patrimonio, debe ser considerado como aquel hecho notorio y es al que usualmente apuntan los ciberdelincuentes mediante la manipulación de los sistemas informáticos, como por ejemplo la clonación de tarjetas, robos de cuentas bancarias a través del internet, entro otros. Vásquez (2024) explica que el patrimonio se constituye por datos, documentos electrónicos de carácter privado que tienen los equipos, pues existen casos en los que los delincuentes secuestran el disco duro del aparato electrónico (p. 44). La suplantación de identidad no centra su objetivo únicamente en el robo de los datos personales, sino en la posibilidad de utilizarlos para la comisión de actividades ilícitas. En ese escenario Gercke (2013) establecen que el uso de una identidad usurpada sirve para (p. 23):

Comisión de delitos financieros: A través de la información personal el delincuente puede administrar cuentas financieras existentes o crear nievas suplantando la identidad de la víctima con la finalidad de efectuar transacciones bancarias como, trasferencias o compras.

Venta de la información: El principal objetivo que persigue esta forma de utilizar una identidad falsa, es generar una ganancia directa sin la necesidad de cometer el delito, esta información puede servir para falsificar documentos de identidad, utilizarlos para la consecución de nuevos delitos como, viajes ilícitos, inmigración ilegal, etc.

Encubrimiento de la identidad: Se busca establecer el anonimato para la ejecución de actividades ilícitas como, el blanqueo de dinero, que consiste en generar información de identidad falsa y facilitar las transferencias a distancia mediante la utilización de herramientas tecnológicas.

El autor ha enfocado su estudio en describir los actos ilícitos que se cometen a través de la suplantación de identidad en un escenario patrimonial. Este delito también puede estar asociado a los delitos que atentan contra el honor, en el cual el victimario lleva a cabo una serie de conductas que lesionan la reputación y el honor de una persona, sirviéndose de una identidad

falsa o suplantada de la propia víctima, a través del uso de datos personales obtenidos de redes digitales o sustraídos de forma indebida de soportes informáticos.

Añadido a esto, Martínez (2024) considera que otra de las finalidades que motiva la ejecución de esta conducta es la suplantación de identidad por mera venganza, cuando por ejemplo, una persona ingresa al perfil original de su expareja debido a que conoce las claves de seguridad y efectúa actos como, emitir a nombre de la víctima comentarios ofensivos a sus seguidores causándole daño a su reputación, en el contexto de violencia de género, acoso o provocación de odio mediante el uso de un lenguaje obsceno e indecente, amenazante (p. 208). Esta conducta puede generar una grave afectación psicológica y psicosexual ya que se utiliza información sensible e íntima de la víctima. Otro ejemplo señalado por el autor es cuando un adolescente utiliza la imagen de una compañera de clase con el objetivo de hacer un montaje fotográfico de connotaciones sexuales y hacerse pasar por ella en la red social, ridiculizándola o molestándola.

Es decir que, existen diversas modalidades de la comisión de delitos a través de la suplantación de identidad, que va desde las formas más sencillas que puede ejecutar cualquier persona por el uso de técnicas de ingeniería social o engaño, hasta los métodos más complejos de la ingeniería social, circunstancia que se encuentra al alcance de pocos individuos. En una red social, el robo de identidad puede darse por dos formas, la primera es mediante el acceso indebido a las cuentas personales de la víctima y el segundo es por la creación de un perfil auténtico con la utilización de datos personales. Con todo esto, se deja claro que el bien jurídico afectado puede variar dependiendo de la circunstancia de cada caso y debe ser analizado por el operador de justicia a la hora de activar el poder punitivo del Estado. De ahí para Gercke (2013) “el acceso a datos relacionados con la identidad permite al infractor cometer otros delitos. Siendo que, los infractores no se interesen solamente por los datos, sino por la posibilidad de utilizarlos para actividades delictivas” (p. 22).

Suplantación de identidad con contenido sexual: Bien Jurídico afectado, Identidad, Identidad digital o Intimidad

La identidad crea vínculos sociales y culturales con la sociedad civil para ejercer y hacer efectivos sus derechos políticos y civiles. Para Lawson (2013) los elementos que componen la identidad son nombres y apellidos, nacionalidad, fecha de nacimiento, profesión u ocupación, antecedentes familiares y laborales, datos biométricos (p.31). En este sentido, en el COIP se contemplan delitos que atentan contra el derecho a la identidad como la supresión, alteración

o suposición de la identidad y estado civil y la suplantación de identidad contenidos en los artículos 211 y 212. En este sentido, se refiere a una identidad física y a una suplantación de identidad de una persona que existe en el mundo exterior, por ejemplo, hay suplantación de identidad cuando un individuo se hace pasar por otra persona mediante la utilización de un documento público como la licencia de conducir. Este derecho es considerado un bien jurídico autónomo y es relevante para la construcción de la dignidad personal. Martínez (2024) menciona que sirve como presupuesto del ejercicio de facultades reconocidas y amparadas en el ordenamiento jurídico.

En el contexto digital, el robo de identidad como lo menciona Guzmán et al. (s.f) consiste en la apropiación o usurpación de datos y documentos de identificación de un determinado individuo, cuya finalidad es la creación de documentos de identidad para desarrollar condiciones mínimas de identidad que sirvan como plataformas digitales en perjuicio de la víctima para ejecutar todo tipo de operaciones delictivas (p. 666). La información contenida en el ciber espacio debe considerarse sensible, puesto que al estar inmersa en una red de alto impacto social surge un riesgo significativo en la protección de la identidad digital. Cabe aclarar que la identidad digital no está reconocida como un derecho en el ordenamiento jurídico, sin embargo, como lo afirma Castillo (2024) es el resultado de los cambios sociales que provoca el avance de las tecnologías de la información y de la comunicación (p. 10). Este presupuesto se construye con la información que un individuo comparte en las redes digitales, como su nombre y apellido, dirección física, datos fiscales, correo electrónico, número de teléfono o su imagen, fotografías, historiales de navegación y comportamiento en línea, cuestiones que forman parte del contenido más íntimo de la persona.

En el mundo actual, el desarrollo de servicios de internet como las redes sociales implica que los individuos se presenten a sí mismo en un mundo virtual y mantengan contacto con otros usuarios. Los datos compartidos en estos medios incluyen desde nombres y apellidos, hasta cuestiones de índole sexual, frente a esto, los delincuentes tienen un libre acceso a esta información pública que utilizan con fines delictivos. Bajo esta perspectiva Batuecas (2022) manifiesta que

> La realidad viene a demostrarnos que la informática, en general, y el big data y el tratamiento de los datos personales, en particular, afectan a la identidad de las personas. Ello es así desde el momento que en Internet existen datos de la mayoría de las personas relacionados directa o indirectamente con su identidad (p. ej., nombre, filiación, lugar

> de nacimiento, ideología, creencias, trabajo, aficiones, etc.), de tal modo que con un simple y sencillo cruce de esos datos es posible construir perfiles de cada uno de sus titulares. (p. 951)

Por ello, la identidad digital se ha convertido en un concepto esencial en el ámbito jurídico, representando la forma en que una persona o entidad se presenta y es reconocida en el entorno digital. Este concepto no solo abarca los datos personales y la actividad en línea, sino que también implica una serie de derechos y protecciones que son esenciales para salvaguardar la dignidad y la privacidad de los individuos. Con el avance tecnológico se ha empezado a considerar a la identidad digital como un posible bien jurídico protegido, que incluye el derecho a existir en Internet y a ser reconocido como individuo. Este derecho está relacionado con otros derechos fundamentales, como el derecho a la privacidad y el derecho al olvido, que permiten a los individuos controlar su información personal y decidir qué datos se pueden compartir (Fernández, 2012).

Ahora bien, vale preguntarse qué bien jurídico se afecta la conducta de suplantación de identidad con contenido sexual que surge en los entornos digitales. Esta conducta constituye una grave infracción que puede atentar contra varios bienes jurídicos, empero en particular en contra de la intimidad, dignidad e integridad de la víctima. La Corte Constitucional ha referido en la sentencia 2064-14-EP/21 que, "pertenece a la esfera más íntima del individuo dado que esta constituye una manifestación del ejercicio de su sexualidad" (párr. 152). Este delito no solo implica una usurpación de identidad del individuo, sino que también lleva a cabo la difusión no consentida de imágenes o información sensible que impacta significativamente en la vida de las víctimas. En este contexto, es fundamental analizar como el ordenamiento jurídico aborda esta problemática, identificando mecanismos de protección establecidos para garantizar el ejercicio de derechos fundamentales de las personas frente a conductas delictivas que vulneran su esfera más íntima y privada.

La intimidad es un derecho fundamental que se encuentra protegido por diversas normativas y principios jurídicos, siendo considerado un bien jurídico esencial en la vida de las personas. Este concepto abarca la esfera personal y familiar de los individuos, garantizando que puedan vivir sin injerencias indebidas de terceros, ya sean particulares o entidades públicas. Los delitos contra la intimidad se relacionan con derechos como la dignidad, el honor, el buen nombre de los individuos.

Tabla 4: *Comparación de la protección jurídica de los bienes jurídicos afectados en la suplantación de identidad con contenido sexual.*

Bien jurídico	**Protección jurídica**
Identidad	Reconocido en la Constitución de la República del Ecuador en el artículo 66. Los delitos que atentan contra este bien jurídico están contenidos en los artículos 211 y 212 del Código Orgánico Integral Penal.
Intimidad	Reconocido en la Constitución de la República del Ecuador en su artículo 66. Los delitos que atentan contra este bien jurídico están tipificados en los artículos 178, 179, 189 y 181 del Código Orgánico Integral Penal.
Identidad digital	No está reconocido en el contexto jurídico la identidad digital, sin embargo, la jurisprudencia y doctrina lo considera como un derecho que surge en el entorno digital.

Nota: Información recogida del Código Orgánico Integral Penal actualizado 2024.

Prevención y sanción de la suplantación de identidad

La suplantación de identidad es una conducta cuyo fin es múltiple, por ejemplo, efectuar fraudes bancarios, estafas, robo de identidad digital y datos, espionaje, dañar la reputación e imagen del titular de los datos, entre otros. En los últimos años a través de las redes de telecomunicación, el uso de internet y las plataformas sociales esta conducta a aumentado. Según la Agencia de Regulación y Control de las Telecomunicaciones los casos de suplantación de identidad surgen cuando los atacantes roban los datos de los usuarios a fin de usarlos en su propio beneficio. Por lo que, el Centro de Respuestas a Incidentes Informáticos de Arcotel (EcuCERT) ha previsto las siguientes medidas que reducen el riesgo de el robo de datos personales.

- Evitar dejar copias de documentos de identidad o cualquier otro tipo de documento importante sin supervisión o en manos de personas desconocidas.
- Informarse sobre las implicaciones de la suplantación de identidad, incluyendo técnicas como el phishing y otros métodos de robo de información en el entorno digital.
- Ajustar la configuración de privacidad y seguridad en perfiles de bancos, tarjetas de crédito, plataformas de compra en línea, redes sociales y cualquier otra plataforma digital que se utilice.

- Utilizar contraseñas robustas que tengan más de 10 caracteres, incluyendo números, letras mayúsculas y símbolos, evitando información personal como fechas de nacimiento o nombres familiares que podrían ser fácilmente identificables por un atacante.
- Cambiar las contraseñas periódicamente y considerar el uso de un gestor de contraseñas para facilitar la gestión de la seguridad.
- No compartir imágenes o videos sensibles, especialmente con desconocidos, y evitar ceder ante exigencias del destinatario.
- Revisar las políticas de privacidad y seguridad, así como los términos del servicio en plataformas bancarias, de compras en línea y redes sociales.
- Asegurarse de que los sitios web donde se realizan transacciones son seguros, verificando que la dirección comience con "https://" y tenga un ícono de candado en la barra del navegador.
- No dejar dispositivos como teléfonos móviles, tabletas o computadoras portátiles desatendidos en espacios públicos.
- Evitar conectarse a redes Wi-Fi no confiables y abstenerse de realizar transacciones o ingresar información sensible en redes públicas.
- No publicar información personal abiertamente, especialmente en redes sociales.
- Implementar la autenticación en dos pasos en todas las plataformas que lo permitan, utilizando métodos como una contraseña combinada con un mensaje de texto.

Es importante aclarar que las autoridades que investigan este tipo de conductas encuentran una gran limitante debido a que los delincuentes se valen del uso informático y la aplicación de altos conocimientos en ingeniería social y hace que las evidencias sean difíciles de encontrar. La prevención para evitar ser víctima de estos actos delictivos se encamina a la educación digital que la sociedad debe tener al navegar en línea.

El Código Orgánico Integral Penal tipifica esta conducta como un delito que atenta contra el derecho a la identidad, estableciendo que, “La persona que de cualquier forma suplante la identidad de otra para obtener un beneficio para sí o para un tercero, en perjuicio de una persona, será sancionada con pena privativa de libertad de uno a tres años” (Art. 212). Como se ha mencionado a lo largo de la investigación, la identidad es el conjunto de datos personales que singularizan a un individuo dentro de la sociedad. La identidad es un derecho reconocido por la Constitución en su artículo 66 numeral 28 y desarrollado en normas jurídicas infra constitucionales como la Ley Orgánica de Gestión de la Identidad y Datos Civiles. Pero, hoy

en día un individuo no solo posee una identidad física, en un mundo globalizado este derecho trasciende a fronteras digitales. Bajo este precepto, el estudio y análisis de los derechos que involucran la protección de datos personales realizados por la Corte Constitucional del Ecuador en la sentencia 2064-14-EP con una visión de tutela de derechos en el ámbito digital adquiere relevancia para el análisis de este tipo penal.

1.2 Objetivos

Objetivo general

Analizar la influencia de la Sentencia No. 2064-14-EP/21 de la Corte Constitucional del Ecuador en el marco jurídico penal del Ecuador.

Objetivos específicos

Examinar el alcance y los componentes de los datos personales en el ámbito digital establecidos en la sentencia.

Establecer de qué manera el tratamiento de datos personales en redes digitales conlleva al cometimiento del delito de suplantación de identidad con contenido sexual en el contexto digital.

Evaluar la eficacia de la Sentencia No. 2064-14-EP/21 de la Corte Constitucional del Ecuador en la prevención y sanción de la conducta de suplantación de identidad con contenido sexual considerando la legislación ecuatoriana vigente y jurisprudencia relevante.

CAPÍTULO II. - METODOLOGÍA

La investigación es definida como un proceso sistemático que aplica un método científico cuyo fin es generar un nuevo conocimiento capaz de ser verificado. La metodología implica una búsqueda ordenada y sistemática de información para la solución de una problemática. El método dentro de una investigación constituye el camino o procedimiento que debe seguir el investigador para descubrir o dar a conocer hechos. En definitiva, la metodología de la investigación es definida como el estudio de procedimientos que permite obtener nuevos conocimientos en el campo de la investigación científica. Villanueva (2022) señala que los ejes de la metodología son: ordenar y sistematizar nuevos conocimientos; presentar la solución a un determinado problema; ser un camino para descubrir o interpretar el problema analizado; anticiparse a situaciones futuras para prevenirlas (p.17).

El estudio se desarrolló mediante la aplicación de la metodología de la investigación, puesto que se empleó un proceso sistemático que buscó la solución a un problema social de alto impacto en los últimos tiempos. Se basó en el saber de ciencias existentes y se utilizó técnicas e instrumentos de recolección y análisis de datos con el objetivo de conocer objetivamente las causas y consecuencias del fenómeno estudiado. Además, se plantearon interrogantes sobre la Sentencia 2064-14-EP de la Corte Constitucional del Ecuador y la suplantación de identidad con contenido sexual como: ¿cuándo sucedió? ¿dónde sucedió? ¿Cómo pasó? ¿por qué pasó? preguntas que conforme Villanueva (2022) el investigador se dedica hacer con frecuencia para dar respuesta al fenómeno indagado (p. 17).

2.1 Materiales

Para el desarrollo de la investigación se utilizaron materiales e instrumentos que conllevaron a realizar un análisis exhaustivo de la Sentencia 2064-14-EP de la Corte Constitucional y la conducta de suplantación de identidad con contenido sexual en un contexto digital. Para recoger la información sobre esta problemática se utilizaron fuentes tanto primarias como secundarias, a través de la revisión, detección, consulta, extracción, recopilación e integración.

Las fuentes primarias según Gallardo (2017) “proporcionan datos de primera mano” (p. 45), ya que se trata de documentos en los que se incluyen los resultados de estudios correspondientes. Hernández (2014) señala que alguno de los ejemplos de fuentes primarias es, libros, antologías, artículos de publicaciones periódicas, monografías, tesis, documentos oficiales, testimonios de expertos, etc. Bajo esta premisa, en el estudio se utilizaron como

fuentes primarias libros obtenidos de la Biblioteca Virtual de la Universidad Técnica de Ambato y se realizaron entrevistas a expertos en Derecho Penal con la finalidad de obtener información primaria que sustentó la indagación.

Por otro lado, Mar et al. (2020) aseguran que las fuentes secundarias son documentos escritos desarrollados mediante el análisis e interpretación de textos o investigaciones ya existentes (p.180). Es decir, la información es obtenida de enciclopedias, bibliografías, críticas literarias, diarios, publicaciones y otros materiales. En este contexto, fue fundamental contar con acceso a bases de datos especializados, legislación relevante, jurisprudencia y estudios previos relacionados con el tema. Además, en la búsqueda bibliográfica se incluyeron investigaciones previas obtenidas de fuentes indexadas como Google Académico, SciELO, Dialnet, Scopus.

2.2 Métodos

Técnicas e instrumentos

El trabajo se desarrolló empleando una metodología cualitativa, que para Pérez et al. (2020) esta investigación es interpretativa, inductiva, multimetódica, reflexiva y flexible, en donde el propósito es descubrir lo nuevo y establecer teorías fundadas empíricamente (p. 171). El objeto de estudio son los sujetos, las personas, sus vidas y perspectivas subjetivas de un problema. Por ello, para efectuar la investigación cualitativa se tomó en cuenta que los fenómenos no se descubren, sino que se construyen, entendiendo la realidad como un todo y no busca postular leyes generales preexistentes, sino que tiene la finalidad de comprender los fenómenos sociales partiendo de algo particular. Es importante señalar que, para los autores, las técnicas más frecuentes que se utilizan en las investigaciones cualitativas son, las entrevistas, los grupos focales, la observación, estudio de casos, entre otros. Bajo este criterio, el trabajo desarrollado parte del estudio de la Sentencia 2064-14-EP de la Corte Constitucional del Ecuador.

Vale resaltar que para la recolección de datos en una investigación se emplea un conjunto de herramientas y técnicas utilizadas por el investigador. Para la recolección de información en el desarrollo de este estudio se empleó una técnica documental, por cuanto se revisó bibliografía relacionada con los temas abordados en la sentencia 2064-14-EP de la Corte Constitucional del Ecuador y la conducta de suplantación de identidad con contenido sexual en el contexto digital. Los documentos abordados fueron respecto a temas sobre el derecho a la privacidad, intimidad, datos personales, protección de datos personales, suplantación de identidad, teoría del delito, era digital.

Es importante resaltar lo que menciona Trejo (2021) respecto de la técnica documental o también denominada bibliográfica, que es aquella técnica que permite recabar datos contenidos en diversos tipos de documento, con carácter interpretativo, a través de esta técnica el investigados sintetiza y da a conocer un conocimiento producido con anterioridad (p.39). La importancia de esta técnica radica en el proceso de identificar, organizar, categorizar y analizar documentos que versan sobre un determinado objeto o fenómeno de estudio. Además, Trejo (2021) señala que esta técnica permite definir y precisar el objeto del estudio, así como establecer los objetivos del estudio y en algunos casos formular hipótesis y construir el marco teórico que sirve como soporte (p.40).

En este contexto, se utilizó documentos de materia judicial como sentencias de los tribunales de justicia tanto a nivel nacional como internacional, esto con la finalidad de conocer los comportamientos ilegales y la práctica social en el mundo digital en relación con el uso y protección de datos personales. Así también, se revisaron documentos académicos y teóricos cuyo objeto fue comprender la conducta de suplantación de identidad con contenido sexual en el contexto digital y la protección jurídica referente a los datos personales contenidos en el ordenamiento jurídico y desarrollados por la Corte Constitucional en sus fallos. En suma, la recolección de información en el trabajo se enfocó en la revisión de instrumentos físicos y digitales como libros, informes, revistas, artículos científicos, entre otros.

Se debe aclarar que la técnica y el instrumento si bien están relacionadas éstas poseen sus diferencias. Rojas (2023) explica que los instrumentos constituyen recursos necesarios para viabilizar las técnicas (p. 152). El instrumento utilizado dentro de esta investigación fue un formulario de 10 preguntas dirigidas a jueces y abogados que desempeñan sus funciones en materia penal y 5 preguntas enfocadas en conocer la percepción de fiscales respecto de la Sentencia 2064-14-EP de la Corte Constitucional y la conducta de suplantación de identidad con contenido sexual en el contexto digital, utilizado en una entrevista semiestructurada que ofrece un grado de flexibilidad y mantiene uniformidad para alcanzar el propósito de estudio. Desde el punto de vista de Rojas (2023) la entrevista es una técnica conversacional planificada por el entrevistador que se relaciona con el enfoque cualitativo y la investigación de campo (p. 154). Con el consentimiento de los entrevistados se utilizaron dispositivos de audio y video para registrar la información que el profesional experto menciona a la hora de la entrevista, esto con la finalidad de analizar detenidamente la consecución de la entrevista y sus respuestas.

Nivel de investigación

Explicativo: El nivel explicativo va más allá de la mera descripción de un objeto, es más avanzada en el sentido de que no solo busca evidenciar o recoger datos sobre un determinado estudio, sino que este busca explicar el porqué de un determinado problema. Para Vidal (2022) este tipo de investigación tiene su enfoque en identificar los hechos de la realidad para detectar las causas, busca conocer y modificar los efectos. Señala que es importante que el estudio de la variable dependiente se la realice mediante una tendencia o mapeo histórico para observar la conducta, retroceso o avance que permita identificar una posible causa que guíe una modificación de la realidad (p. 22).

En este contexto, la investigación se enfocó en establecer las causas y los efectos de la Sentencia 2064-14-EP de la Corte Constitucional del Ecuador que tenía en relación con los casos de suplantación de identidad con contenido sexual en el contexto digital. Se realizó el análisis de las causas que originaron el criterio de la Corte y los efectos que tiene para casos futuros en dónde se encuentran inmersos derechos constitucionales que por la evolución tecnológica trascienden el espacio físico. Se identificó la relación causal entre las dos variables de estudio, a través del nivel explicativo se analizó el efecto que la variable dependiente tiene sobre la independiente.

Modalidad de investigación

Métodos

Inductivo: Este método implica el análisis y determinación de características generales basadas en el estudio específico de un caso en concreto, inicia con la observación de un fenómeno o problema en particular y genera conocimiento general. Es decir, es un estudio parte de premisas particulares para establecer una conclusión de carácter general. De acuerdo con Lafuente y Martín (2008), a través de este método se crean enunciados generales a partir de la experiencia, observando un fenómeno y revisando fenómenos comparables con la finalidad de establecer leyes de carácter universal (p. 6). En el presente estudio se partió de un caso en particular, es decir de la Sentencia 2064-14-EP de la Corte Constitucional con la finalidad de analizar las reglas generales que se pueden aplicar a partir de este pronunciamiento emitido por la Corte. Además, con la información obtenida en la ejecución de las entrevistas que versó sobre el caso en particular, se buscó generar conocimiento general sobre el reconocimiento y tratamiento de datos personales y los derechos relacionados a la protección de datos personales, intimidad, privacidad en un contexto digital.

Analítico: El método analítico conforme Trejo (2021) tiene como fundamento el desatar, descomponer, desliar el fenómeno de estudio. Esta descomposición busca conocer los principios y elementos del problema, para así observar de manera secuencial las causas y los efectos (p 30). Cuando se descompone un problema por partes tiene como objeto investigar por separado cada elemento para posterior evaluar la relación que existe entre estos. Así, en el presente trabajo se estudiaron los componentes de la sentencia, los derechos a los cuales se refiere la Corte, además la conducta de suplantación de identidad con contenido sexual en el contexto digital se estudió desde una mirada de la teoría del delito, con la finalidad de analizar de forma individualizada los derechos en la era digital y la adecuación de la conducta a un tipo penal, para con ello, realizar una interrelación de las variables y comprender la problemática planteada.

Síntesis: A diferencia del método analítico, este busca reconstruir un todo, unir los elementos y estudiarlos de manera holística e integral. A criterio de Trejo (2021) una vez que se desarticula los componentes de un todo, es esencial recopilarlos con la finalidad de generar una comprensión de su totalidad y sus relaciones (p.31). Este método se caracteriza por la exposición metódica que se realiza de los elementos que son extraídos de un plano mayor para su posterior análisis. En este sentido, una vez que se estudia de forma individual los presupuestos contenidos en la Sentencia de la Corte Constitucional y se analiza de forma singular la conducta de suplantar la identidad con contenido sexual en el contexto digital, a través de este método se analizó de forma conjunta los elementos, con la finalidad de obtener conclusiones respecto de la influencia que tiene la sentencia en las decisiones de los juzgadores en materia penal.

Histórico: El objetivo principal de aplicar un método histórico es analizar el contexto del fenómeno social. En el ámbito jurídico, Martínez (2023) considera que este método forma parte de la comprensión de la evolución del Derecho como un fenómeno histórico social, de naturaleza subjetiva, compleja, dinámica y mutable (p.3). Dado que, con este método se busca estudiar los hechos del pasado para encontrar explicaciones causales al comportamiento de las sociedades actuales, este método de investigación es analítico-sintético. Es decir que, es fundamental descomponer los elementos del fenómeno estudiado a través del tiempo para reconstruirlo y explicar el hecho histórico.

En este trabajo se empleó el método histórico, toda vez que analizó de forma singularizada la evolución del reconocimiento y tratamiento de datos personales, la protección jurídica a través

del tiempo de los derechos a la privacidad, intimidad, protección de datos personales presupuestos contenidos en la sentencia, y la evolución del tipo penal de suplantación de identidad. Pues, el contexto digital ha hecho que derechos como la protección de datos personales, intimidad y privacidad queden en desamparo jurídico por su falta de regulación normativa. Para ello, se indagó en fuentes bibliográficas a fin de obtener información respecto de la evolución normativa que han tenido estos derechos.

Comparativo: El método comparativo en las ciencias jurídicas incide en el conocimiento del Derecho comparado, a juicio de Martínez (2023) busca contrastar puntos de coincidencia y diferencias específicas de las posiciones jurídicas de un sistema jurídico internacional (p. 3). La comparación tiene su fundamento inicial en la homogeneidad, pues se identifican identidad de elementos que legitiman la comparación, para ello, se necesita un análisis sistemático y riguroso que implique la observación de propiedades y atributos a ser comparados.

La aplicación de este método se empleó con la finalidad de comprender de manera global y regional la regulación normativa sobre los derechos esgrimidos en la Sentencia 2064-14-EP de la Corte Constitucional y la sanción a las conductas de suplantar la identidad con contenido sexual en un contexto digital. Se realizó un estudio comparativo entre el ordenamiento jurídico nacional y la normativa jurídica de La Unión Europea, España y Colombia con respecto de la reconocimiento y protección de datos personales y datos personales sensibles. Así también, se comparó con jurisprudencia colombiana los derechos de protección, privacidad, intimidad en el contexto digital. Por otro lado, se efectuó un análisis comparado de la tipificación del delito de suplantación de identidad cuando esta conducta es realizada con contenido sexual en el ámbito digital entre la legislación ecuatoriana y colombiana.

Población

La población es el conjunto de sujetos a la que se dirige la investigación denominada también como el universo de estudio. En el presente trabajo de investigación, se aplicaron siete entrevistas dirigidas a fiscales, jueces y abogados en libre ejercicio, los profesionales entrevistados fueron:

- Dra. Maricela Yánez - Agente fiscal de violencia de género del cantón Latacunga.
- Dra. Amparo Virginia Tasipanta Romero- Agente fiscal- multicompetente en el cantón Latacunga**.**
- Dr. Jorge Nagales- Asistente de Fiscalía en el cantón Latacunga.

- Verónica Altamirano Guerra- Asistente de Fiscalía en el cantón Latacunga.
- Dr. Christian Israel Rodríguez- Juez de Garantías Penales en el cantón Ambato.
- Dr. Fabián Altamirano - Juez de Garantías Penales en el cantón Ambato.
- Dr. Misael Rodríguez - Abogado en libre ejercicio.

CAPÍTULO III. - RESULTADOS Y DISCUSIÓN

Tabla 5: *Conducta de suplantación de identidad con contenido sexual.*

1. ¿En qué tipo penal se encuadra el uso indebido de datos personales sensibles, como fotos íntimas para suplantar la identidad de una persona, y cuáles son los criterios que guían esta clasificación en el contexto de la legislación ecuatoriana?		
PROFESIONAL ENTREVISTADO	**RESPUESTA**	**ANÁLISIS**
Dra. Maricela Yánez (Agente fiscal de violencia de género)	Esta conducta se encuadra en el delito de violación a la intimidad contenido en el artículo 178 del Código Orgánico Integral Penal, dentro de la sección Delitos contra el derecho a la intimidad personal y familiar, debido a que evidentemente el uso indebido de datos personales sensibles como fotos íntimas para suplantar la identidad de una persona en el	El Art. 178 del COIP determina que: La persona que, sin contar con el consentimiento o la autorización legal, acceda, intercepte, examine, retenga, grabe, reproduzca, difunda o publique datos personales, mensajes de datos, voz, audio y vídeo, objetos postales, información contenida en soportes informáticos, comunicaciones privadas o reservadas de otra persona por cualquier medio, será sancionada con pena privativa de libertad de uno a tres años. En este sentido, las fotos íntimas según la jurisprudencia constitucional son consideradas datos sensibles y el uso de estos datos en la era digital con la finalidad de suplantar la identidad es un fenómeno que ha crecido significativamente. El criterio que utiliza la Dra. Yánez se centra en el daño psicológico que produce esta conducta, a esto, es importante añadirle que la violación a la intimidad no solo

	contexto digital, causa un daño psicológico a la víctima.	afecta a la víctima individualmente, sino que también plantea un desafío para el sistema legal ecuatoriano. Es decir, la normativa jurídica debe abordar nuevas formas de delitos cibernéticos y garantizar una protección adecuada a los individuos. El criterio de la Dra. Yánez se enfoca únicamente en determinar el tipo penal con fundamento en el daño psicológico que recibe la víctima, sin embargo, debe considerarse aspectos como: **Naturaleza del dato:** Los datos sensibles son considerados vulnerables y su uso indebido conlleva a generar consecuencias más graves. **Medios utilizados:** La forma en la que se obtienen los datos influye en la gravedad del delito y en su investigación, puesto que la forma de obtener implica efectuar un tratamiento sobre el dato personal. La Corte Constitucional del Ecuador en la Sentencia 2064-14-EP/21 menciona que en principio el mero acceso puede considerarse como tratamiento de datos personales, pues puede consistir en una operación mental que se realiza sobre el dato, en dónde se visualiza el documento en el que se contiene el dato, así como implicaría realizar operaciones adicionales al acceso, como la descarga del dato. En este punto, le corresponde al juez analizar el caso concreto para determinar si el acceso constituye una forma de tratamiento. **Finalidad:** El uso de datos personales sensibles como fotografías íntimas con la finalidad de suplantar la identidad en el contexto digital debe ser considerada como una vulneración más grave para la imposición de una sanción penal.

Dra. Amparo Virginia Tasipanta Romero (Agente fiscal-multicompetente)	Considerado como un delito autónomo de acuerdo con las consecuencias y hechos específicos del caso. Se puede hablar de suplantación de identidad cuando una persona de forma física asume la identidad de otra, con la finalidad de financiarse de algo, a través de un documento legal, esta conducta está sancionada según el Art. 212 "Suplantación de identidad". Por otro lado, no existe el tipo penal de suplantar la identidad con contenido sexual, pero si puede encajar en otro tipo de delitos, se habla del delito de violación a la intimidad porque este tipo penal establece que cuando sin contar con el consentimiento o autorización	La Dra. Amparo Tasipanta que desenvuelve sus actividades laborales como fiscal multicompetente en el Cantón Latacunga realiza un análisis más profundo respecto de la conducta de usar datos personales sensibles como fotos íntimas con la finalidad de suplantar la identidad en el contexto digital. Su respuesta tiene un enfoque finalista, es decir que determina cual es el objetivo del uso de estos datos y de acuerdo con ello establece el tipo penal al que puede encajar la conducta. La entrevistada deja claro que la identidad de una persona solo puede ser física y los documentos que habilitan esa situación únicamente son aquellos que otorga una entidad pública, como la cédula de ciudadanía o la licencia para conducir, es decir, una persona suplanta la identidad de otra cuando se hace pasar por ella mediante el uso de un documento de identidad. La identidad es un derecho reconocido por la Constitución ecuatoriana, presupuesto que permite que un individuo se involucre en la sociedad. Tratadistas como Mead (1972) citado por Gómez y Ortíz (2012) consideran que la identidad es un proceso de construcción, en el que las personas se definen de forma simbólica (p.16). La identidad se compone de atributos, creencias, deseos y principios de una persona. Bajo estos criterios se puede aducir que la identidad adquiere doble sentido, por un lado, es una construcción social y por otro es un sentido de individualidad como fuente de respeto para sí mismo.

	legal, acceda, intercepte, examine, retenga, grabe, reproduzca, difunda o publique datos personales, mensajes de datos, voz, audio y video, soportes informáticos, comunicaciones privadas o reservadas de otra persona por cualquier medio, será sancionada con pena privativa de libertad de uno a tres años. Es uno de los delitos en los que puede encajar esa conducta. Pero sin vamos a una conducta que implica la comercialización de este material, tenemos como tipos penales como la Pornografía con utilización de niñas, niños o adolescentes; Comercialización de pornografía con utilización de niñas, niños o adolescentes, estos delitos son considerados graves debido a la naturaleza del delito que va en	Entonces, la doctora sostiene su clasificación del uso indebido de datos personales íntimos como una conducta punible que se subsume al tipo penal que amerite. En el caso de suplantar la identidad con contenido sexual, la doctora manifiesta que solo puede existir suplantación de identidad como un delito autónomo y cuando se usen documentos públicos de identidad para cometer tal acto. Ahora bien, Llaneza (2021) señala que desde el contexto digital se habla de una traslación de la identidad legal a los entornos digitales (p. 68). Esta traslación conlleva problemas para la seguridad jurídica, integridad de las operaciones, protección a la intimidad y los datos personales. La identidad digital en el ordenamiento jurídico ecuatoriano no está reconocida formalmente, sin embargo, esto no significa que no merezcan protección jurídica, pues está claro que el uso de identidad digital se relaciona con la protección de datos personales en la red y otros derechos como la intimidad, buen nombre, dignidad e imagen. En concordancia con esto, Llaneza (2021) deja claro que el surgimiento de las nuevas tecnologías y la forma del uso de datos personales por actores estatales y no estatales permite que el número de delitos y ataques cibernéticos se incremente (p. 71). Por ende, los sistemas de identificación deben poseer marcos legales regulatorios sólidos que integren un enfoque de privacidad y seguridad, a fin de garantizar la protección y control de los datos personales en la era digital. Sumado a esto, el autor sostiene que pese a que no exista un pago para la creación de la identidad digital y que esta se genere en ocasiones mediante un registro de datos

	contra de los NNA. El hostigamiento, violencia sexual. El tipo penal encuadra de acuerdo con la acción y consecuencia de la conducta. En definitiva, el delito es único, autónomo, la suplantación de identidad física y la violación a la intimidad.	falsos, inventados o erróneos esto no le quita sustantividad a una identidad que se genera mediante el comportamiento del individuo a los efectos de ser sujetos de derechos. Con todas estas consideraciones, discrepo de la respuesta emitida por la Doctora, sobre que solo puede existir una identidad física, pues como varios autores han mencionado, existe en la actualidad una identidad digital propensa a sufrir algún tipo de abuso, como es el caso de una suplantación de identidad digital, delito que no se encuentra contemplado en la normativa penal ecuatoriana. Ahora bien, la entrevistada contempla otro análisis cuando existe una conducta de suplantación de identidad que involucra contenido sexual, deja claro que, al utilizar contenido íntimo de una tercera persona, esta conducta es considerada como una violación a la intimidad, Baño y Reyes (2020) explican que con los avances tecnológicos el alcance jurídico del derecho a la intimidad personal y familiar se encuentran inoperantes en la práctica (p. 51). Esto debido a que con el uso de la tecnología y redes sociales los contraventores violan este derecho mediante el uso no autorizado de audios, videos, imágenes entre otros, circunstancia que atenta contra la imagen, buen nombre y honra de la víctima. En este caso, el criterio de la Dra. Amparo Tasipanta es muy acertado, ya que resalta que el derecho a la intimidad es vulnerado cuando un tercero sin autorización previa divulga información personal de la víctima y más aún si esta involucra contenido de la vida sexual. Partiendo de esta premisa, la suplantación de identidad con contenido sexual implica el uso no autorizado de fotografías, videos y/o audios íntimos que afectan

		la esfera íntima de la víctima. Según el Reglamento 2016/679 de la Unión Europea, está prohibido el tratamiento de datos personales que relativos a la vida sexual de una persona física (Art. 9.1). Entonces, queda claro que el hacer uso de datos personales de carácter sensible implica un tratamiento no autorizado del mismo, vulnera además la protección de datos personales garantizado y reconocido en la Constitución ecuatoriana. Por otro lado, la doctora realiza un análisis de esta conducta cuando la víctima es un niño, niña o adolescente. Esta conducta se tipifica en el Art. 103 como pornografía con la utilización de niñas, niños o adolescentes y es considerada más grave puesto que la víctima está dentro del grupo de atención prioritaria que establece la Constitución en su artículo 35. Art. 35.- Las personas adultas mayores, niñas, niños y adolescentes, mujeres embarazadas, personas con discapacidad, personas privadas de libertad y quienes adolezcan de enfermedades catastróficas o de alta complejidad, recibirán atención prioritaria y especializada en los ámbitos público y privado. La misma atención prioritaria recibirán las personas en situación de riesgo, las víctimas de violencia doméstica y sexual, maltrato infantil, desastres naturales o antropogénicos. El Estado prestará especial protección a las personas en condición de doble vulnerabilidad. Por otro lado, también hace alusión al delito de hostigamiento, tipificado en el artículo 145.2 del COIP, cuando una persona natural o jurídica molesta, perturba o

		angustia de forma insistente o reiterada a otra por sí misma o a través de cualquier medio tecnológico o digital con el objeto de causar daño físico o sexual. En las redes sociales usualmente este tipo de hostigamiento proviene de perfiles falsos quienes a través de mensajes insistentes perturban la tranquilidad de la víctima, pero esto no implica que se haga uso de datos personales sensibles, por ello, considero que si bien es cierto este delito involucra una afectación grave a la víctima y es ocasionado a través de medios tecnológicos, no implica un uso de datos personales que afecten a la intimidad o a la identidad como bienes jurídicos protegidos. Finalmente, la Fiscal ha establecido que esta conducta puede ser tratada desde una perspectiva de violencia sexual. El COIP establece que Art. 158.- Violencia sexual contra la mujer o miembros del núcleo familiar.- La persona que, como manifestación de violencia contra la mujer o un miembro del núcleo familiar, se imponga a otra y la obligue a tener relaciones sexuales u otras prácticas análogas, será sancionada con el máximo de las penas previstas en los delitos contra la integridad sexual y reproductiva, cuando se trate de niños, niñas y adolescentes, personas adultas mayores y personas con discapacidad. En este punto, debo enfatizar que, la conducta de suplantar la identidad con contenido sexual a través de herramientas de la inteligencia artificial como el *deepfake* tiene como principales víctimas a las mujeres, este criterio también lo comparte O´Halloran (2021) citado por Ramos (2024) quien sostiene que, este

		avance tecnológico permite la creación de imágenes y videos alterados que representan a individuos en contextos inapropiados, pero que principalmente este atentado se dirige hacia las mujeres (p. 368). Con estos presupuestos, es importante analizar la conducta desde una perspectiva de género tal como lo realiza la Dra. Tasipanta, quien expresamente mencionó *"las mujeres sufren doble vulnerabilidad en las redes, debido a que son vistas con obscenidad por los usuarios".*
Dr. Jorge Nagales (Asistente de Fiscalía)	Cuando eso ocurre nos vamos específicamente al tipo penal de Suplantación de Identidad contenido en el Art. 212 del COIP. Se inician las investigaciones pertinentes para saber de qué fuente se extrae la información que está circulando, dentro de fiscalía investigamos estas conductas con la ayuda del sistema especializado de investigación de medicina legal y ciencias forenses en la cual hace énfasis en la Policía Judicial (PJ).	El Doctor Nagales considera que esta conducta se encuadra en el tipo penal de suplantación de identidad contenido en el artículo 212 del COIP. Es importante señalar que, el entrevistado si reconoce la existencia de una identidad digital y por ende manifiesta que merece una protección jurídica adecuada y acorde a las circunstancias actuales en las que se desenvuelve la sociedad dentro de una era cada vez más digitalizada. La identidad digital permite que los usuarios se identifiquen dentro de la red y forma parte inescindible de la identidad personal de cada individuo desde un enfoque psicológico, social y moral, este presupuesto ya se estudió en el análisis anterior. Pero, es fundamental dilucidar que, la suplantación de identidad tiene varios fines, Borghello y Temperini (2012) menciona que la usurpación, robo o suplantación de identidad afecta el honor, reputación, trabajo, imagen, salud social y psicológica o actividades financieras y económicas de la víctima. Esta conducta está asociada al hecho de obtener información personal para efectuar algún tipo de perjuicio al titular de los datos. Más allá del perjuicio económico, social u otro que provoca esta conducta, la víctima tiene un daño

		psicológico producido como consecuencia de la pérdida de una parte de su vida. En relación con la suplantación de identidad que involucra contenido sexual la finalidad de esta conducta puede ser afectar la reputación, la honra y el buen nombre de la víctima. Cuando involucra contenido sexual se habla de una afectación a la parte más íntima de una persona, estos datos personales gozan de una protección especial según el ordenamiento jurídico de la Unión Europea, pues son considerados datos sensibles que pueden provocar discriminación y que reflejan la vida sexual de una persona. Claro está que, la conducta puede ser sancionada mediante el tipo penal contenido en el artículo 212 del COIP, pero si se toma en consideración la protección jurídica que merecen los datos sensibles que utiliza el infractor, la vulneración se efectúa al bien jurídico de la intimidad. En definitiva, estoy de acuerdo con el doctor con relación a que existe una identidad digital y que debe ser tutelada eficazmente por el ordenamiento jurídico, pero cuando esta conducta afecta a la intimidad es necesario reconocer el bien jurídico al que se atenta.
Verónica Altamirano Guerra (Asistente fiscal)	Al involucrar contenido sexual considerado datos de carácter sensible, se encuadra en el tipo penal de violación a la intimidad contenida en el articulo178 del COIP	Los datos considerados sensibles son una subcategoría de los datos personales. Peyrano (2002) argumenta que estos datos se refieren a las características físicas o morales de las personas y a los hechos de su vida privada o íntima, como hábitos personales, origen racial, ideologías y opiniones políticas, convicción religiosa, estado de salud y vida sexual (p. 514). Entonces, al forman parte de la esfera íntima de los individuos, estos datos tienen una protección especial y su tratamiento debe

		estar expresamente autorizado, debido a que el conocimiento público puede generar actos de perjuicio o discriminación. La protección especial que el ordenamiento jurídico otorga a estos datos es con la finalidad de proteger la intimidad y evitar discriminación hacia los titulares. En este caso, mi postura frente a la respuesta de la Dra. Verónica Altamirano es positiva, la conducta de suplantar la identidad mediante contenido sexual se debe adecuar al tipo penal de violación a la intimidad, por el material que se utiliza, es decir las fotos íntimas que revelan la vida sexual de su titular.
Comentario personal: De la realización de la entrevista se ha logrado determinar que 3 de los profesionales concuerdan en que la conducta de suplantar la identidad con contenido sexual en el contexto digital encaja en un delito de violación a la intimidad contenido en el artículo 178 del Código Orgánico Integral Penal, uno de ellos, explica que esta conducta se direcciona directamente al tipo penal de suplantación de identidad, contenido en el artículo 212 del COIP. En relación con esto, mi postura es concordante con los profesionales que señalan el tipo penal de violación a la intimidad, por cuanto según el Reglamento (UE) 2016/679 de la Unión Europea los datos que revelen información sobre la vida sexual de la persona son considerados datos personales sensibles, además en la sentencia 2064-14-EP/21 la Corte Constitucional del Ecuador, ha establecido que las fotografías de esta índole forman parte de lo más íntimo de la persona. En este sentido, la doctrina ha señalado que la intimidad es un derecho personalísimo e inherente al ser humano. Touriño (2014) considera que este derecho es irrenunciable, inalienable e imprescriptible y concede el poder a su titular para excluir a terceros de entrometerse en su esfera íntima y supone la existencia de un ámbito propio y reservado que le permite mantener una calidad mínima de la vida humana (p. 52). De ahí que, existe vulneración a este derecho cuando, por ejemplo, una tercera persona publica en una red social información personal que forma parte del círculo privado de otra, sin que haya consentimiento para ello. Similar situación ocurre cuando existe la difusión no consentida de videos o imágenes intimas de una persona, además este acto involucra una afectación al derecho a la propia imagen. De este supuesto, al analizar la conducta de suplantar la identidad con la utilización de contenido sexual en el ámbito		

digital encaja como una violación al delito a la intimidad, pues se hace uso arbitrario de datos sensibles, como lo han mencionado los entrevistados. Es menester señalar que, este derecho está reconocido tanto en la Constitución como en instrumentos internacionales como la Declaración Universal de los Derechos Humanos, en dónde se establece que,

> 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. (Art. 12)

En este sentido, el derecho a la intimidad es interdependiente a derechos como, la protección de datos personales, derecho a la imagen, derecho a la honra y reputación, entre otros. Esto implica que el sistema judicial debe actuar de forma efectiva y ágil en los casos de violación a la intimidad, los agentes fiscales juegan un papel fundamental a la hora de investigar este tipo de conductas, pues se enfrentan a obstáculos tecnológicos que dilatan la investigación. Vale aclarar que, de las respuestas emitidas por los profesionales se logra verificar que efectivamente el uso de datos personales íntimos para suplantar la identidad debe ser considerado como una violación a la intimidad.

Nota: Información obtenida de la entrevista desarrollada por la autora.

Tabla 6: *Evaluación del daño a la víctima en los casos de suplantación de identidad.*

2. **¿Qué criterios utilizan para evaluar el daño significativo a la víctima en casos de suplantación de identidad con contenido sexual, y cómo se aplica esta evaluación en el contexto digital?**		
PROFESIONAL ENTREVISTADO	**RESPUESTA**	**ANÁLISIS**
Dra. Maricela Yánez (Agente	En lo que respecta a las víctimas, como es una afectación a su intimidad se	En los casos de suplantación de identidad con contenido sexual, los cuatro profesionales mencionan que para evaluar el daño significativo que esta conducta le ocasiona a la víctima se realizan pericias psicológicas, psiquiátricas e informáticas, con la finalidad

fiscal de violencia de género)	considera el daño o trauma psicológico que provoca el uso de su información intima en el contexto sexual. En el contexto digital es igual, se analiza el daño psicológico que pueda tener la víctima, que en ocasiones incluso terminan en un daño psiquiátrico debido a las múltiples consecuencias que atentan a su dignidad humana, esto es honra, buen nombre e imagen.	de conocer el impacto que tuvo la divulgación de material íntimo de la víctima, la pericia informática tiene como fin analizar el grado de difusión que tuvo la publicación. En este punto, hay que dejar claro que, la suplantación de identidad con contenido sexual implica el uso de datos personales sensibles y por ende el infractor realiza un tratamiento sobre estos datos. Cuestiones que claro está son prohibidas en el ordenamiento jurídico, pues como ya se mencionó *ut supra,* se viola la intimidad. Esta violación en el contexto digital se caracteriza por ser un delito de naturaleza específica, es decir que la conducta es efectuada mediante el uso de Tecnologías de la Información y Comunicación y expone públicamente aspectos que forman parte de la vida privada y reservada de la víctima. Añadido a esto, implica una mayor gravedad en los casos de exposición de imágenes o videos con contenido sexual. Iricibar (2022) citado por Flores et al. (2024) estudia las consecuencias psicológicas y sexuales que produce la difusión de contenido sexual sin consentimiento, menciona que, las víctimas experimentan angustia emocional intensa, ansiedad, depresión e incluso ideas suicidas (p. 18). Por otro lado, García (2022) citado por Flores et al. (2024) establecen que, a nivel social, las víctimas enfrentan estigmatización y juicio de la sociedad, acoso cibernético (p. 18). Este tipo de conductas tienen una repercusión significativa en el proyecto de vida de la víctima. Pese a los esfuerzos normativos para proteger los datos personales en la era digital, estas conductas surgen a menudo principalmente en las redes sociales, en donde las personas cargan fotografías personales sin ningún tipo de restricción. Los principios establecidos en la LOPD tienen
Dra. Amparo Virginia Tasipanta Romero (Agente fiscal-multicompetente)	Se determina los daños psicológicos de la víctima con el informe pericial y cuando hay un daño significativamente grave, se lo realiza a través de un examen psiquiátrico. Por lo general los informes	

	psiquiátricos se lo realizan a los NNA, porque tienen afectación a su psiquis. Aún más cuando la conducta es reiterada la victima adquiere un carácter de normalización.	por objeto asegurar que el tratamiento de datos personales se desarrolle de forma legítima, respetando derechos y libertados de los individuos titulares de los datos. En este sentido, la Dra. Verónica Altamirano enfatiza en la necesidad de llevar a cabo una pericia informática a fin de conocer el impacto o grado de difusión que tuvo la publicación del contenido íntimo, pues cuando una persona suplanta la identidad en una red social, no solo se adueña de datos personales ajenos, sino que actúa como el titular de los datos, es decir, interactúa en la red, comparte, publica y/o hace visibles datos sensibles correspondientes a la vida sexual de la víctima.
Dr. Jorge Nagales (Asistente de Fiscalía)	Con respecto a los criterios prácticamente lo analizaría el juez al emitir la sentencia teniendo en cuenta las consideraciones de la víctima, para ordenar la reparación integral. La reparación que el juez puede otorgar a la víctima puede ser simbólicas o no simbólicas, la restitución del derecho, la garantía de no repetición. Sin embargo, se evalúa el daño psicológico que puede llegar a tener la víctima a	Los profesionales resaltan la importancia de las pericias psicológicas para conocer el grado de afectación que tuvo en la víctima, esto porque en las redes sociales una persona posee una identidad, interactúa y mantiene una vida digital, es decir, involucra derechos como, la imagen, buen nombre y honra. Estos derechos son interdependientes entre sí y se vinculan a la vida digna. La conducta de suplantar la identidad mediante el uso de contenido sexual afecta a las víctimas en el estado psicológico y social, más aún cuando a través de la manipulación digital y con la aplicación de inteligencia artificial se crea contenido falso y convincente que muestra a una persona participando en actividades sexuales. Es necesario estudiar los derechos que afectan esta conducta, para así comprender el grado de afectación psicológica que puede llegar a producir en la víctima. Los derechos al honor, intimidad y propia imagen son propensos de ser vulnerados con el avance tecnológico, puesto que se evidencia una brecha en su protección eficaz.

	través de la UAPI (Unidad de Atención Pericial Integral) de la fiscalía, que disponga un psicólogo/a que realice una evaluación, que serviría al momento de dictar una sentencia y ordenar la reparación integral.	**- Derecho al honor:** Este derecho protege la dignidad y reputación de los individuos frente a los actos que pueden desmerecerlo en la sociedad, su principal objetivo es preservar la dignidad humana. La Constitución ecuatoriana prevé que, todas las personas tienen "derecho al honor y al buen nombre. La ley protegerá la imagen y la voz de la persona" (Art. 66.18). Al respecto, Casquete (2023) indica que este derecho se entiende como "la opinión y el respeto que otros sienten y manifiestan hacia la propia persona, y por tanto debe entenderse que recoge tanto la autoestima, como la reputación" (p. 9), además, evoluciona y se modifica de acuerdo con el cambio social. Este derecho es considerado personalísimo y protege al individuo tanto en la esfera pública como privada. En el derecho europeo, el honor tiene dos aristas, el sentido objetivo entendido como la reputación de las personas, y el sentido subjetivo que involucra la autoestima. Mientras que la jurisprudencia constitucional ecuatoriana en la Sentencia No. 2064-14-EP/21 considera que posee una dimensión interna que atañe a la autoestima y honra de las personas, y una dimensión externa objetiva que refiere al buen nombre o reputación de la persona (párr. 196). El ordenamiento jurídico penal del Ecuador tipifica las conductas que atentan contra los derechos al honor y buen nombre, expresamente sanciona el delito de calumnia con una pena privativa de libertad de seis meses a dos años. La suplantación de identidad con contenido sexual puede dañar la reputación de la víctima e influir en la vida personal y profesional, sin la necesidad de que exista la imputación falsa del cometimiento de un
Verónica Altamirano Guerra (Asistente fiscal)	Pericia informática que involucra la revisión del material pornográfico y la Pericia psicológica que sirve para la valoración a la víctima.	
Dr. Christian Israel Rodríguez Juez de Garantías Penales en el cantón Ambato	Depende mucho de la prueba que presentan en cada caso concreto, para así determinar el grado de influencia y el grado de daño que pudo tener la víctima, entre este daño se habla de:	

	- Afectación psicológica, económica, familiar. - Se daña el proyecto de vida, si debido a ese acto se ve en riesgo las cuestiones personales de la víctima.	delito como lo menciona el COIP. En correlación con esto, la Corte Constitucional del Ecuador a través de la sentencia No. 048-13-SEP-CC ha determinado que: El derecho al honor alude, desde una vertiente personal, a la conciencia que uno tiene de su propia dignidad moral, a la autoestima. Desde una perspectiva social el derecho al honor sería la imagen que los demás tienen de nosotros, esto es, la reputación, buen nombre o fama que uno tiene ante los demás. La violación de este derecho al honor ocurre cuando públicamente se imputa a una persona hechos falsos que menoscaban su reputación o atentan contra su autoestima. (p. 9) Es así como, la vulneración de este derecho también afecta al buen nombre y limita el ejercicio de otras libertades, su protección jurídica es de índole tanto constitucional, civil y penal. **- Derecho a la imagen:** Con la aparición de las redes sociales la imagen a alcanzado un doble plano, uno personal y espiritual, y otro patrimonial y económico. La Corte Constitucional ecuatoriana en la Sentencia No. 2064-14-EP/21 ha señalado que este derecho "presupone el derecho de todo individuo al manejo de su propia imagen, misma que se materializa gráficamente, por ejemplo, por medio de una fotografía o video" (párr. 205). En esta misma línea Casquete (2023) destaca que, el derecho a la propia imagen establece límites legítimos para la obtención y explotación de la imagen de las personas (p. 12). Esto toda vez que, faculta al titular a decidir sobre qué información
Dr. Fabián Altamirano **Juez de Garantías Penales en el cantón Ambato**	Se analiza el alcance de la publicación, el nivel de exposición que tiene la persona en redes sociales, porque existen personas que llegan a una mayor cantidad de seguidores vs una persona que tiene menos cantidad de seguidores. Cuando existe una venta del contenido sexual también existe otro tipo de daño. Además, se observa el daño psicológico.	

Dr. Misael Rodríguez **Abogado en libre ejercicio**	Principalmente se evalúa el daño psicológico, emocional y la afectación al proyecto de vida de la víctima. Siempre a través de pericias psicológicas que ayuden a determinar ese nexo causal entre la conducta y la consecuencia del daño.	que posee sus rasgos físicos puede ser difundida de manera pública y la capacidad para impedir su captación, reproducción o publicación de terceros. En consecuencia, goza de protección constitucional y su vulneración es sancionada penalmente, para ello, el COIP contempla en el inciso segundo del artículo 179 que, > Será sancionada con pena privativa de libertad de uno a tres años quien revele o divulgue a terceros contenido digital, mensajes, correos, imágenes, audios o vídeos o cualquier otro contenido íntimo de carácter sexual de una persona en contra de su voluntad. (Art. 179) En este caso, se habla de una divulgación de imágenes íntimas sin el consentimiento de su titular, pero la suplantación de identidad con dicho contenido implica una afectación más grave a la víctima, puesto que se ejecuta con la utilización de datos de carácter sensible que atentan contra su dignidad, intimidad, buen nombre, imagen y honor. Circunstancia que genera consecuencias negativas psicológicas y sociales.
Comentario personal: Frente a la argumentación esgrimida por los profesionales en esta pregunta, estoy de acuerdo. Desde una perspectiva personal esta conducta afecta a la privacidad, intimidad y dignidad de las personas, dejando graves secuelas psicológicas en su entorno personal, familiar y social. Las redes sociales al ser plataformas digitales de alto impacto social, puede convertirse en un escenario de abuso, pues cuando alguien se ve obligado a enfrentar la difusión no consentida de contenido sexual bajo su nombre el impacto psicológico afecta a su autoestima y a sus relaciones sociales, familiares, educativas o laborales. Sobre todo, cuando el estigma social hace que la víctima sea revictimizada en su entorno. Por ello, considero que la suplantación de identidad con contenido sexual debe ser visto más allá de un delito común, puesto que es una evidente violación a la salud mental y emocional de las personas. Por ello, sostengo que es útil, pertinente y conducente el efectuar pericias psicológicas a las víctimas. Además, debo destacar la importancia de llevar a cabo una pericia informática tal como lo ha mencionado la Dra.		

Altamirano, ya que con ello se puede evidencia el nivel de difusión del material íntimo de la víctima, para así poder asociarlo con la afectación psicológica que genera.

Nota: Información obtenida de la entrevista desarrollada por la autora.

Tabla 7: *Procedimientos específicos para recabar evidencias.*

3. **¿Qué procedimientos específicos sigue para recabar evidencias en casos de suplantación de identidad con contenido sexual en el entorno digital, y qué desafíos se presentan?**		
PROFESIONAL ENTREVISTADO	**RESPUESTA**	**ANÁLISIS**
Dra. Maricela Yánez (Agente fiscal de violencia de género)	A través de una pericia informática se establece el IP de dónde se produjo la publicación de este tipo de fotografías o información considerada de carácter restringido y que evidentemente viola el derecho a la intimidad de la persona. Ahora bien, con un énfasis en los casos que las víctimas son ***NNA*** sin excluir a las personas adultas. Otro procedimiento utilizado por fiscalía es el testimonio anticipado de la víctima, versiones de los usuarios	La CRE ha previsto que el Estado a través de la fiscalía general es el titular de la acción penal pública. Este ente tiene por objeto investigar el cometimiento de las conductas penalmente relevante. Este proceso de investigación le permite establecer la materialidad de los hechos y de hallar mérito acusar a los presuntos infractores ante el juez (Art. 194). Es decir, los fiscales tienen el deber de dirigir la investigación preprocesal y procesal penal, con sujeción en lo previsto en el ordenamiento jurídico. Con este preámbulo, se debe resaltar que los cuatro entrevistados concuerdan en que el principal procedimiento que utilizan para recabar evidencias en los casos de suplantación de identidad con contenido sexual en el ámbito digital es la pericia informática. Desde la posición de Gallardo (2023) la pericia informática es el estudio e investigación

	que recibieron las fotografías digitales que son obligados a denunciar y de no hacerlo forman parte de la distribución ilícita de este material. Los desafíos a los que nos enfrentamos principalmente es la falta de celeridad en cuanto a establecer reconocimiento de las IP que generalmente tardan, toda vez que los equipos tecnológicos existen en determinadas jurisdicciones (Quito, Guayaquil y Cuenca)	realizado por un experto en el campo, que se orienta a la obtención de una prueba o evidencia electrónica (p.90). El perito se encarga de efectuar un informe pericial informático con un análisis técnico que logre determinar hechos complejos, integra de forma ordenada, estructurada y agrupara la información obtenida en la pericia. Los entrevistados han explicado que esta pericia tiene por objeto obtener la IP de la publicación, en este punto, la Dra. Altamirano enfatiza que este procedimiento técnico se lo lleva a cabo cuando la publicación es a través de una red social, puesto que la tecnología ha dejado de ser un elemento accesorio y se ha posesionado como un elemento necesario paras las interrelaciones personales, sociales y comerciales. En consecuencia, esta herramienta de la tecnología contribuye a la rápida difusión del material íntimo obtenido sin permiso o robadas de dispositivos electrónicos, además aumenta el impacto y la visibilidad de este material al momento de compartir, reenviar o publicar en entornos digitales. Por ello, esta pericia permite conocer de dónde proviene dicha publicación, con la finalidad de determinar al autor de la conducta. Por otro lado, la Dra. Altamirano explica que el procedimiento para recabar evidencias en este tipo de casos depende del medio en el que esté contenido el material íntimo, sea este un CD, un aparato tecnológico
Dra. Amparo Virginia Tasipanta Romero (Agente fiscal- multicompetente)	Se lo realiza a través de una pericia informática con cooperación internacional, porque el ecuador no posee esas pericias, solo se lo hace a través de un informa de ciberdelitos. Esto lo manejan con la asistencia penal internacional. Los IP´s se lo obtiene a través de una pericia informática. Los desafíos a los que se	

	enfrentan es que en el caso del Ecuador no existe la tecnología necesaria y se solicita ayuda internacional, la demora es un tiempo prudencial.	como un teléfono móvil o en una red social. Además, aclara que la información se extrae con una pericia informática. El ciberdelito se caracteriza por la complejidad de investigación, sin embargo, es necesario que los actos cometidos a través de la tecnología sean identificados, desde su origen, sus causas, motivaciones y actores. De tal manera que, Salazar (2021) sostiene que, "la idoneidad del derecho penal es de gran importancia para el enjuiciamiento del delito cibernético, ya sea nacional o internacional" (p.10). Frente a esto, es evidente que el ciberdelito es una eminente amenaza que presenta desafíos para el derecho penal y el sistema de justicia en general. De ahí que para los entrevistados el principal desafío que enfrentan a la hora de investigar esta conducta es, la falta de peritos especializados en la materia de informática, así también, el Dr. Nagales ha expuesto que un desafío adicional es que los peritos no se encuentran lo suficientemente capacitados, y en ocasiones vulneran la cadena de custodia y no mantienen la integridad del contenido que se extrae, dando como consecuencia que se alegue la falta de autenticidad del material extraído. Frente a esto, Salazar (2021) expresa que la Fiscalía General del Estado (FGE) en coordinación con las unidades investigativas desarrollan programas de capacitación y formación enfocado en delitos cibernéticos, programas que han sido auspiciados por organismos internaciones como
Dr. Jorge Nagales (Asistente de Fiscalía)	A la hora de investigar estos hechos, lo primero que se debe hacer dependiendo del tipo penal y como se habla de un ámbito sexual en la suplantación de identidad cuando están involucrados menores se envía al UNCIS (Unidad de Investigación contra la Integridad Sexual) que tratan justamente temas de carácter sexual. En delitos informáticos de la misma manera, cuando está circulando contenido sexual en una página pornográfica o se encontró en alguna computadora personal, lo primero que se hace es extraer la información y	

	materializan dicha información y de eso se encargan los peritos de criminalística. También los peritos informáticos pueden detectar URLS para evidenciar el direccionamiento, ósea la casa específica donde se guarda el contenido sexual. Los desafíos que se presentan a la hora de recabar las evidencias en el ámbito digital es que muchas veces los peritos vulneran la cadena de custodia, no mantienen la integridad de lo que se extrae y muchas veces eso ha hecho que se caigan muchos procesos, porque los abogados alegan que lo extraído no es auténtico, los peritos no logran verificar la autenticidad de lo que se descargan.	el Departamento de Estado, el Servicio de Pesca y Vida Silvestre de Estados Unidos, la Oficina de las Naciones Unidad contra la Droga y el Delito, y por instituciones nacionales como la Dirección Nacional de Ciberdelitos de la Policía Nacional. Posada (2021) destaca la necesidad de promover una adecuada y eficaz investigación, judicialización y sanción de los delitos cometidos en la era tecnológica, con el fin de prevenir su comisión futura y proteger la seguridad de la información cargada en la red (p. 19). La adecuada investigación, judicialización y sanción de este tipo de delitos busca proteger la disponibilidad, tratamiento, integridad y confidencialidad de los datos. A fin de garantizar una investigación que respete el marco jurídico ecuatoriano y permita recopilar las evidencias necesarias dentro de la investigación, la Dra. Amparo Tasipanta ha explicado que es importante la cooperación internacional. A este efecto, Posada (2021) argumenta que el Convenio sobre la Ciberdelincuencia de Budapest delimita los aspectos esenciales para la cooperación entre los Estados con el fin de combatir la ciberdelincuencia y proteger los bienes jurídicos en el campo de las tecnologías de la información (p. 12). Este instrumento internacional enfatiza en tres aspectos esenciales, medidas legislativas sustantivas, legislación procesal adecuada y cooperación internacional y regional en el ámbito de los ciberdelitos. La cooperación internacional surge debido
Verónica Altamirano Guerra (Asistente fiscal)	Los procedimientos que utiliza fiscalía para investigar estos casos son:	

	1. Cuando se tiene los videos se realiza únicamente la pericia y para ello se obtener en CD la información para realizar la pericia. 2. Cuando se obtiene desde el celular se realiza la extracción de información a través de una pericia informática, siempre y cuando no estén bloqueados, cuando están bloqueados es otro procedimiento. 3. Cuando el contenido sexual proviene de una red social se obtiene mediante un perito informático para obtener el IP, cuando la plataforma es pública. Por ejemplo, cuando están en tik tok y la red social es abierta al público, se ingresa con el link que se	a la falta de especialización en el Ecuador, la entrevistada que habló sobre este aspecto, menciona que el tiempo de espera es prudencial, no es ágil pero tampoco tarda mucho. Considero personalmente que estos delitos deben ser tratados de forma inmediata evitando la revictimización de la víctima en la investigación y garantizando un acompañamiento psicológico durante el proceso penal. Ahora bien, a más de las cuestiones esgrimidas *ut supra* la Dra. Yánez considera que es necesario la implementación del testimonio anticipado de la víctima y la toma de versiones de los usuarios que tuvieron acceso a los datos sensibles. El testimonio anticipado para Yanes (2021) es comúnmente usado en los delitos de naturaleza sexual (p. 5). Por otro lado, Buitrago (2004) sostiene que constituye un medio de prueba que puede ser realizada en una etapa anterior a la audiencia de juicio (p. 133). Generalmente, el testimonio anticipado en delitos de naturaleza sexual es utilizado cuando la víctima son Niños, Niñas o Adolescentes, bajo la fundamentación jurídica de proteger a la víctima de situaciones traumáticas dentro del proceso y en el principio de interés superior del niño. El COIP en el artículo 502 ha determinado las reglas generales para que el juzgador pueda recibir como prueba anticipada los testimonios. Así, establece que las causas para rendir testimonio anticipado son:

	envía y esa información se la baja en CD y de ahí se pide la autorización al juez y se obtiene la materialización. El principal desafío para esta investigación es la falta de peritos especializados, pues existen solamente 2 en Ambato, en Quito varios. Depende también de que plataforma se vaya a usar. Otro desafío es cuando se presentan fotos borrosas.	• Personas gravemente enfermas. • Físicamente imposibilitadas. • Personas que van a salir del país. • Víctimas o testigos protegidos. • Informantes. • Agentes encubiertos. • Todas aquellas personas que demuestren la imposibilidad de asistir a la audiencia de juicio. Las víctimas de los casos de suplantación de identidad con contenido sexual en las redes digitales pueden ser niñas, niños, adolescentes, jóvenes hombres y mujeres que navegan en la red. Por el nivel de exposición y por el material implícito, los NNA tienen la posibilidad de solicitar rendir el testimonio anticipado con la finalidad de evitar afectaciones psicológicas dentro del proceso penal. Por su parte, las personas adultas que han sido víctimas de esta conducta deben ajustar su situación a una de las causales que determina el COIP. Es importante que este presupuesto se ajuste a los derechos contemplados en el Art. 76 de la Constitución, esto es, el debido proceso, garantizando el derecho a la defensa, contradicción, inmediación e imparcialidad. Finalmente, se ha señalado que a través de la toma de versiones se recaban evidencias para determinar la conducta punible. Estas versiones

		son tomadas a las personas que reciben las fotografías, videos u otro material íntimo de la víctima. Es fundamental señalar que, el o la fiscal tiene la facultad de "Recibir las versiones de la víctima y de las personas que presenciaron los hechos o de aquellas a quienes les conste algún dato sobre el hecho o sus autores" (Art. 444.6). La finalidad de este mecanismo es conocer los hechos controvertidos, recabar información sobre la circunstancia de los hechos y autores. Otra entidad que se vincula al proceso de investigación con la Fiscalía en este tipo de casos es la Dirección Nacional de Investigación de la Policía Nacional, este organismo tiene como misión investigar los delitos de ejercicio de la acción penal pública, con la utilización de técnicas especializadas con apego al ordenamiento jurídico. La integridad de las investigaciones en los delitos informáticos debe vincularse a la administración de justicia, respeto a la dignidad y derechos de las personas, buscando establecer los elementos de convicción para evitar que este tipo de conductas quede en la impunidad.
Comentario personal: Los argumentos tomados en cuenta por los profesionales son muy acertados. En la era digital las conductas que afectan a los bienes jurídicos protegidos especialmente a la intimidad deben ser investigados mediante la aplicación de la ingeniería social. Tomando en cuenta que, la tecnología ha transformado las interacciones sociales y a consecuencia de esto, se ha convertido en un medio idóneo para la difusión acelerada de material íntimo sin el consentimiento de su titular, como efecto de la exposición constante de datos personales en las redes digitales. La FGE juega un papel fundamental en la investigación de estos actos ilícitos. Los agentes fiscales encargados del impulso de la acción de ejercicio		

público coordinan con instituciones de investigación como la Policía Judicial, Peritos Informáticos e incluso solicitan Apoyo Internacional. Sin embargo, la falta de peritos especializados en informática es un punto crítico a lo que apuntan los entrevistados, situación que pone en evidencia la necesidad urgente de capacitación y formación en el ámbito cibernético. La poca celeridad que ofrecen los procedimientos investigativos a través de las pericias informáticas puede dejar en la impunidad estas conductas. Por ello, pienso que es esencial recabar evidencias a través de otros procedimientos como el testimonio anticipado, que es una medida que busca proteger a las víctimas, especialmente cuando son menores de edad; de afectaciones psicológicas durante el proceso judicial, de manera que se equilibre la justicia con la dignidad y los derechos de las víctimas. Así también, el empleo de la toma de versiones de personas que evidenciaron el contenido íntimo en las redes es trascendental para conocer la materialidad de la infracción y posiblemente establecer al infractor y las circunstancias del hecho. Es decir, el abordaje integral propuesto por los entrevistados busca enfrentar los desafíos que plantea las conductas reprochables penalmente en el entorno digital. Es necesario adoptar un enfoque multidisciplinario que combine aspectos legales, tecnológicos y psicológicos para garantizar una efectiva tutela judicial, prevenir la comisión de futuros delitos y proteger a las víctimas que han sufrido el daño por estas conductas delictivas.

Nota: Información obtenida de la entrevista desarrollada por la autora.

Tabla 8: *Influencia de la Sentencia N° 2064-14-EP/21*

4. **¿De qué manera la Sentencia N° 2064-14-EP/21 de la Corte Constitucional podría influir en la determinación de sanciones en los casos de suplantación de identidad con contenido sexual?**		
PROFESIONAL ENTREVISTADO	**RESPUESTA**	**ANÁLISIS**

Dra. Maricela Yánez (Agente fiscal de violencia de género)	Influye significativamente en estos casos que existen violaciones de derechos, ya que establece de forma detallada el contenido de los derechos que pueden llegar a vulnerarse en este tipo de conductas, aún más cuando se da en el contexto digital. En la sentencia se desarrollan criterios jurídicos en torno al reconocimiento del alcance de ciertos derechos en el ámbito digital (datos personales, intimidad, protección de datos personales, tratamiento de datos). Además, podría vincularse a un mejor tratamiento, eficaz dentro de las resoluciones en las cuales se emitan sentencias condenatorias, así como en la reparación integral de las víctimas.	La era tecnológica, el internet y las nuevas tecnologías ha provocado un cambio significativo en las relaciones sociales de comunicación, la normativa y la jurisprudencia nacional no responde eficazmente a la nueva necesidad de protección de derechos en el contexto digital. La Sentencia 2064-14-EP/21 de la Corte Constitucional ecuatoriana evidencia un avance en cuanto a la protección de datos personales y en específico de datos de carácter sensibles contenidos en redes digitales que usualmente utilizan los individuos para compartir, recibir, enviar información personal o no. Aspectos que los entrevistados han concordado por unanimidad, pues han sentado la importancia de lo establecido por la CC en referencia a los criterios jurídicos sobre el alcance, componentes y protección de los datos personales. A criterio de Arce (2022) esta sentencia constitucional es trascendental para crear precedente jurisprudencial, esto debido a que aborda categorías jurídicas susceptibles de ser vulneradas por un indebido tratamiento de datos personales (p. 89). Sin duda, los argumentos de la Corte fijan ciertos avances claves para la protección de datos personales, datos personales sensibles y sus derechos conexos.

Dra. Amparo Virginia Tasipanta Romero (Agente fiscal-multicompetente)	La Sentencia N° 2064-14-EP de la Corte Constitucional de Ecuador tiene un impacto significativo en la determinación de sanciones en casos de suplantación de identidad que involucran contenido sexual. Esta sentencia establece criterios claros sobre la protección de datos personales y el derecho a la intimidad, lo que puede influir en la forma en que se abordan estos delitos en el ámbito penal.	Este hecho se evidencia en la promulgación de la Ley Orgánica de Protección de Datos Personales, normativa que recoge la línea jurisprudencial desarrollada en la sentencia. La nueva realidad digital provoca que los datos personales contenidos en archivos digitales estén propensos a ser tratados de una forma indebida, sin el consentimiento de su titular y con fines delictivos. La principal razón por la cual se vulneran datos personales a través de plataformas digitales como los derechos a la honra, buen nombre, imagen, entre otros, es debido a la facilidad de acceso a internet, creación de páginas web, redes sociales y otros; espacios en donde se puede publicar información personal de terceros sin su consentimiento.
Dr. Jorge Nagales (Asistente de Fiscalía)	La Corte ha enfatizado que las fotografías íntimas y otros datos sensibles son parte del derecho a la intimidad, lo que implica que cualquier violación de este derecho, como la suplantación de identidad con contenido sexual, debe ser tratada con especial atención. Esto sugiere que las sanciones deben ser	Ahora bien, el Dr. Nagales manifiesta que las fotografías íntimas y otros datos sensibles son parte del derecho a la intimidad, los jueces constitucionales a través de la sentencia tutelan de una forma más amplia su respeto en el entorno digital. Hoy en día, tomarse fotografías íntimas y compartirlas con la pareja sentimental se ha convertido en una actividad frecuente entre jóvenes que utilizan redes sociales, sin embargo, cuando este tipo de datos sensibles son publicadas en plataformas digitales de acceso público con un grado significativo de alcance, los derechos

	severas y proporcionales al daño causado a la víctima, considerando la naturaleza sensible del contenido involucrado.	vinculados a la intimidad son gravemente afectados. Los entrevistados han resaltado la adecuada motivación que los jueces realizan en la sentencia, pues, incluyen doctrina, jurisprudencia del Tribunal Constitucional de la Unión Europea y la Corte Constitucional de Colombia; y normativa comparada de países que poseen legislaciones avanzadas sobre el derecho a la protección de datos personales. En esta línea, Arce (2022) considera que la Corte Constitucional "interpretó normas jurídicas nacionales a partir del contexto normativo; logrando así la coexistencia, correspondencia y armonía de los precedentes jurisprudenciales para que vayan acorde a la normativa vigente y sobre todo sean constitucionalmente válidos y aplicables" (p. 92).
Verónica Altamirano Guerra (Asistente fiscal)	La Corte también ha abordado el tema de la reparación integral para las víctimas de violaciones a sus derechos. Esto implica que, además de las sanciones penales, se debe considerar un mecanismo para restituir los derechos vulnerados y compensar el daño sufrido por las víctimas. En casos de suplantación de identidad con contenido sexual, esto puede incluir medidas específicas como la eliminación del contenido difamatorio y compensaciones económicas.	La Corte Constitucional ha determinado el carácter imperativo al momento de argumentar y justificar una decisión de poder jurisdiccional, sobre la constatación de vulneraciones a los derechos constitucionales. Por ende, señala que en el caso que es materia de análisis, existe una inapropiada tutela de los derechos constitucionales, hecho que permite activar su capacidad legal para emitir un análisis de mérito. El control de mérito conforme Villagómez et al. (2022) tiene por objeto verificar la transgresión de derechos constitucionales en el proceso originario (p.102).

		En efecto, este control permitió que la corte desarrolle un amplio abordaje jurídico de los derechos constitucionales en el entorno digital. Este caso fue calificado de relevancia, precisando que en la actualidad el internet y medios digitales se han posesionado como instituciones de grande impacto que involucran una falta de protección jurídica que todavía el ordenamiento jurídico y la jurisprudencia no ha desarrollado.
Comentario personal: La sociedad se encuentra en constante evolución, el avance acelerado que ha tenido la tecnología en los últimos años hace que el comportamiento del ser humano se adapte a las nuevas realidades, por lo tanto, el derecho debe estar a la par de esta dinámica social, es esencial que los legisladores y el sistema judicial ajuste las instituciones jurídicas con el fin de proteger los derechos. Si bien es cierto, la sentencia *in examine* ha constituido un gran avance en el reconocimiento de derechos que surgen en las redes digitales, además que el análisis constitucional y crítico desarrollado es adecuado e idóneo para la protección de datos personales sensibles, a criterio personal, la resolución deja aún cuestiones por resolver, como la reparación integral que las víctimas deben recibir cuando por el indebido tratamiento de sus datos personales sensibles han sido afectadas psicológicamente a nivel personal, social, educativo o laboral. Asimismo, considero que la Sentencia constituye una guía integral para enfrentar los desafíos que en la actualidad surgen en torno al uso, tratamiento y transmisión de datos personales en redes digitales.		

Nota: Información obtenida de la entrevista desarrollada por la autora.

Tabla 9: *Tipificación de la conducta de suplantar la identidad con contenido sexual en el contexto digital.*

5. **¿Considera necesaria la tipificación de la conducta de suplantar la identidad con contenido sexual en el contexto digital? Y de serlo ¿En qué sección debería ser incluido el tipo penal?**		
PROFESIONAL ENTREVISTADO	**RESPUESTA**	**ANÁLISIS**
Dra. Maricela Yánez (Agente fiscal de violencia de género)	Si, al ser una agresión de tipo sexual debería tratarse como una violencia de género dado que se está vulnerando el derecho a la libertad sexual, tratándose de personas adultas y segundo porque el daño psicológico en el desarrollo psicosexual de la víctima le afecta en ese ámbito. Sin embargo, esta conducta puede adecuarse al tipo penal de violación a la intimidad.	En este punto, de los siete profesionales entrevistados dos sostienen que es necesario tipificar la conducta de suplantar la identidad con contenido sexual, uno de ellos considera que no es necesario, puesto que, únicamente debería realizarse un análisis del caso para adecuar al tipo penal correspondiente. Mientras que cuatro de ellos han considerado que es necesario una modificación en el delito de violación a la intimidad. Del contenido de las entrevistas se desprende que los profesionales enfocan a esta conducta como un delito contra la identidad o un delito contra la intimidad.
Dra. Amparo Virginia Tasipanta Romero (Agente fiscal-multicompetente)	No, únicamente sugiere que sea analizada la conducta para ir adecuando al tipo penal. Si suplantan la identidad se sanciona como lo establece el COIP en el artículo 172, en el caso de la utilización de material sexual	Para efectuar el análisis correspondiente es preciso señalar que el Art. 212 contempla el delito de suplantación a la identidad como un delito autónomo, establece una sanción con pena privativa de libertad de uno a tres años.

	considero que puede adecuarse al tipo penal de violación a la intimidad, comercialización o pornografía infantil.	**Art. 212 Suplantación de identidad. -** La persona que de cualquier forma suplante la identidad de otra para obtener un beneficio para sí o para un tercero, en perjuicio de una persona, será sancionada con pena privativa de libertad de uno a tres años. ***Elementos objetivos del tipo penal*** ***Sujeto activo:*** El artículo establece que el sujeto activo es cualquier persona. ***Sujeto pasivo:*** Se considera sujeto pasivo al dueño del bien jurídico protegido, por ende, en el caso concreto será el dueño de la identidad (nombre, apellido, nacionalidad, filiación y otros datos) que ha sido suplantada. ***Bien Jurídico protegido:*** "Derecho a la Identidad", toda vez que este delito se encuentra tipificado en la Sección Décima de "Delitos Contra el derecho a la identidad". Este derecho como se ha mencionado a lo largo de la investigación está reconocido en la Constitución ecuatoriana en su artículo 66 numeral 28. Según la Enciclopedia Jurídica la identidad es el conjunto de datos a través del cual se establece si una persona es verdaderamente la que se presume que es, estos datos incluyen, nombre, apellido, nacionalidad, filiación, entre otros.
Dr. Jorge Nagales (Asistente de Fiscalía)	La suplantación de identidad en el art. 212 ya tiene sus verbos rectores previamente establecidos. El tipo penal debería orientarse de forma adecuada, si se habla de una conducta que involucra contenido sexual, este debe ser analizado desde el tipo penal de violación a la intimidad. La conducta de suplantar la identidad con contenido sexual se ajusta más a una violación a la intimidad y a criterio personal sería preciso reformar el tipo penal de violación a la intimidad incluyendo el verbo rector de "suplantar"	
Verónica Altamirano Guerra (Asistente fiscal)	Si se analiza la conducta dependiendo de las consecuencias podría tratarse como una extorsión, sin embargo, no es tan viable adaptarlo de esa manera, por ello considero	

	que, si fuese bueno incluir el tipo penal, en el delito de violación a la intimidad, por contener información sensible, es decir fotos intimas.	***Verbo Rector:*** **"**Suplante". De acuerdo con el Diccionario panhispánico del español jurídico, suplantar significa "Quitar a una persona su sitio de manera fraudulenta, ocupando su cargo o posición, o asumiendo sus funciones". De lo analizado *ut supra* se puede evidenciar que no existe como tal una tipificación a la conducta de suplantar la identidad con contenido sexual, si bien se lo puede estudiar o sancionar bajo este tipo penal como lo han manifestado dos de los entrevistados, considero que al no estar reconocida una identidad digital con todos los componentes que surgen dentro de la era tecnológica, es muy difícil sancionarlo, puesto que el Derecho Penal es de ultima ratio y se puede alegar esa circunstancia frente a esta conducta. Por otro lado, el delito de violación a la intimidad está contenido en el artículo 178 ibidem. **Art. 178.- Violación a la intimidad. -** La persona que, sin contar con el consentimiento o la autorización legal, acceda, intercepte, examine, retenga, grabe, reproduzca, difunda o publique datos personales, mensajes de datos, voz, audio y vídeo, objetos postales, información contenida en soportes informáticos, comunicaciones privadas o reservadas de otra
Dr. Christian Israel Rodríguez **Juez de Garantías Penales en el cantón Ambato**	Si, pero más bien considero que es necesario que debiese tratarse como una agravante en el delito que atenta contra la intimidad personal o al mismo tipo penal agravándole la pena, cuando sea cometido haciendo uso de este tipo de contenido sexual, por ejemplo, tomando en cuenta la grave afectación que puede tener la víctima cuando eso trasciende una esfera personal y llega a visualizarse por personas ajenas a su círculo familiar, cuando además provoca circunstancias de acoso u hostigamiento.	
Dr. Fabián Altamirano **Juez de Garantías Penales en el cantón Ambato**	Considero que es necesario una modificación, pero bajo el contexto de uso de datos personales sensibles, teniendo en cuenta que el bien jurídico sería el derecho a	

	la intimidad. Esto, tomando en consideración que, si no existe un tipo penal claro para el juzgamiento de estos actos, no se puede legislar o sancionar mediante jurisprudencia.	persona por cualquier medio, será sancionada con pena privativa de libertad de uno a tres años. ***Sujeto activo:*** El artículo establece que el sujeto activo es cualquier persona. ***Sujeto pasivo:*** Se considera sujeto pasivo al dueño del bien jurídico protegido, por ende, en el caso concreto será el dueño de la intimidad a la que se haya afectado.
Dr. Misael Rodríguez Abogado en libre ejercicio.	Considero que, si es necesario una modificación en el cuerpo normativo penal, debido a la creciente prevalencia de delitos relacionados con el uso de datos personales íntimos en la era digital. Esta modificación, pienso que debería incluirse en el delito de violación a la intimidad, por el contenido sexual de la víctima que expone su intimidad.	***Bien Jurídico protegido:*** **"**Derecho a la intimidad". El Diccionario panhispánico del español jurídico define a este derecho como la capacidad que tienen las personas para gozar de un espacio propio y reservado para desenvolver su vida personal y familiar plena y libre, sin intromisión de terceros. ***Verbo Rector:*** El COIP ha determinado un tipo penal compuesto disyuntivo separado por la letra "o". Los verbos rectores que incorpora el legislador son acceda, intercepte, examine, retenga, grabe, reproduzca, difunda o publique. Es importante determinar que, este tipo penal engloba las circunstancias que ocurren dentro de la era digital, realiza una tutela judicial ya en un ámbito más allá de lo tradicional.

Comentario personal: La conducta de suplantar la identidad mediante el uso de contenido sexual considero que es un tema de amplio abordaje doctrinario, jurídico y legal, puesto que como lo han manifestado dos de los entrevistados existe el delito de suplantación de identidad, sin embargo, el Tribunal Superior de Justicia de España en la Sentencia N° 292/2024 alude que el simple hecho de suplantar la identidad no puede configurarse como un delito, es decir, no es delito la suplantación de identidad momentánea y parcial, sino que esta conducta debe ser continuo y persistente; además, el infractor debe asumir la personalidad ajena del titular con ejercicio de sus derechos y acciones dentro de su "status" tanto familiar como social (p. 4). En este sentido, los entrevistados han dejado claro que la identidad es una sola y se le atribuye solo físicamente. Por otro lado, el delito de violación a la intimidad protege de forma directa al derecho a la intimidad, esto incluye aquellos datos personales considerados sensibles contenidos en redes digitales, incluye verbos rectores que configuran un tratamiento de los datos personales. Por ello, personalmente mi postura se enmarca en adecuar la conducta de suplantación de identidad con contenido sexual en el delito de violación a la intimidad. Sostengo que es necesario que el tipo penal como agravante el uso de datos personales sensibles para suplantar la identidad mediante contenido sexual en las redes digitales. Vale aclarar que, los objetos sobre los que recaen las acciones típicas que violan la intimidad son los datos reservados de carácter personal o familiar que se hallen registrados en ficheros o soportes informáticos, electrónicos o telemáticos, sea público o privado.

Nota: Información obtenida de la entrevista desarrollada por la autora.

Entrevistas dirigidas a jueces en materia penal y abogados en libre ejercicio.

Tabla 10: *Criterios de la Corte sobre el tratamiento de datos personales.*

¿Considera que la Sentencia N° 2064-14-EP de la Corte Constitucional establece criterios claros para el tratamiento de datos personales?		
Profesional entrevistado	**Respuesta**	**Análisis**
Dr. Christian Israel Rodríguez	Desconoce la sentencia, sin embargo, luego de exponer la	Del total de los entrevistados, dos profesionales conocen el contenido de la sentencia y consideran que la Corte explica criterios claros sobre el

Juez de Garantías Penales en el cantón Ambato	misma por el entrevistador. Considera que al referirse a derechos que surgen en la nueva era digital es una sentencia acertada pero que únicamente serviría como base de análisis de los derechos esgrimidos por la Corte Constitucional.	tratamiento de los datos personales, sin embargo, uno de ellos desconoce totalmente el contenido, empero tras una exposición detallada de los argumentos que la Corte expone, considera que al referirse a los derechos que surgen con el avance tecnológico es una sentencia acertada, misma que debe servir como base para el análisis de los derechos. El tratamiento de datos personales enmarca un conjunto de derechos relacionados con la protección de estos datos. Es así como, Trigo Kramcsák citado por Villagómez et al. (2022) ha señalado expresamente que este presupuesto "debe reconocer su fundamento en la protección y tutela de la autodeterminación informativa" (p. 105). Debe entenderse que este derecho integra la capacidad para que el titular tenga autocontrol y autonomía respecto de sus datos personales. Cabe destacar que, las actuaciones que terceras personas hagan sobre los datos personales de otros necesitan la autorización legal de la persona titular, sin que ello signifique la pérdida de su titularidad. La Ley de Protección de Datos Personales del Ecuador ha contemplado una definición amplia sobre el tratamiento de datos personales, el artículo 4, inciso final menciona que es "cualquier operación o conjunto de operaciones realizadas sobre datos personales". Sumado a esto, la CC en la sentencia materia de análisis desarrolla una serie de criterios para desarrollar el tratamiento de datos en la esfera personal y doméstica. También determina
Dr. Fabián Altamirano Juez de Garantías Penales en el cantón Ambato	Si, son claros y se anticipan a cuestiones que por el momento no se encuentran reguladas en el ordenamiento jurídico ecuatoriano. Dentro de la sentencia se abarca jurisprudencia española debido a la falta de normativa nacional. Esto es favorable debido a que como la tecnología avanza el marco jurídico debe adecuarse a la conducta humana dentro de esta nueva realidad.	

		que el simple acceso puede ser considerado como tratamiento de datos personales, pero deja claro que a determinación debe realizarla el operador de justicia mediante la casuística. El tratamiento datos personales puede constituir una grave afectación a la privacidad e intimidad, de tal forma que Ryan Calo citado por Villagómez et al. (2022) sostiene que existen dos componentes del daño a la privacidad, el primero es el daño objetivo como consecuencia real, cita textualmente el robo de identidad en sí misma o la formación de una opinión negativa, como consecuencia de la pérdida del control de su titular, por otro lado, señala el daño subjetivo, como la pérdida de control que causa temor o incomodidad (p. 106). Con base a estos razonamientos, la Corte señala la importancia de los jueces de brindar una tutela judicial efectiva analizando casuísticamente. En línea con lo argumentado por la Corte, es imprescindible que el juzgador tome en cuenta la jurisprudencia constitucional, pero también los presupuestos legales contenidos en el ordenamiento jurídico internacional, principalmente la normativa de la Unión Europea. En este contexto, según Rodríguez (2019) el RGPD tenía como objetivo principal, dotarle de poder al ciudadano, como titular de los datos, para supervisar y controlar las circunstancias del uso y tratamiento de sus datos personales (p. 28). Es así como el legislador incorpora principios atenientes al tratamiento de datos personales con el fin
Dr. Misael Rodríguez Abogado en libre ejercicio	Son claros, pero es necesario un abordaje más profundo de la temática, es importante que el profesional del Derecho esté en constante aprendizaje, más ahora que aparecen nuevas modalidades de interactuar y delinquir.	

		de precautelar su protección y evitar vulneraciones a derechos fundamentales. Relacionado con esto, la legislación ecuatoriana en la Ley Orgánica de Protección de Datos Personales contempla los principios de juridicidad, lealtad, transparencia, finalidad, pertinencia y minimización de datos personales, proporcionalidad del tratamiento, confidencialidad, calidad y exactitud, conservación, seguridad de datos personales, responsabilidad proactiva y demostrada, aplicación favorable al titular, independencia del control (Art. 10). Se debe tomar en consideración que el tratamiento de datos personales debe ser de manera lícita, leal y transparente en relación con el interesado. El artículo 6.1 del RGPD expresamente señala que para que sea lícito es fundamental que: - El interesado manifieste el consentimiento para el tratamiento de los datos personales. - El tratamiento sea para el cumplimiento de un contrato en el que el interesado es sea parte o para medidas de naturaleza precontractual. - El tratamiento sea en función del cumplimiento de una obligación legal. - El tratamiento sea necesario para proteger intereses vitales. - Se establezca la necesidad del tratamiento con fine de interés público.

		- El tratamiento sea justificado por la necesidad de satisfacer intereses legítimos, siempre que no prevalezcan los intereses o derechos del interesado. El siguiente presupuesto que determina la norma internacional es que el tratamiento debe ser leal, es decir irrestrictamente ceñirse a los requisitos, derechos y garantías de protección de datos personales. Además, el tratamiento debe ser transparente, que refiere al deber de informar al titular las circunstancias que rodean el tratamiento de sus datos personales, en un lenguaje claro y sencillo.
Comentario personal: La sentencia aborda argumentos claves en el desarrollo del derecho en el ámbito digital. La Corte aborda criterios claros que no solo protegen los derechos individuales, sino que también promueven una comprensión profunda del derecho a la intimidad. Desde una perspectiva personal pienso que las respuestas de los entrevistados son acertadas. Es fundamental que los individuos tengan la capacidad de controlar su información personal, desde el acceso y uso de sus datos personales efectuado por terceras personas. Se debe destacar la importancia que ha señalado la Corte de adaptar la normativa a instrumentos jurídicos internacionales como el Reglamento General de Protección de Datos Personales de la Unión Europea, en dónde se destaca la importancia del consentimiento del titular de los datos personales para su tratamiento. Ahora en una sociedad cada vez más digitalizada es importante que el ordenamiento jurídico establezca de forma clara y coherente la delimitación de los derechos en el contexto digital. Bajo este criterio, en las redes sociales se evidencia constantemente el uso inadecuado de los datos personales de los usuarios, es así como la Corte estima que la divulgación no autorizada de estos datos, con especial énfasis en aquellos considerados de carácter sensible, vulnera derechos fundamentales como la intimidad, imagen, buen nombre. Este reconocimiento subraya la importancia de proteger los datos personales en un escenario donde el uso indebido puede tener consecuencias graves para los individuos.		

Nota: Información obtenida de la entrevista desarrollada por la autora.

Tabla 11: *Determinación del tratamiento de datos personales por los operadores de justicia.*

¿Considera que la Corte Constitucional en la sentencia N° 2064-14-EP deja a criterio de los jueces la determinación del tratamiento de datos personales efectuado en redes sociales?		
Dr. Christian Israel Rodríguez **Juez de Garantías Penales en el cantón Ambato**	Establece criterios que pueden ser considerados por los operadores de justicia a la hora de analizar los derechos establecidos en la constitución en la era digital. No declaran derechos, únicamente se analizan los derechos que posiblemente que se pudieron haber vulnerado en el caso de inicio o caso de origen.	Los entrevistados de forma unánime señalan que la Sentencia no determina directrices exactas para el tratamiento de datos personales, más bien, se denotan criterios que deben ser tomados en cuenta por los operadores de justicia a la hora de evaluar los derechos constitucionales en el contexto digital. Esto sugiere que, aunque se proporcionan pautas jurídicas, la interpretación y aplicación de estas dependen del contexto particular de cada caso. En contraste, dos de los entrevistado han explicado que, si bien la sentencia analiza de forma amplia los derechos relacionados con el tema del tratamiento de datos personales, un juez no puede resolver los procesos basándose en jurisprudencia, siempre debe existir una noma que motive su decisión. De manera que no se vulnere el derecho constitucional establecido en el artículo 76, numeral 7, literal I, apartado que menciona “. No habrá motivación si en la resolución no se enuncian las normas o principios
Dr. Fabián Altamirano **Juez de Garantías Penales en el cantón Ambato**	No, más bien es limitada. Esto por dos cuestiones, la primera es que al momento de juzgar no se puede dejar abierta una resolución, con una norma en blanco y segundo no se puede dejar a criterio discrecional cuestiones que a futuro	

	podría generar mucha influencia. Lo que marca es un camino claro de cómo hay que proceder en temas que, si bien están regulados en la Ley de Protección de Datos Personales, aunque no en su totalidad, no abarca muchas otras cuestiones. En este sentido, la sentencia da unas pautas para que los jueces hagan su análisis.	jurídicos en que se funda y no se explica la pertinencia de su aplicación a los antecedentes de hecho" (Art. 76.7.l). Por ello, los profesionales entrevistados han considerado que la sentencia no deja a criterio de los jueces la determinación del tratamiento de datos personales, más bien otorga directrices para que sean tomadas en cuenta en cada caso concreto. Vale aclarar que, entre los argumentos que deben tomar los jueces a la hora de determinar el tratamiento de datos personales está: • Es deber del juzgador aproximar el concepto de "operación sobre el dato" para examinar en el caso concreto si el acceso es o no una forma de tratar los datos personales. • El tratamiento de datos personales en la esfera exclusivamente personal o doméstica y sus efectos. • El tipo de información que se trate, el contexto, la duración y el abuso que se pueda generar como efecto del acceso. • El consentimiento previo, expreso e inequívoco del titular de los datos personales, sin que ello signifique la pérdida del control sobre sus datos.
Dr. Misael Rodríguez **Abogado en libre ejercicio**	Establece bases jurídicas para la tutela de derechos y protección de datos personales en la era digital, pero no necesariamente es aplicable en todos los casos. Por ello, no se puede decir que a discrecionalidad del juez se va a determinar el tratamiento de datos personales de forma automatizada en todos los casos.	

		Desde la perspectiva de Laica (2022) cuando se emplea el uso de tecnologías de la información y redes sociales el uso de datos integra todas las actuaciones que comprometen los datos de una persona (p. 39). Siendo deber del juzgador fijar objetivamente las acciones que devienen del tratamiento de datos personales a fin de resolver de manera justa y equilibrada. Las redes sociales al formar parte de la vida cotidiana de los individuos pueden ser considerada como un componente doméstico, por consiguiente, el subir fotografías no vulnera derechos constitucionales, más aún cuando la publicación se la realiza en la esfera doméstica, es decir en el círculo privado del usuario de la cuenta. Sin embargo, el juzgador deberá tomar en cuenta el tipo de contenido cargado en la red, el nivel de afectación que provoque su reproducción o uso, etc. La postura de los tres profesionales del derecho se direcciona a reconocer la importancia que tiene en la actualidad los criterios emitidos por la Corte en referencia a la protección de datos personales, así también, reflejan la necesidad de la instauración y actualización constante de la normativa ecuatoriana.

Comentario personal: Los argumentos de los profesionales son totalmente acertados, la Corte prescribe que el tratamiento de datos personales incluye un espectro amplio de actuaciones que da pautas para identificar escenarios en los que se constituya un tratamiento de datos. Esto como consecuencia del desarrollo de las nuevas tecnologías y medios digitales que cada vez permite a los individuos acceder y procesar información personal de manera diferente. Así, la Corte le otorga al juez el deber de determinar caso por caso cuando se está frente al tratamiento de datos personales, mediante la implementación del ordenamiento jurídico y de los argumentos presentes en como determina un juez como la Sentencia. Es decir, los entrevistados esgrimen las cuestiones señaladas por la CC. Por lo tanto, desde un criterio personal, la sentencia es el inicio de una protección más efectiva que el sistema judicial ofrece en la protección de datos personales contenidos en redes digitales. Pero, es fundamental que exista una capacitación constante y una difusión íntegra de la jurisprudencia relevante que atañe a este tema.

Nota: Información obtenida de la entrevista desarrollada por la autora.

Tabla 12: *Estándares de las empresas privadas para la protección de datos personales.*

En su opinión, las empresas privadas, como plataformas digitales, ¿cumplen con estándares suficientes para proteger los datos personales de sus usuarios en casos de suplantación de identidad?		
Dr. Christian Israel Rodríguez Juez de Garantías Penales en el cantón Ambato	Las empresas privadas, especialmente las plataformas digitales, enfrentan un desafío significativo en la protección de los datos personales de sus usuarios, particularmente en situaciones de suplantación de identidad. Aunque existen marcos legales como	Los tres profesionales entrevistados concuerdan que, las empresas privadas no cumplen con los estándares suficientes para proteger los datos personales, independientemente de su uso o finalidad. En el caso de suplantación de identidad con contenido sexual en el contexto digital las plataformas digitales no establecen normas de privacidad efectivas que eviten que los usuarios de las redes usen de forma arbitraria e ilegítima datos personales sensibles de otros usuarios con

	la Ley Orgánica de Protección de Datos Personales en Ecuador, que busca garantizar el acceso y la protección de la información personal, la implementación efectiva de estas regulaciones presenta varios obstáculos. aunque las empresas privadas tienen el deber legal de proteger los datos personales, la realidad muestra que muchos aún no cumplen con los estándares necesarios para prevenir suplantaciones de identidad efectivamente. La combinación de un marco legal emergente, la responsabilidad empresarial en la implementación de medidas adecuadas y una mayor educación en ciberseguridad son fundamentales para mejorar la	la finalidad de atentar contra su imagen, dignidad, honor, haciéndose pasar por su titular. Se debe resaltar que, el derecho a la vida privada se fundamenta en la dignidad humana, Herrera (2016) explica que su definición y delimitación es difícil, pues es un presupuesto que muta con el transcurso del tiempo y es distinta en cada sociedad y cultura (p.88). De tal forma que, la doctrina, la ley y la jurisprudencia deben establecer cuando una situación vulnera la privacidad de un individuo y fijar los límites de lo público y lo privado. En este contexto, la Corte Constitucional del Ecuador por medio de la Sentencia N° 2064- 14-EP/21 estudia la expectativa razonable de la privacidad y determina que, deben existir dos elementos para que se configure este presupuesto, uno subjetivo y otro objetivo. El elemento subjetivo responde a que quien alegue la violación a la intimidad pueda considerar válidamente que su actividad, comportamiento o esfera esté protegida de posibles injerencias, *contrario sensu* el elemento objetivo consiste en que la sociedad pueda asumir dicha expectativa. Las plataformas digitales como las redes sociales han sido definidas por INTECO (2009) como el conjunto de servicios que se ofrece a través de internet, en el cual se pueden generar perfiles y hacer público los datos e información personal; esta herramienta permite

	protección de los datos personales en el entorno digital ecuatoriano.	interactuar con otros usuarios de las redes (p. 6). La exposición de los datos personales en las redes digitales provoca que los usuarios pierdan el control de su reproducción, uso y tratamiento. Evidentemente, cuando una persona publica una fotografía no tiene la certeza de qué personas la están observando o más aún, quiénes están haciendo uso de ellas. Por otro lado, cuando un usuario de la red comparte con otro, bajo su consentimiento fotografías íntimas, tampoco se asegura que esa foto no rebase la esfera privada. Por ende, como lo afirma INTECO (2009) los usuarios deben valorar siempre el tipo de contenido que publican en las plataformas digitales, ya que no tiene la misma trascendencia el tratamiento por parte de la plataforma los datos personales que otra información con contenido más sensible como aquella que refleja la vida sexual (p.109). Uno de los entrevistados a mencionado que las plataformas digitales cumplen con parámetros muy mínimos de protección, esto se puede corroborar debido a que las redes digitales establecen avisos legales, condiciones de uso y políticas de privacidad redactados en un lenguaje de difícil comprensión. De tal manera que, el estar cargado en la red estos avisos, esto no garantiza y no alcanza la finalidad, es decir que el usuario comprenda el objeto, la forma y el plazo para el que son recabado y tratado sus datos.
Dr. Fabián Altamirano **Juez de Garantías Penales en el cantón Ambato**	No, las empresas generalmente establecen parámetros muy mínimos para proteger los datos personales, imágenes.	
Dr. Misael Rodríguez **Abogado en libre ejercicio**	Aunque la Ley Orgánica de Protección de Datos Personales (LOPD) en Ecuador establece un marco legal que busca garantizar la privacidad y seguridad de la información personal, la implementación y cumplimiento de estos estándares por parte de las empresas aún presenta deficiencias.	

Comentario personal: Desde mi punto de vista, la protección de datos personales en el contexto de las plataformas digitales es un tema que requiere una atención urgente y constante. Aunque muchas empresas han comenzado a implementar políticas de privacidad y medidas de seguridad, la realidad es que aún hay un largo camino por recorrer para garantizar que los datos de los usuarios estén verdaderamente protegidos, especialmente frente a amenazas como la suplantación de identidad. El marco legal proporciona una base necesaria para la protección de datos, pero es evidente que las empresas deben hacer más para cumplir con estos estándares y garantizar la seguridad de sus usuarios. La confianza del público en las plataformas digitales depende de su capacidad para demostrar un compromiso genuino con la protección de datos personales. Solo así podremos construir un entorno digital más seguro y confiable para todos.

Nota: Información obtenida de la entrevista desarrollada por la autora.

Tabla 13: *Protección de datos personales en el sistema jurídico actual*

¿Considera que el actual marco jurídico nacional en protección de datos personales es suficiente para abordar casos de suplantación de identidad con contenido sexual en la era digital?		
Dr. Christian Israel Rodríguez Juez de Garantías Penales en el cantón Ambato	No es suficiente, de hecho, el problema es que el tema digital siempre va a estar muchos pasos más adelante que el contenido normativo de cada país, entonces no se puede decir que existe una adecuada regulación de las actividades que se pueden desarrollar dentro de la era digital. Existe norma general	Los profesionales afirman que la normativa ecuatoriana en el marco de protección de datos personales sensibles en la era digital es insuficiente. Uno de los aspectos analizado por los profesionales es el avance desacelerado que ha tenido la tecnología y la respuesta tardía del Derecho frente al uso y abuso de plataformas digitales. Todos los profesionales coinciden en que la tecnología ha evolucionado a un ritmo que supera la

	o casos mediante los cuales se puede tutelar los derechos en el ámbito digital. Siempre se tiende a tratar de regular, pero de ahí que se encuentre en la ley no. Si hay algo, pero no es completamente adecuada.	capacidad del marco legal, provocando vacíos en su regulación y afectaciones a derechos constitucionales como protección de datos personales, intimidad, privacidad. Los jueces han mencionado ejemplos concretos de áreas donde la legislación es considerada insuficiente. El Dr, Altamirano destaca la falta de regulación jurídica sobre dispositivos emergentes como drones y tecnologías relacionadas con la Inteligencia Artificial. En este punto, es importante enfatizar en el uso de herramienta de la IA como el *deepfake* para la creación de material íntimo a través del uso de datos personales como fotografías. Pese a los esfuerzos del legislador por regular delitos informáticos, hay un reconocimiento de que muchas actividades digitales contemporáneas no están contenidos en el ordenamiento jurídico. Pese a que el ordenamiento jurídico constitucional e infra constitucional protege derechos fundamentales como la privacidad y la integridad personal, los jueces señalan que esta protección es más teórica que práctica. La existencia de una ley específica sobre la protección de datos personales no garantiza su efectiva tutela. En este sentido, el Dr. Rodríguez enfatiza en que, hay normas generales que no abordan suficientemente las complejidades que surgen en el entorno digital.
Dr. Fabián Altamirano **Juez de Garantías Penales en el cantón Ambato**	No, es totalmente insuficiente. El problema es que desde que hay desarrollo de las nuevas tecnologías y por ende, desde que se lograron determinar los delitos informáticos como tal, la legislación siempre va detrás del avance tecnológico y hoy por ejemplo pese a que están regulados ya de manera bastante adecuada, no total, en nuestra legislación no todas las infracciones electrónicas están reguladas, por ejemplo no se regula el uso de ciertos dispositivos electrónicos como los drones y tampoco cuestiones de la Inteligencia Artificial. Entonces, si alguien utilizando los datos personales crea desde cero informaciones falsas, como no está	

	regulada deja en impunidad al uso de programa que en la actualidad utilizan para la creación de algo, en caso del uso de contenido sexual, por ejemplo. Pese a que constitucionalmente están protegidos los datos personales, el nombre, la imagen, la indemnidad sexual de menores de edad, integridad sexual si es mayor de edad, esto no permite abarcar desde una cuestión tecnológica.	En relación con esto, la promulgación reciente de la Ley Oránica de Protección de Datos Personales (LOPD) en 2021, presenta un paso positivo, pero también plantea interrogantes sobre su implementación y efectividad, por ello, la sola existencia de la norma no garantiza los derechos. La LOPD en Ecuador aparece debido a la fuga masiva de datos del país en Estados Unidos, así como por la exigencia internacional de la Unión Europea. El análisis efectuado por los entrevistados revela un consenso sobre la necesidad de fortalecer el marco jurídico ecuatoriano respecto a la privacidad, intimidad y protección de datos personales. Otro aspecto que considerar es la educación digital como un componente trascendental para mejorar la protección de datos personales. La falta de conocimiento sobre derechos digitales y sobre cómo manejar adecuadamente la información personal, limita la capacidad de una tutela jurídica. Vale aclarar que en concordancia con la legislación sobre la protección de datos personales debe estar la implementación de políticas y programas que busquen el ejercicio del derecho a la protección de datos personales. En este aspecto, es importante tener en cuenta el pensamiento de Troncoso (2010) que
Dr. Misael Rodríguez **Abogado en libre ejercicio**	Es insuficiente, el avance tecnológico está más avanzado que el ordenamiento jurídico, además que la Ley de protección de datos personales en ecuador se promulgó apenas en el año 2021, cuando la tecnología estaba en su mayor auge debido al confinamiento social.	

		manifiesta “el derecho fundamental a la protección de datos personales no trata de impedir el recurso a las nuevas tecnologías sino de conciliarlo con el respeto a la dignidad de la persona” (p. 595).
Comentario personal: Desde mi perspectiva, el marco jurídico nacional en Ecuador para la protección de datos personales es un paso positivo hacia la salvaguarda de la privacidad y la dignidad de los ciudadanos. Sin embargo, al abordar problemas tan complejos y dinámicos como la suplantación de identidad con contenido sexual queda claro que se requieren ajustes y mejoras significativas. La rapidez con la que evoluciona la tecnología y las plataformas digitales plantea desafíos que las leyes actuales a menudo no pueden anticipar. La suplantación de identidad, especialmente en un contexto donde las imágenes íntimas pueden ser compartidas y manipuladas con facilidad, exige una respuesta legal que no solo castigue a los infractores, sino que también ofrezca un apoyo real a las víctimas. Esto incluye mecanismos claros para la eliminación de contenido no autorizado y un sistema de reparación que aborde tanto los daños materiales como los emocionales. Además, considero que la protección de la privacidad y la identidad personal no debería ser solo una cuestión legal, sino un compromiso colectivo para crear un entorno más seguro y respetuoso para todos.		

Nota: Información obtenida de la entrevista desarrollada por la autora.

Tabla 14: *Obstáculos en el sistema judicial para aplicar la Sentencia N°2064-14-EP/21.*

¿Qué obstáculos enfrenta el sistema judicial para aplicar de forma uniforme la sentencia 2064-14-EP en términos de manejo de datos personales?		
Dr. Christian Israel Rodríguez Juez de	Esta sentencia, emitida por la Corte Constitucional, establece importantes precedentes sobre la protección de datos	El análisis de los desafíos que enfrenta el sistema judicial ecuatoriano para la aplicación de la sentencia en relación con el manejo de datos personales revela una serie de desafíos complejos.

Garantías Penales en el cantón Ambato	personales y el derecho a la intimidad, pero su implementación efectiva se ve dificultada por varios factores como por una combinación de falta de capacitación, ambigüedad normativa, resistencia institucional, desigualdad en el acceso a la justicia y desafíos tecnológicos. Estos factores deben ser abordados para garantizar que los derechos consagrados sean efectivamente protegidos y aplicados.	Las respuestas de los profesionales del derecho ofrecen una visión integral sobre las dificultades que deben superarse para garantizar una implementación efectiva de esta jurisprudencia constitucional. Un aspecto crítico señalado por el Dr. Christian Rodríguez es la falta de capacitación a los profesionales que integran el sistema judicial. La protección de datos personales es un campo en constante evolución que requiere conocimientos específicos sobre tecnologías digitales y sus implicaciones legales. Sin una formación adecuada, los jueces pueden tener dificultades para interpretar correctamente la sentencia y aplicar los principios constitucionales y legales en casos concretos. La falta de capacitación no solo afecta a la motivación de las decisiones judiciales sino a la capacidad del sistema judicial para adaptarse a los desafíos contemporáneos. La ausencia de un marco jurídico claro es también uno de los desafíos que señalan los profesionales. Pese a que la sentencia en mención establece importantes principios sobre la protección de datos personales y los derechos que se vinculan a este, no puede sustituir a una legislación específica que regule estas cuestiones. La jurisprudencia debe concatenar con leyes concretas que definan claramente los derechos y responsabilidades relacionados con el
Dr. Fabián Altamirano Juez de Garantías Penales en el cantón Ambato	Una cosa es aplicar la jurisprudencia y otra es aplicar la ley, para ser viable la jurisprudencia es necesario que exista una ley o modificar la ley de datos personales o aumentar o transformarla en los puntos centrales que la Corte Constitucional establece en la sentencia. Lo esgrimido por la corte es una guía para regular cuestiones de vulneraciones de derechos en el ámbito digital, sin embargo, no se puede legislar a través de la jurisprudencia. Para casos	

	análogos puede ser considerada esta sentencia.	tratamiento de datos personales. Sin esta base legislativa, los argumentos de la Corte Constitucional pueden resultar insuficientes para el abordaje y la tutela jurídica de estos derechos. Los desafíos tecnológicos es otro factor que influye en estos casos, pues la rápida evolución de las tecnologías digitales plantea interrogantes sobre cómo se deben manejar y proteger los datos personales. Sumado a esto, la falta de conocimientos técnicos dentro del sistema judicial involucra en la instauración de medidas protectoras. Con todas estas cuestiones abordadas, es importante mejorar en la capacitación del personal judicial, el desarrollo de un marco normativo claro, la superación de resistencias institucionales, la adaptación a los avances tecnológicos.
Dr. Misael Rodríguez **Abogado en libre ejercicio**	La ambigüedad de la normativa jurídica, pues no establece parámetros en lo que respecta al tratamiento de datos personales. La falta de claridad en las leyes relacionadas con la protección de datos personales puede dar lugar a interpretaciones diversas y decisiones inconsistentes, lo que dificulta la aplicación uniforme de la jurisprudencia.	
Comentario personal: Estoy totalmente de acuerdo con los entrevistados, la falta de una legislación que aborde los vacíos legales e incluya la revisión de los mecanismos de protección y el fortalecimiento de los derechos sobre el manejo de la información personal, provoca el uso inadecuado y arbitrario de los datos contenidos en plataformas digitales. Es importante entender que, al fortalecer las leyes existentes y abordar las necesidades emergentes en un entorno digital, se puede mejorar no solo la protección efectiva de los derechos individuales, sino también aumentar la confianza al sistema judicial. Los legisladores deben analizar el contexto normativo de otros países como la Unión Europea, puesto que es uno de los países en hacer más referencia a la protección de datos personales en el contexto digital. Por su parte, la legislación colombiana tipifica conductas en las que se afectan los datos personales sensibles, por ende, considero necesario una adecuación penal que tenga como base la legislación penal de Colombia.		

Nota: Información obtenida de la entrevista desarrollada por la autora.

Tabla 15: *Recomendaciones para mejorar el sistema judicial en la protección de datos personales.*

¿Qué aspectos recomendaría mejorar en el sistema judicial para garantizar una protección más efectiva de los datos personales de carácter sensible de las víctimas de suplantación de identidad con contenido sexual?		
Dr. Christian Israel Rodríguez Juez de Garantías Penales en el cantón Ambato	En el tema de reparaciones sería mucho mejor, si se pudo determinar que se afectó el bien jurídico a la intimidad, es importante que los jueces orden a la empresa privada que ponga más responsabilidad con efecto irradiante como usualmente se lo realiza en otros países.	El Dr. Christian Rodríguez plantea un aspecto fundamental sobre la responsabilidad de las empresas en la protección los datos personales. Esto implica una responsabilidad irradiante, es decir que, al determinarse una violación a la intimidad, los jueces deben exigir a las empresas que implementen medidas correctivas y preventivas. En países como Alemania y Francia existen regulaciones jurídicas que obligan a las empresas a ser responsables de sus acciones directas y del manejo indebido de los datos personales por parte de terceros. Para alcanzar este objetivo, es indispensable modificar la legislación existente para incluir sanciones claras y mecanismos de reparación para las víctimas, como compensaciones económicas o la obligación a las empresas de ofrecer servicios de monitoreo y protección contra el robo de identidad. Desde la perspectiva del Dr. Altamirano, es importante la capacitación en el tratamiento adecuado de datos
Dr. Fabián Altamirano **Juez de Garantías Penales en el cantón Ambato**	Ahora, ya existe el mecanismo de ocultar los datos públicos. Creo que lo principal sería una capacitación de la forma de tratamiento de datos personales públicos en el contexto digital.	
Dr. Misael Rodríguez **Abogado en libre ejercicio**	Es esencial que el sistema judicial cuente con normas claras sobre cómo manejar casos relacionados con suplantación de	

	identidad. Esto incluye procedimientos para garantizar la confidencialidad durante el proceso judicial y protocolos para el manejo seguro de información sensible.	personales, tanto a entidades públicas, privadas y particulares. Señala que actualmente ya existe un mecanismo para ocultar datos públicos, pero no es suficiente porque no están adecuadamente formados. De hecho, la capacitación debería abarcar no solo a los operadores de justicia y personal judicial, sino también a funcionarios públicos, empresas tecnológicas y ciudadanos. Esta capacitación debe ser integral e incluir la formación sobre legislación vigente, mejores prácticas en ciberseguridad, impacto emocional y social que produce las conductas como la suplantación de identidad con contenido sexual.
Comentario personal: Considero que un punto importante que refiere en este apartado es la noción de responsabilidad irradiante que implica que las empresas no solo deben responder por sus propias acciones, sino también por el manejo indebido de datos por parte de terceros. Esto es especialmente relevante en un contexto donde las violaciones a la intimidad son cada vez más comunes y perjudiciales. Reitero en la necesidad de implementar sanciones claras y mecanismos de reparación para las víctimas como un paso trascendental en la protección de datos personales. Así, las compensaciones económicas y servicios de monitoreo son medidas que no solo beneficiarían a los afectados, sino que también incentivarían a las empresas a adoptar prácticas mas seguras. En conclusión, se requiere un esfuerzo conjunto entre el Estado, las empresas y los ciudadanos para garantizar que los derechos fundamentales sean protegidos en un mundo cada vez más digitalizado, con capacitaciones integrales constantes que abarque legislación vigente, mejores prácticas de ciberseguridad y uso de tecnologías.		

Nota: Información obtenida de la entrevista desarrollada por la autora.

Tabla 16: *Las fotografías íntimas como datos personales sensibles.*

¿Las fotos íntimas de una persona que se encuentran en una red social deben ser consideradas como datos personales sensibles en la legislación ecuatoriana?		
Dr. Christian Israel Rodríguez Juez de Garantías Penales en el cantón Ambato	En el contexto de la legislación ecuatoriana, las fotos íntimas de una persona que se encuentran en una red social deben ser consideradas como datos personales sensibles. Esta consideración se basa en la interpretación y los principios establecidos por la Corte Constitucional en la sentencia 2064-14-EP.	Los juristas están de acuerdo en que las fotos íntimas deban ser incorporadas dentro de la categoría de datos personales sensibles. Tomando en consideración que la LODPDP del Ecuador define a los datos sensibles como aquellos que pueden revelar aspectos íntimos de la vida de una persona y esto incluye su vida sexual. Según el Dr. Altamirano, esta clasificación es esencial ya que el tratamiento a estos datos puede dar lugar a alguna discriminación o vulneración de derechos fundamentales. La Sentencia 2064-14-EP/21 de la Corte Constitucional ecuatoriana establece principios sobre la protección de datos personales. Esta sentencia refuerza la idea de que cualquier dato que pueda afectar la dignidad o integridad personal deba ser protegida con un carácter especial. De las respuestas se obtiene que existe un vacío normativo sobre el abordaje del tratamiento de datos personales sensibles en el contexto digital, pese a la existencia de la
Dr. Fabián Altamirano Juez de Garantías Penales en el cantón Ambato	Si, los datos personales sensibles como las fotos íntimas deben ser consideradas como tal, debido a que forman o expresan la vida sexual de un individuo, además la ley de protección de datos personales prevé que son considerados sensibles aquellos datos que pueden provocar algún tipo de discriminación. En este caso, las fotos íntimas	

	revelan cuestiones personales de la víctima y de su vida sexual. Pese a que el ordenamiento jurídico ecuatoriano actualmente no cuenta con una regulación normativa adecuada.	LOPDP, puesto que no proporciona mecanismos suficientes para prevenir el uso indebido de estos datos en las redes digitales y las consecuencias que de ello implica. Para analizar estos presupuestos, se debe citar a Pfeiffer (2008) que explica que datos sensibles "Es una denominación que se usa preferentemente en el ámbito del derecho jurídico y tiene que ver con los datos que afectan a lo más propio de la persona, podríamos decir a su intimidad" (p.25). Estos datos incluyen aspectos del ser humano de índole ideológico, racial, sexual, económico de salud y cualquier otro que pueda considerarse como una amenaza para el individuo. Adquiere un carácter de protección especial puesto que, solo pueden ser revelados de manera voluntaria y con presunción de confidencialidad por la persona titular. Estos datos solamente importan a su titular y quien reciba esta información intima debe mantenerla bajo el precepto de "confidencialidad", pues el titular pese a que llegue a compartirlo con un tercero, no pierde el control sobre estos. Conforme Pfeiffer (2008) la confidencialidad es la actitud de respeto, silencio, reserva que pide el dato íntimo o privado a la persona que lo conoce (p. 27).
Dr. Misael Rodríguez **Abogado en libre ejercicio**	Sí, las fotos íntimas de una persona que se encuentran en una red social deben ser consideradas como datos personales sensibles según la legislación ecuatoriana. De acuerdo con la Ley Orgánica de Protección de Datos Personales (LOPD), los datos sensibles son aquellos que, por su naturaleza, pueden afectar la esfera más íntima de una persona y cuyo tratamiento indebido puede dar origen a discriminación o atentar contra los derechos humanos y la dignidad de las personas	

Comentario personal: La consideración de las fotos íntimas como datos personales sensibles en la legislación ecuatoriana es un paso fundamental hacia la protección de la privacidad y la dignidad de las personas en el entorno digital. En un mundo donde las redes sociales son una extensión de nuestras vidas personales, es alarmante pensar en la facilidad con la que pueden ser compartidas o mal utilizadas imágenes que revelan aspectos tan íntimos de nuestra identidad. Añadido a las respuestas de los entrevistados, desde mi perspectiva, esta clasificación no solo refuerza la importancia del consentimiento y el respeto por la intimidad ajena, sino que también subraya la necesidad de una mayor educación sobre el manejo responsable de la información personal en línea. Muchas personas, especialmente los jóvenes, a menudo no son plenamente conscientes de las implicaciones que conlleva compartir contenido íntimo en plataformas digitales

Nota: Información obtenida de la entrevista desarrollada por la autora.

Figura 15: *Reparación integral que se dicta a favor de la víctima.*

En los casos de suplantación de identidad con contenido sexual en el contexto digital ¿Cuál es la reparación integral que se dicta a favor de la víctima?		
Dr. Christian Israel RodríguezJuez de Garantías Penales en el cantón Ambato	Una de las reparaciones significativas en el sistema judicial internacional, por ejemplo, que sucedió en argentina con la empresa de WhatsApp en un caso de divulgación de este tipo de contenido de una figura pública y se ordenó a la empresa tomar medidas para garantizar el efectivo goce de derechos en la era digital de los usuarios y	La conducta de suplantar la identidad con contenido sexual en un contexto digital ha cobrado relevancia debido al aumento de casos donde se utilizan perfiles falsos para difundir datos personales sensibles que atentan contra la intimidad de la víctima. En este sentido, el Dr. Christian Rodríguez menciona que existe un caso en Argentina donde se ordenó a WhatsApp implementar medidas que garanticen los derechos de los usuarios y protejan su privacidad e

	así evitar la vulneración o afectación a la intimidad de la persona.	intimidad. Este enfoque resalta la responsabilidad de las plataformas digitales en la protección de los datos personales de los usuarios.
Dr. Fabián Altamirano **Juez de Garantías Penales en el cantón Ambato**	- Reparación económica - Reparación simbólica. - Orden de eliminación de los registros de búsqueda. Sin embargo, esta reparación no se la puede garantizar mediante una acción de hábeas data, sino mediante una acción judicial ordinaria, esto es el bien penal.	Se ha señalado que la víctima puede ser reparada integralmente de manera económica, que puede incluir compensaciones monetarias por los daños sufridos, así también, existe una reparación simbólica que involucra acciones que reconozcan el daño contra la víctima. Sin embargo, la efectividad de estas reparaciones puede variar dependiendo del contexto legal y las plataformas implicadas. Como medida específica se ha determinado la orden de eliminación de registro de búsqueda. No obstante, esta medida no siempre es efectiva mediante acciones legales simples, como un hábeas data, sino que requiere un procedimiento judicial ordinario.
Dr. Misael Rodríguez **Abogado en libre ejercicio**	Según el Código Orgánico Integral Penal (COIP), específicamente en su Artículo 212, se establece que la suplantación de identidad es un delito que puede acarrear penas privativas de libertad, pero también es crucial considerar las formas de reparación que se deben ofrecer a las víctimas. Estas reparaciones pueden ser	Para determinar la reparación integral, es importante evaluar el daño a la reputación personal, a su integridad, honor, imagen, buen nombre, dignidad, intimidad y el impacto psicológico y emocional que estas conductas pueden provocar en la víctima.

	económicas, es decir que la víctima tiene derecho a recibir indemnización que cubra los daños materiales y morales causados por esta conducta.	La víctima en el proceso penal es considerada como sujeto procesal de mayor relevancia, considerando que es la persona que se ha visto afectada por la consecución de un delito, es quien sufre la lesividad de un bien jurídico protegido. En base a esto, se puede esgrimir que la víctima tiene derecho a una reparación integral. reparación integral involucra medidas destinadas a desaparecer los efectos de las violaciones cometidas y a indemnizarlas. En este sentido, puede existir reparaciones materiales e inmateriales, esta reparación le corresponde al victimario. Según (Benavides) El establecimiento de la reparación incluirá los valores que deben estar debidamente cuantificados en lo referente a la indemnización material; en tanto que la reparación inmaterial como por ejemplo: conocer la verdad del hecho, pedir disculpas públicas, publicar dichas disculpas en medios de comunicación social o cualquier otra medida que tenga como finalidad reparar el daño moral ocasionado a la víctima, deberá ser pensado en atención a los diferentes mecanismos de reparación escritos en la norma u otros que considere pertinentes además, a la

		voluntad de la víctima o sus familiares, si fuere el caso. (p. 293) De tal forma que, el Estado debe garantizar una reparación integral a la víctima mediante un enfoque de derechos. Además, debe entenderse a la reparación integral como el resarcimiento del daño ocasionado a la víctima.
Comentario personal: La suplantación de identidad con contenido sexual en el contexto digital es un problema alarmante que refleja las vulnerabilidades inherentes a nuestra creciente dependencia de la tecnología. Este fenómeno no solo afecta la reputación y la intimidad de las víctimas, sino que también puede tener repercusiones profundas en su bienestar emocional y psicológico. Lo que más me preocupa es la rapidez con la que se pueden difundir imágenes y datos sensibles en línea, lo que dificulta enormemente el control sobre la propia identidad. En un mundo donde las redes sociales y las plataformas digitales son parte integral de nuestras vidas, es fundamental que se establezcan mecanismos robustos de protección y reparación para quienes sufren este tipo de delitos. Es alentador ver que se están llevando a cabo investigaciones y se están adoptando medidas legales, como la Sentencia N°2064-14-EP/21, para abordar estas cuestiones. Sin embargo, queda mucho por hacer. La educación sobre el uso responsable de la tecnología y la promoción de una cultura de respeto hacia la privacidad ajena son esenciales para prevenir estos delitos.		

Nota: Información obtenida de la entrevista desarrollada por la autora.

3.1 Análisis y discusión de los resultados

En el presente trabajo se aplicaron siete entrevistas, cuatro de ellas fueron realizadas a fiscales del cantón Latacunga, dos a jueces de la Unidad Penal del cantón Ambato y una a un abogado en libre ejercicio especialista en Derecho Penal. Se empleo un cuestionario de 5 y 10 preguntas respectivamente direccionadas al cumplimiento de los objetivos propuestos en la investigación. De manera que:

Para cumplir el primer objetivo específico que fue "Examinar el alcance y los componentes de los datos personales en el ámbito digital establecidos en la sentencia" las preguntas 1 y 8 del cuestionario de la entrevista dirigida a jueces y abogados en libre ejercicio están direccionadas a determinar el alcance y componente de los datos personales en relación con su tratamiento dentro de un contexto digital. De los tres profesionales entrevistados, todos concuerdan que el avance tecnológico evoluciona aspectos cotidianos de la vida del ser humano. Así pues, manifiestan que es necesario la incorporación de normativa legal que amplíe el significado de datos personales desde una visión digital, por otro lado, resaltan la necesidad de la protección que debe brindar el sistema judicial frente al advenimiento de nuevas modalidades delictivas. Además, han concordado que el ordenamiento jurídico de la Unión Europea en cuanto al reconocimiento de datos personales es más avanzado que el del Ecuador, razón por la cuál es necesario adoptar la visión que tiene la Corte Constitucional en la Sentencia N° 2064.14. EP/21. Adicionalmente, la pregunta 8 a determinado que, según los profesionales expertos, es necesario el reconocimiento de las fotos íntimas como datos de carácter sensible por cuanto estos forman parte de la vida íntima de su titular. Es decir, con una sociedad cada vez más digitalizada el alcance de los datos personales cambia y la normativa debe ajustar su protección.

En función al segundo objetivo que fue "Establecer de qué manera el tratamiento de datos personales en redes digitales conlleva al cometimiento del delito de suplantación de identidad con contenido sexual en el contexto digital" las preguntas 1, 2, 3, 7, 9 y 10 de la entrevista dirigida a jueces y abogados en libre ejercicio; y, las preguntas 2 y 3 empleadas a fiscales del cantón Latacunga permitieron conocer la visión holística de los profesionales expertos en relación al tratamiento de datos personales y la conducta de suplantar la identidad con contenido sexual. Entre los principales criterios otorgados por los entrevistados se ha logrado determinar que el tratamiento de datos personales en el contexto digital es amplio, su investigación requiere de peritajes informáticos, cooperación internacional y otros factores fundamentales que surgen con las nuevas tecnologías. El tratamiento de datos personales

generalmente lo hacen personas que tienen conocimiento en ingeniería social, por ende, sus los fiscales sostienen que su investigación es compleja.

Ahora bien, el uso de datos personales sensibles para suplantar la identidad en el contexto digital puede ser considerado como un tratamiento de datos personales susceptible de ser sancionado penalmente, esto, a criterio de los jueces y abogados en libre ejercicio, depende del análisis que realice el operador de justicia. De ahí radica la importancia de los argumentos establecidos en la sentencia *in examine* sobre la forma de determinar cuándo se está frente a un tratamiento de datos personales. Los profesionales, tanto fiscales, jueces y abogados concuerdan que la sentencia es una base que determina la Corte para el análisis y estudio de las conductas que vulneran derechos fundamentales en la era digital.

En relación con lo mencionado, para dar cumplimiento al tercer objetivo específico que es "Evaluar la eficacia de la Sentencia No. 2064-14-EP/21 de la Corte Constitucional del Ecuador en la prevención y sanción de la conducta de suplantación de identidad con contenido sexual considerando la legislación ecuatoriana vigente y jurisprudencia relevante" se aplicaron las preguntas 4 y 5 tanto de la entrevista para jueces, abogados y fiscales. Estas preguntas fueron direccionadas a realizar un abordaje evaluativo por parte de los profesionales con respeto a la aplicación de la sentencia. Los entrevistados han concordado que la sentencia establece pautas necesarias que deben ser consideradas por los profesionales del Derecho. La importancia de la sentencia radica en el hecho de que recoge cuestiones trascendentales que no han sido estudiadas o incluidas en el ordenamiento jurídico. Así como, resalta la jurisprudencia y normativa internacional que debe tomar en cuenta el juzgador a la hora de emitir su decisión. Esto con la finalidad de proteger de forma holística los datos personales contenidos en plataformas digitales y los derechos que de ello deriva.

CAPÍTULO IV. - CONCLUSIONES Y RECOMENDACIONES

4.1. Conclusiones

4.2 Recomendaciones

Tabla 17*: Conclusiones y recomendaciones en función de los objetivos*

Objetivo específico 1: Examinar el alcance y los componentes de los datos personales en el ámbito digital establecidos en la sentencia.	
Conclusiones	**Recomendaciones**
• Los datos personales incluyen toda aquella información que identifica o hace identificable a una persona, gozan de protección jurídica, son personalísimos y extrapatrimoniales. El alcance de estos datos está determinado por la normativa jurídica cuando menciona que son “cualquier información” es decir permite un abordaje amplio para considerar el alcance de estos datos. Sin embargo, esta amplitud que ofrece la normativa puede llegar a ser ambiguo y carecer de protección jurídica. En el contexto digital el alcance de estos datos involucra incluso a los “datos no personales” que combinados con otros pueden identificar o hacer identificable a una persona física. Este tipo de datos, no gozan de protección jurídica. Así la doctrina estudia los llamados metadatos o datos compuestos, que	• La protección de los datos personales en la era digital es un tema poco abordado por la jurisprudencia, la doctrina y la normativa. En el contexto digital la recopilación y el tratamiento de información se realizan a gran escala. Por ello, es fundamental que las leyes que regulan estos datos sean revisadas y clarificadas para evitar ambigüedades. La normativa y la doctrina actual deben definir con precisión qué se considera "cualquier información", asegurando que las protecciones se apliquen de manera efectiva a todos los tipos de datos, incluidos aquellos que, aunque no son personales por sí mismos, pueden combinarse para identificar a individuos. • Frente a la deficiente regulación normativa respecto de la protección de datos personales, se recomienda la instauración de legislación que abarque una protección jurídica en el entorno

implica un estudio de manera conjunta de los llamados “datos no personales”. • Los criterios de los profesionales entrevistados han reflejado la necesidad de implementar normativa jurídica y desarrollar doctrina que involucre el tema de datos personales en la era digital, su alcance, protección y tratamiento. Frente al advenimiento tecnológico, concuerdan que el derecho ha quedado un paso atrás, permitiendo vulneraciones a derechos fundamentales, más aún cuando se atenta a la intimidad de los individuos que desemboca en afectaciones psicológicas y emocionales difícil de reparar. • Del estudio comparativo de la legislación de la Unión Europea, española, colombiana y ecuatoriana en lo que respecta de la protección de datos personales, se concluye que, si bien la normativa ecuatoriana contempla una protección jurídica reciente instaurada en el año 2021 y en base a los criterios de la Unión Europea, aún no garantiza una eficaz protección. Este criterio recoge incluso los profesionales entrevistados, pues es evidente que el avance tecnológico evoluciona de manera que deja al derecho en una desactualización constante. Además, del análisis comparativo sobre la protección jurídica penal que	digital. Es importante la implementación de políticas públicas capaces de proteger los datos personales inmersos en soportes informáticos públicos y privados. • Se recomienda que los legisladores, académicos y profesionales del derecho e informática trabajen conjuntamente para crear un entorno regulatorio que garantice la protección efectiva de los datos personales, promoviendo así un equilibrio entre innovación tecnológica y respeto a los derechos humanos, asegurando que las personas puedan navegar en el mundo digital sin temor a sufrir violaciones a su intimidad. • Es importante que el legislador tome en cuenta los criterios establecidos en el Reglamento General de Protección de Datos Personales de la Unión Europea, normativa que instaura estándares para el tratamiento y protección de datos personales. En suma, se deben incluir mecanismos efectivos de supervisión y sanciones para garantizar su cumplimiento. La creación de organismos nacionales que tengan como fin garantizar el cumplimiento del ordenamiento jurídico sobre la protección de datos personales.

otorga cada legislación al uso o tratamiento de datos personales sensible se verifica que la legislación ecuatoriana penal no contempla una sanción al uso de este tipo de datos que afecta a la intimidad, sino que se lo sanciona de manera generalizada.	
Objetivo específico 2: Establecer de qué manera el tratamiento de datos personales en redes digitales conlleva al cometimiento del delito de suplantación de identidad con contenido sexual en el contexto digital.	
Conclusiones	**Recomendaciones**
• Con la revolución tecnológica que se vive en las últimas décadas, a través de redes digitales se recogen y almacenan gran cantidad de datos personales sin garantizar la transparencia o seguridad adecuada a la hora de su tratamiento. El tratamiento de estos datos es regulado por la Ley de Protección de Datos Personales, en la cual se engloba una definición amplia y establece la obligación de respetar los principios establecidos en la normativa. Sin embargo, esta ley se refiere en gran medida al tratamiento de datos personales que las entidades públicas y privadas realizan sobre la base de datos recogidas en sus sistemas, dejando de lado el tratamiento que los particulares pueden efectuar sobre los datos personales de otros individuos. En este mismo sentido, la Sentencia No. 2064-EP deja abierta la posibilidad a los operadores de justicia de determinar cuándo	• Es importante la instauración de marcos normativos específicos que se adapten al avance tecnológico y regule el tratamiento de datos personales de particulares a particulares, asegurando una efectiva protección frente a usos ilícitos. Ya que en la actualidad se evidencia una brecha significativa entre el desarrollo de la tecnología y la legislación. La normativa que se sugiere debe mantener un enfoque de género, ya que la investigación ha demostrado que delitos como la suplantación de identidad con contenido sexual afecta de forma desproporcionada a las mujeres. • La legislación debe mantener un enfoque de género, dado que las investigaciones han demostrado que delitos como la suplantación de identidad afectan desproporcionadamente a las mujeres. Esto implica que cualquier normativa nueva debe

una persona hace un tratamiento de datos personales, pero no establece lineamientos claros para determinar esta situación. Este tratamiento masivo y no regulado adecuadamente permite la entrada actos delictivos como la suplantación de identidad, pues los datos son recolectados a través de redes sociales y demás y son usados para la creación de perfiles falsos o para manipular el contenido personal, facilitando el cometimiento de este delito con un enfoque sexual. • Los datos personales son el componente para determinar la identidad de una persona dentro de un colectivo. El derecho a la identidad es reconocido en el Constitución de la República del Ecuador y en instrumentos internacionales en materia de Derechos Humanos. En la actualidad se habla de una identidad digital basada en atributos personales como imágenes, videos y otra información compartida en redes digitales de comunicación, constituye un blanco vulnerable. El tratamiento inadecuado de esta información pone en tela de duda no solo el derecho a la privacidad, sino derechos conexos como la intimidad, buen nombre, imagen, identidad. En la actualidad, el avance de la tecnología y el surgimiento de la Inteligencia Artificial ha permitido la creación de nuevas herramientas	contemplar medidas específicas para proteger a este grupo vulnerable. La jurisprudencia existente, como la Sentencia No. 2064-EP de la Corte Constitucional del Ecuador, proporciona un marco útil para entender los derechos vinculados a la protección de datos personales y debería ser utilizada como referencia para desarrollar políticas más eficaces. • La investigación sobre delitos como la suplantación de identidad requiere el uso de informes periciales informáticos y cooperación internacional. Es importante establecer protocolos claros para la recopilación y análisis de evidencia digital, así como fomentar la colaboración entre países para abordar estos delitos que a menudo cruzan fronteras. Esto permitirá una respuesta más efectiva ante el uso indebido de tecnologías avanzadas, como el deepfake. • Es preciso el fortalecimiento de los procesos de investigación y protección de las víctimas, especialmente en un entorno donde la tecnología y la inteligencia artificial complican la identificación de los infractores. Para ello, se debe fomentar capacitación continua de fiscales y personal judicial en el uso de herramientas informáticas y técnicas forenses digitales, para realizar investigaciones efectivas y precisas.

tecnológicas como el *deepfake* que efectúa una manipulación y creación de representaciones falsas de individuos a partir de sus datos. Estas tecnologías es un factor crítico a través del cual se ilustra como el tratamiento de datos personales combinado con las tecnologías avanzadas facilita la creación de contenido sexual no consentido en donde las principales víctimas son las mujeres. • La investigación para la determinación de un hecho punible en los casos de suplantación de identidad con contenido sexual en el contexto digital requiere de informes periciales informáticos y cooperación internacional debido a que los infractores realizan o utilizan los medios tecnológicos para cometer el acto punible. Las y los fiscales han señalado que esta conducta principalmente tiene como víctimas a las mujeres, debido al sistema social que coloca a la mujer como objeto sexual. Añadido a esto, herramientas digitales de la Inteligencia Artificial hacen que la conducta y la determinación del responsable sea difícil de investigar en el campo tecnológico. • Con los criterios adoptados por los entrevistados, se ha logrado evidenciar que efectivamente el uso de datos personales para cometer actos como suplantar la identidad de otra persona en el	• Se recomienda fortalecer la cooperación internacional e interinstitucional entre autoridades judiciales y policiales, dado que los delitos cibernéticos con frecuencia trascienden fronteras. Esto puede incluir la creación de redes de colaboración con organismos internacionales que faciliten el intercambio de información y recursos para abordad eficazmente estas conductas. • El desarrollo de campañas de sensibilización dirigidas a la sociedad civil en genera, sobre las implicaciones del acoso digital y la suplantación de identidad, con un enfoque en la protección de las víctimas. Estas campañas deberán promover una cultura de respeto y dignidad hacia todas las personas, así como informar los recursos legales que están a disponibilidad de las víctimas. • Se debe considerar la regulación y supervisión del uso de herramientas de inteligencia artificial para garantizar que no se utilicen para perpetuar abusos o facilitar la suplantación de identidad. Esto incluye establecer marcos éticos claros y mecanismos de responsabilidad para los desarrolladores y proveedores de tecnología. Con estas acciones, se puede avanzar hacia un entorno digital más seguro y justo, donde se

contexto digital, es un tratamiento de datos personales, pero le corresponde al juzgador emitir su análisis en cada caso concreto, esto en relación con lo que determina la doctrina, el ordenamiento jurídico, el criterio de los profesionales y las cuestiones desarrolladas en la sentencia. • Es necesario la adecuación del tipo penal de violación a la intimidad, con la finalidad de sancionar estas conductas que afectan derechos fundamentales como el honor, imagen, buen nombre, dignidad, entre otros. Esta adecuación debe incluir las nuevas modalidades del uso de datos personales sensibles como fotos íntimas en plataformas digitales e incluir una reparación integral a favor de la víctima.	protejan los derechos de todas las personas, especialmente las más vulnerables (NNA).
Objetivo específico 3: Evaluar la eficacia de la Sentencia No. 2064-14-EP/21 de la Corte Constitucional del Ecuador en la prevención y sanción de la conducta de suplantación de identidad con contenido sexual considerando la legislación ecuatoriana vigente y jurisprudencia relevante.	
Conclusiones	**Recomendaciones**

• La sentencia 2064-14/EP de la Corte Constitucional del Ecuador desarrolla las definiciones de los derechos vinculados a la protección de datos personales con un enfoque en la tutela judicial en la era digital. Además, establece parámetros para la consecución de la acción constitucional del hábeas data, dejando a salvo la vía ordinaria en los casos de la utilización sin consentimiento de datos personales. El desarrollo jurisprudencial en esta línea adquiere una relevancia significativa para garantizar el efectivo goce de los derechos constitucionales en un mundo cada vez más digitalizado. Dicta los parámetros a considerar por parte tanto de jueces constitucionales como juezas y jueces en la vía ordinaria. • La acción constitucional del hábeas data debe ser vista como una herramienta complementaria al derecho penal, permitiendo respuestas rápidas para salvaguardar derechos fundamentales, pero no debe ser la única vía para sancionar el uso arbitrario de datos. En este sentido, se debe fomentar la colaboración entre instituciones para investigar delitos relacionados con la suplantación de identidad, asegurando así una respuesta integral y efectiva.	• Se recomienda implementar capacitaciones sobre los derechos en la era digital a las personas que integran el sistema judicial en general y a toda la sociedad civil en general. La sensibilización sobre el suso responsable de la información y datos personales, y las implicaciones legales del tratamiento indebido contribuirá a crear un entorno digital más seguro. Puesto que, es necesario que los operadores de justicia, incluidos jueces y fiscales, estén capacitados para interpretar y aplicar estas normativas en casos relacionados con el uso indebido de datos personales. • La suplantación de identidad con contenido sexual representa una grave violación a varios bienes jurídicos protegidos por el ordenamiento jurídico, incluyendo la identidad digital y física, así como la intimidad de las personas. Para abordar adecuadamente esta problemática, es fundamental que los operadores de justicia consideren los principios establecidos en la Sentencia No. 2064-14-EP de la Corte Constitucional del Ecuador. Esta sentencia proporciona un marco para analizar los derechos constitucionales que se ven afectados en el contexto digital, permitiendo una evaluación más integral de las circunstancias específicas de cada caso.

• Sin bien la acción constitucional de hábeas data permite una respuesta oportuna y pronta para salvaguardar los derechos constitucionales en torno a la protección de datos personales en el mundo digital, no es la vía idónea para sancionar la conducta arbitraria del uso de datos personales para obtener beneficio propio. En este sentido, el derecho penal aparece como una vía ordinaria idónea para sancionar esta conducta y ordenar la reparación integral de la víctima. Es así como, la presentación de una acción de hábeas data en sede constitucional no limita a la víctima a iniciar un proceso penal que active el *ius puniendi* del Estado. • En los casos de suplantación de identidad con contenido sexual, el análisis de mérito desarrollado por la Corte Constitucional en la sentencia 2064-14-EP le permite al juzgador analizar de forma amplia el bien jurídico lesionado, con una visión integral, que no incluye únicamente la identidad y los datos personales en el espacio físico, sino que abarca los presupuestos del espacio virtual en el que actualmente la sociedad interactúa continuamente, estableciendo los mecanismos idóneos para evitar la revictimización de la víctima y una reparación integral. En este escenario, la Corte reconoce que las imágenes intimas	• Es necesario la difusión de la Sentencia 2064-14-EP/21 a los operadores de justicia, a fin de que tengan el conocimiento sobre las cuestiones aludidas por la Corte Constitucional en lo que respecta derechos fundamentales en la era digital. • Se recomienda que el proceso penal éxito un acompañamiento continuo de profesionales en el área psicológica, esto debido a las graves afectaciones que provoca la exposición de datos personales sensibles de la víctima, a fin de precautelar su salud psicológica y psicosexual. Este apoyo especializado es fundamental para garantizar el bienestar emocional de la persona afectada y facilitar su recuperación durante todo el proceso judicial.

forman parte de los datos personales de carácter sensible y por tanto de la identidad de una persona, por lo que los jueces en materia penal deben tener en cuenta este presupuesto a la hora de juzgar la conducta penalmente relevante. • La conducta de suplantar la identidad con contenido sexual afecta a varios bienes jurídicos protegidos por el ordenamiento jurídico, como la identidad (digital o física) e intimidad. Para la determinación de sanciones es importante que los operadores de justicia consideren los presupuestos establecidos por la Corte Constitucional del Ecuador en la sentencia 2064.14. EP en dónde se desarrolla el análisis de los derechos constitucionales que influyen en el contexto digital. Si bien la normativa incluye sanciones sobre el uso de datos personales sensibles como fotos íntimas, este es muy amplio y es necesario el análisis del caso concreto, la afectación que recibe la víctima y las repercusiones en la vida de la víctima, su intimidad personal y familiar. • La legislación debe incluir mecanismos que garanticen una reparación integral a las víctimas de suplantación de identidad. Esto no solo implica sanciones para los infractores, sino también apoyo psicológico y emocional para las víctimas, así	

como medidas que les permitan recuperar su dignidad e integridad personal. La reparación debe ser parte fundamental del proceso judicial para asegurar que se aborden adecuadamente las secuelas del delito.	

C. MATERIALES DE REFERENCIA

Referencias Bibliográficas

Agencia de Regulación y Control de las Telecomunicaciones (s.f). Protocolo de seguridad para evitar la suplantación de identidad. https://www.arcotel.gob.ec/protocolo-de-seguridad-para-evitar-la-suplantacion-de-identidad/

Aquino, N. (2020). Comparación de regulaciones jurídicas sobre la prevención del robo de identidad entre México y Argentina del año 2010 al 2018. [Tesis de licenciatura, Universidad Autónoma del Estado de México]. Universidad Autónoma del Estado de México. http://ri.uaemex.mx/handle/20.500.11799/112985

Arce, G. (2022). *LA PROTECCIÓN DE DATOS SENSIBLES A TRAVÉS DE LA GARANTÍA JURISDICCIONAL DE HÁBEAS DATA. ANÁLISIS DE LA SENTENCIA No. 2064- 14-EP/21 DE LA CORTE CONSTITUCIONAL DEL ECUADOR*. [Tesis de maestría, Universidad Tecnológica Indoamérica]. Archivo digital. https://repositorio.uti.edu.ec/bitstream/123456789/4911/1/ARCE%20CORDERO%20GRACE%20DAYANA.pdf

Arévalo, S. (2022). *Prevención en delitos informáticos.* Fundación Universitaria San Mateo Editorial. https://elibro-net.uta.lookproxy.com/es/ereader/uta/219190?page=1

Argüello, M. (31, enero de 2022). Episodio 2: Los datos personales y su naturaleza jurídica. Derecho e Inversión. https://www.derechoeinversion.com/post/datos-personales-y-naturaleza-juridica

Asamblea General de la ONU. (1948). Declaración Universal de Derechos Humano (217 [lll]. París.

Asamblea Nacional del Ecuador. (2021, 21 de mayo). Ley orgánica de protección de datos personales. *Registro Oficial Suplemento* 459. https://www.lexis.com.ec/biblioteca/ley-organica-proteccion-datos-personales

Asamblea Nacional. (2015, 18 de febrero). Ley Orgánica de Telecomunicaciones. *Registro Oficial Suplemento 439.* https://www.lexis.com.ec/biblioteca/ley-organica-telecomunicaciones

Ayjón, M. M. (2020). *La protección de datos de carácter personal en la justicia penal:* (ed.). J.M. BOSCH EDITOR. https://elibro-net.uta.lookproxy.com/es/ereader/uta/130486?page=93

Baño, A. y Reyes, J. (2020). Vulneración del derecho a la intimidad personal y familiar en las redes sociales. *Crítica y Derecho Revista Jurídica, 1 (1),* 49-60. https://revistadigital.uce.edu.ec/index.php/criticayderecho/article/view/2447/2518

Barriuso, C. (2009). Las redes sociales y la protección de datos hoy. Anuario Facultad de Derecho – Universidad de Alcalá II, 301-338.

Batuecas Caletrío, A. (2022). El Derecho a la identidad y la identidad digital. *Anuario de derecho civil*, 923-986. https://www.boe.es/biblioteca_juridica/anuarios_derecho/abrir_pdf.php?id=ANU-C-2022-30092300986

Bautista, M. (2015). *El derecho a la intimidad y su disponibilidad pública:* (ed.). Universidad Católica de Colombia. https://elibro-net.uta.lookproxy.com/es/ereader/uta/70926?page=18

BBC News. (2023, septiembre 23). AI-generated naked child images shock Spanish town of Almendralejo. BBC News. https://www.bbc.com/news/world-europe-66877718

Benavente, H. (2023). *Los métodos y sistemas de la teoría del delito:* (1 ed.). J.M. BOSCH EDITOR. https://elibro-net.uta.lookproxy.com/es/ereader/uta/232962?page=22

Benavides-Benalcázar, M. M. (2019). La reparación integral de la víctima en el proceso penal. *Revista Internacional de Investigación en Ciencias Sociales*, *15*(2), 279-317. http://scielo.iics.una.py/scielo.php?script=sci_arttext&pid=S2226-40002019000200279

Borghello, C. y Temperini, M. (27-31 de agosto de 2012). *Suplantación de Identidad Digital como delito informático en Argentina*. X Simposio Argentino de Informática y Derecho. Sociedad Argentina de Informática e Investigación Operativa, La Plata, Argentina. https://sedici.unlp.edu.ar/handle/10915/124395

Buitrago, A. (2004): *La reforma procesal penal en Colombia.* Editorial ABC.

Burzaco Samper, M. (2020). *Protección de datos personales.* Dykinson. https://elibro-net.uta.lookproxy.com/es/ereader/uta/160010?page=27

Bustamante Requena, J. F. (2020). *Entre el dolo y la culpa: ¿cabe una responsabilidad penal por "conducta arriesgada"?:* (1 ed.). Ediciones Olejnik. https://elibro-net.uta.lookproxy.com/es/lc/uta/titulos/234672

Cabrera Reynoso, S., Dávalos Adad, A., Sánchez Castro, M. y Okamoto Tanada, J. (2019). EFECTOS LEGALES Y FISCALES DE LA SUPLANTACIÓN DE IDENTIDAD DIGITAL. Global Conference on Business and Finance Proceedings. 14 (2), 242- 251. https://www.researchgate.net/profile/Gerardo-Pedraza-Vega/publication/334683140_DIAGNOSTICO_DE_LOS_PROCESOS_QUE_ADELANTA_EL_CENTRO_REGIONAL_IBAGUE_EN_EL_CUMPLIMIENTO_DEL_SISTEMA_DE_INVESTIGACION/links/5d39e0d24585153e5921d5ce/DIAGNOSTICO-DE-LOS-PROCESOS-QUE-ADELANTA-EL-CENTRO-REGIONAL-IBAGUE-EN-EL-CUMPLIMIENTO-DEL-SISTEMA-DE-INVESTIGACION.pdf#page=248

Casquete, C. (2023). La sobreexposición de menores en redes sociales, vulneración de su derecho al honor, la intimidad y la propia imagen. [Tesis de grado, Universidad de Valladolid]. Universidad de Valladolid. Facultad de Derecho. https://uvadoc.uva.es/handle/10324/66528

Castillo, M. (2024). Investigación de ciberdelitos como medio de tutela judicial efectiva. [Proyecto de investigación previo a la obtención de título de Abogada, Pontifica Universidad Católica del Ecuador Sede Ambato]. https://repositorio.puce.edu.ec/server/api/core/bitstreams/ef2e7d83-5602-432d-b913-ec271dd44382/content

Cazurro, V. (2020). *Antecedentes y fundamentos del Derecho a la protección de datos:* (ed.). J.M. BOSCH EDITOR. https://elibro-net.uta.lookproxy.com/es/ereader/uta/130485?page=79

Cisneros Rodríguez, J. (2020). Control de mérito en la acción extraordinaria de protección. *Revista Ruptura*, (02), 211-225. https://doi.org/10.26807/rr.vi02.29

Código Orgánico Integral Penal [COIP]. Registro Oficial Suplemento Número 180. 10 de febrero de 2014 (Ecuador). https://www.lexis.com.ec/biblioteca/coip

Comisión Europea de Derechos Humanos. (s.f) *Guía sobre el artículo 8 del Convenio Europeo de Derechos Humanos.* https://ks.echr.coe.int/documents/d/echr-ks/guide_art_8_spa

Conde, C. (2006). *La protección de datos personales: un derecho autónomo con base en los conceptos de intimidad y privacidad:* (ed.). Dykinson. https://elibro-net.uta.lookproxy.com/es/ereader/uta/60914?page=20

Congreso de Colombia. (2000, julio 24). Ley 599 de 2000. *Diario Oficial 44097.* https://www.funcionpublica.gov.co/eva/gestornormativo/norma_pdf.php?i=6388

Congreso de Colombia. (2012, 17 de octubre). Ley Estatutaria 1581 de 2012. *Diario Oficial 48587.* *https://www.funcionpublica.gov.co/eva/gestornormativo/norma_pdf.php?i=49981*

Consejo de Europa. (1981, 25 de enero). Convenio N° 108 del Consejo de Europa para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal. *Boletín Oficial del Estado núm.* 274 de 15-11-1985. https://www.oas.org/es/sla/ddi/docs/Convenio_108_CE.pdf

Constitución de la República del Ecuador [CRE]. 24 de julio de 2008 (Ecuador). https://www.lexis.com.ec/biblioteca/constitucion-republica-ecuador

Constitución Política de los Estados Unidos Mexicanos [Const]. (1917). Diario Oficial de la Federación el 5 de febrero de 1917. https://www.diputados.gob.mx/LeyesBiblio/pdf/CPEUM.pdf

Cornejo Aguiar, J. y Maza Gonza, J. (2023). *Teorías en torno al error de tipo y el acto:* (1 ed.). Ediciones Olejnik. https://elibro-net.uta.lookproxy.com/es/ereader/uta/258101?page=7

Cornejo Ramos, S. y Sánchez, D. (2023). La protección de datos de carácter personal frente al delito de interceptación ilegal de datos. *Código Científico Revista de Investigación*, *4*(E2), 984-1023. http://revistacodigocientifico.itslosandes.net/index.php/1/article/view/192/401

Corral Jurado, J., y Peschard Mariscal, J. (2010). *Protección de datos personales compendio de lecturas y legislación*. D-R Tiro Corto Editores. https://archivos.juridicas.unam.mx/www/bjv/libros/12/5669/31.pdf

Corte Constitucional del Ecuador. (2019). Somos una nueva Corte Constitucional Gestión 2019. https://esacc.corteconstitucional.gob.ec/storage/api/v1/10_DWL_FL/e2NhcnBldGE6I

CJ3YnJlbmRpMjAyMyIsIHV1aWQ6IjdmYzBmYTQxLTQ0NWItNGM2NC1hNzMyLTgyOTBiZjYzMTg1NC5wZGYifQ==

Creus, C. (s.f). *Esquema de Derecho Penal. Parte General*. Editorial Jurídico Andina.

Cristea Uivaru, L. (2018). *La protección de datos de carácter sensible: historia clínica digital y big data en salud*. J.M. BOSCH EDITOR. https://elibro-net.uta.lookproxy.com/es/ereader/uta/121639?page=44

Dávila, L. (2022). El control de mérito como mecanismo para garantizar la tutela de los derechos. [Tesis de maestría, Universidad de Las Américas]. Repositorio Digital de la Universidad de Las Américas. https://dspace.udla.edu.ec/handle/33000/14554

De Miguel Asensio, P. (2023). Redes sociales y datos personales: bases jurídicas para el tratamiento e implicación de las autoridades de defensa de la competencia. *La Ley Unión Europea*, (117), 1-13. https://docta.ucm.es/rest/api/core/bitstreams/6030f3a6-7126-4368-a095-9dda67027c59/content

Diccionario panhispánico del español jurídico. https://dpej.rae.es/lema/bien-jur%C3%ADdico

Equipo de comunicaciones y Escuela de Seguridad Digital. (11 de 10 de 2021). ¿Qué es una suplantación de identidad digital y cómo puede afectarte? Obtenido de Uso estratégico de 79 internet para el desarrollo: https://colnodo.apc.org/es/experiencias/que-es-unasuplantacion-deidentidad-digital-y-como-puede-afectarte

Fernández Burgueño, Pablo (2012). Aspectos jurídicos de la identidad digital y la reputación online. En: adComunica. Revista Científica de Estrategias, Tenden-cias e Innovación en Comunicación, nº3. Castellón: Asociación para el Desarro-llo de la Comunicación adComunica, Universidad Complutense de Madrid y Uni-versitat Jaume I, 125-142. DOI: http://dx.doi.org/10.6035/2174-0992.2012.3.8

Fernández, D. y Martínez, G. *Ciberdelitos*. (ed). Ediciones Experiencia. https://elibro-net.uta.lookproxy.com/es/ereader/uta/167811?page=19

Flores, J., Vinces, G. & Hidalgo, A. (2024). La protección de datos y el derecho a la intimidad en Ecuador ante la difusión no consentida de contenido íntimo. *Universidad San Gregorio de Portoviejo*. http://repositorio.sangregorio.edu.ec/handle/123456789/3633

Galino, M. (2024). Suplantación de identidad digital. *Revista de Derecho Público.* 72(1) 199-228. https://dialnet.unirioja.es/servlet/articulo?codigo=9598609

Gallardo, E. (2017). Metodología de la investigación: manual autoformativo interactivo. Huancayo: Universidad Continental. https://repositorio.continental.edu.pe/bitstream/20.500.12394/4278/1/DO_UC_EG_MAI_UC0584_2018.pdf

Gallardo, M. (2023). *El delito informático y el perito forense digital.* [Tesis de maestría, Universidad de San Carlos de Guatemala]. Archivo digital. https://www.glifos.biblioteca.cunoc.edu.gt/library/images/9/96/Tesis-165-Gallardo_Tobar%2C_Max_Otoniel.-_2023.pdf

García, A. (2007). LA PROTECCIÓN DE DATOS PERSONALES: DERECHO FUNDAMENTAL DEL SIGLO XXI. UN ESTUDIO COMPARADO. *Boletín Mexicano de Derecho Comparado,* 120, 743- 778. https://www.scielo.org.mx/pdf/bmdc/v40n120/v40n120a3.pdf

García, F. (2021). «Deepfakes»: el próximo reto en la detección de noticias falsas. *Anàlisi: Quaderns de Comunicació i Cultura*, (64), 103-120. https://doi.org/10.5565/rev/analisi.3378

Gercke, M. (2013). Enfoques jurídicos para tipificar el delito de hurto de identidad. En Manual sobre los delitos relacionados con la identidad (pp. 1–151). UNODC, Oficina de las Naciones Unidas Contra la Droga y el Delito. https://www.unodc.org/documents/organized-crime/13-83700_Ebook.pdf

Gil, E. (2022). *El interés legítimo en el tratamiento de datos personales.* (1 ed). LA LEY Soluciones Legales S.A. https://elibro-net.uta.lookproxy.com/es/ereader/uta/218734?page=26

Gómez Córdova, A., Arévalo Leal, S., Bernal Camargo, D. y Rosero de los Ríos, D. (2020). El derecho a la protección de datos personales, tecnologías digitales y pandemia por COVID-19 en Colombia. *Revista de Bioética y Derecho,* (50), 271-294. http://scielo.isciii.es/scielo.php?script=sci_arttext&pid=S1886-58872020000300017&lng=es&tlng=es

Gómez, J. y Ortiz, R. (2012). *Miradas a las Identidades digitales: un análisis del discurso de las Interacciones de las y los usuarios de la Red Social Digital Facebbok:* (ed). D - Universidad de los Andes Venezuela. https://elibro-net.uta.lookproxy.com/es/ereader/uta/118058?page=2

Graf Zu Dohna, A. (2018). *La estructura de la Teoría del Delito:* (1 ed.). Ediciones Olejnik. https://elibro-net.uta.lookproxy.com/es/lc/uta/titulos/234833

Grupo de protección de las personas en lo que respecta al tratamiento de Datos Personales (2007). Dictamen 4/2007 sobre el concepto de datos personales. https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2007/wp136_es.pdf

Guerra, D., Madera., N., Blanco, S. y Quimbayo, W. (2024). La identidad digital como contenido del derecho a la seguridad personal en la era de la IA. *Revista Tejidos Sociales.* 6(1) 1-16. https://revistas.unisimon.edu.co/index.php/tejsociales/article/view/7807

Guijosa, E. (2013). Protección de Datos Personales en Redes Sociales Digitales. [Tesis de licenciatura académica, Universidad Autónoma del Estado de México]. Repositorio Institucional UAEMEX. http://hdl.handle.net/20.500.11799/30086

Guzmán, L., Varela, W. y Briceño, M. (s.f). Ciberseguridad 4.0: Factores que propician el delito de robo de identidad digital por medios informáticos. *Red internacional de investigadores en competitividad.* 658-677. https://riico.net/index.php/riico/article/view/1818/1577

Heidari, A., Jafari Navimipour, N., Dag, H. y Unal, M. (2023). Deepfake detection using deep learning methods: A systematic and comprehensive review. *WIREs Data Mining and Knowledge Discover*y, *14*(2). 20-45. https://doi.org/10.1002/widm.1520

Hernández López, J. (2023). *¿Por qué debemos proteger la privacidad? Cronología, textos y notas sobre intimidad, vida privada y protección de datos:* (1 ed.). J.M. BOSCH EDITOR. https://elibro-net.uta.lookproxy.com/es/ereader/uta/249512?page=245

Hernández Sampieri, R. Fernández Collado, C. y Baptista Lucio, M. (2014). *Metodología de la investigación (6.a ed.).* McGraw- Hill Interamericana. https://apiperiodico.jalisco.gob.mx/api/sites/periodicooficial.jalisco.gob.mx/files/metodologia_de_la_investigacion_-_roberto_hernandez_sampieri.pdf

Hernández Valle, R. (2009). *Delimitación de los derechos a la intimidad y de información en la doctrina y jurisprudencia costarricense:* (ed.). Red Estudios Constitucionales. https://elibro-net.uta.lookproxy.com/es/ereader/uta/98387?page=8

Hernández Vera, D. (2019). La Suplantación de Identidad Cibernética en el Ecuador [Tesis de maestría, Universidad Externado de Colombia]. Universidad Externado de Colombia. https://bdigital.uexternado.edu.co/entities/publication/e4c9884a-ad38-4350-a324-fc732276eb93

Herrán, A, (1998). *La violación a la intimidad en la protección de datos personales.* Dykinson.

Herrera, P. (2016). El derecho a la vida privada y las redes sociales en Chile. *Revista Chilena de Derecho y Tecnología, 5*(1), 87-112. https://dx.doi.org/10.5354/0719-2584.2016.41268

Instituto Nacional de Tecnologías de la Comunicación (INTECO). (2009). *Estudio sobre la privacidad de los datos personales y la seguridad de la información en las redes sociales online.* Madrid: Instituto Nacional de Tecnologías de la Comunicación. https://www.uv.es/limprot/boletin9/inteco.pdf

Jara, N. (2021). El derecho de propiedad sobre los datos. *Revista Chilena de Derecho Privado,* 101-142. https://www.scielo.cl/pdf/rchdp/ntematico/0718-8072-rchdp-thematic-0101.pdf

Jefatura del Estado. (1995, 24 de noviembre). Ley Orgánica 10/1995, de 23 de noviembre, del Código Penal. *Boletín Oficial del Estado* núm. 281. https://www.boe.es/buscar/pdf/1995/BOE-A-1995-25444-consolidado.pdf

Jefatura del Estado. (2002, 11 de julio). Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico. https://www.boe.es/buscar/pdf/2002/BOE-A-2002-13758-consolidado.pdf

Jefatura del Estado. (2018, 06 de diciembre). Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales. *Boletín Oficial del Estado* Núm. 294. https://www.boe.es/buscar/pdf/2018/BOE-A-2018-16673-consolidado.pdf

Jefatura del Estado. (2021, 27 de mayo). Ley Orgánica 7/2021, de 26 de mayo, de protección de datos personales tratados para fines de prevención, detección, investigación y enjuiciamiento de infracciones penales y de ejecución de sanciones penales. *Boletín*

Oficial del Estado Núm. 126. https://www.boe.es/boe/dias/2021/05/27/pdfs/BOE-A-2021-8806.pdf

Jefatura del Estado. (2022, 28 de junio). Ley 11/2022, de 28 de junio, General de Telecomunicaciones. *Boletín Oficial del Estado* núm. 155. https://www.boe.es/buscar/act.php?id=BOE-A-2022-10757

Lafuente, C. y Marín, A. (2008). Metodologías de la investigación en las ciencias sociales: Fases, fuentes y selección de técnicas. Revista Escuela de Administración de Negocios, (64), 5- 18. https://doi.org/10.21158/01208160.n64.2008.450

Laica, M. (2022). *DERECHO A LA PROTECCIÓN DE DATOS PERSONALES Y AUTODERTEMINACIÓN INFORMATIVA, A LA IMAGEN, A LA HONRA Y BUEN NOMBRE. ANÁLISIS DE LA SENTENCIA No. 2064-14-EP/21*. [Tesis de maestría, Universidad Tecnológica Indoamérica]. Archivo digital. https://repositorio.uti.edu.ec/bitstream/123456789/5917/1/LAICA%20SAILEMA%20MARIO%20CLEMENTE.pdf

Lawson, P. (2013). Tipología y criterios de la tipificación del delito de identidad: compendio de ejemplos de leyes pertinentes. En Manual sobre los delitos relacionados con la identidad (pp. 123–196). UNODC, Oficina de las Naciones Unidas Contra la Droga y el Delito

Liceda, E. (2011). La identidad digital. *Anales de la Facultad de Ciencias Jurídicas y Sociales, 8.* 295- 304. https://sedici.unlp.edu.ar/bitstream/handle/10915/20717/Art+23.pdf?sequence=1

Llaneza, P. (2021). Identidad digital: (ed.). LA LEY Soluciones Legales S.A. https://elibro-net.uta.lookproxy.com/es/lc/uta/titulos/196445

López, M. y Müller, M. (2019). *Bullying, ciberbullying, grooming y sexting: guía de prevención:* (ed.). Editorial Maipue. https://elibro-net.uta.lookproxy.com/es/lc/uta/titulos/126733

López, R. y Leal, J. (2018). *El derecho a la información y datos personales en México: una visión comparada con el sistema interamericano y europeo de derechos humanos.* (ed.). Dykinson. https://elibro-net.uta.lookproxy.com/es/ereader/uta/113312?page=114

Machuca Vivar, S.A., Vinueza Ochoa, N.V., Sampedro Guamán, C.R., y Santillán Molina, A.L. (2022). Habeas data y protección de datos personales en la gestión de las bases de datos. *Revista Universidad y Sociedad,* 14(2), 244- 251.

Mar, C., Barbosa, A. y Molar, J. (2020). *Metodología de la investigación. Métodos y técnicas.* EBOOK. https://books.google.com.ec/books?id=e5otEAAAQBAJ&pg=PA180&dq=metodologia+dela+investigacion+fuentes+primarias&hl=es-419&newbks=1&newbks_redir=0&sa=X&ved=2ahUKEwjCjaX4266KAxWKTjABHdJyHgEQ6AF6BAgNEAI#v=onepage&q&f=true

Martínez, G. (2023). Suplantación de identidad digital: hacia una necesaria tutela penal. *Deusto Revista de Derecho Público,* 72(1), 199-228. https://www.unodc.org/documents/organized-crime/13-83700_Ebook.pdf

Martínez, I. (2023). Sobre los métodos de la investigación jurídica. *Revista Chilena de Derecho y Ciencia Política*, *14*(1), 1-4. https://doi.org/10.7770/rchdcp-V14N1-art312

Méndez, V., y Cornejo, J. (2023). Ausencia de protección a la intimidad en la difusión de videos sexuales grabados en mutuo consentimiento. *Revista Debate Jurídico Ecuador. Revista Digital de Ciencias Jurídicas. UNIANDES.* *6*(2), 213- 232. https://revista.uniandes.edu.ec/ojs/index.php/DJE/article/view/2973/3455

Mila, F. (2023). *Manual de derecho penal: Parte general: fundamentos dogmáticos de la teoría del delito desde el funcionalismo constitucional:* (1 ed.). J.M. BOSCH EDITOR. https://elibro-net.uta.lookproxy.com/es/ereader/uta/232935?page=278

Ministerio de la Presidencia, Relaciones con las Cortes y Memoria Democrática. Real Decreto 389/2021, de 1 de junio, por el que se aprueba el Estatuto de la Agencia Española de Protección de Datos. *Boletín Oficial del Estado* núm. 131. https://www.boe.es/buscar/act.php?id=BOE-A-2021-9175

Moreno Arvelo, P. M., Paucar Paucar, C. E. y Cajas Parraga, C. M. (2022). Regulación global para evitar la suplantación de identidad digital. *Revista Universidad y Sociedad*, *14*(6), 690-696. http://scielo.sld.cu/scielo.php?pid=S2218-36202022000600690&script=sci_arttext&tlng=en

Nieves, Y., y Ponjuan, G. (2021). Tratamiento de datos personales y acceso a la información. Visiones a partir de la academia. *Universitas-XXI, Revista de Ciencias Sociales y Humanas*, (35), 167-185. https://doi.org/10.17163/uni.n35.2021.08

Nisa, J. (08 de octubre de 2020). *Origen jurídico histórico de la protección de datos: evolución de las diferentes teorías jurídicas que la han protegido.* ELDERECHO.COM. https://elderecho.com/origen-juridico-historico-la-proteccion-datos-evolucion-las-diferentes-teorias-juridicas-la-protegido

Oyarte, R. (2020). *Acción extraordinaria de protección:* (2 ed.). Corporación de Estudios y Publicaciones. https://elibro-net.uta.lookproxy.com/es/ereader/uta/130114?page=200

Parada, R. y Errecaborde. (2018). *Cibercrimen y delitos informáticos*. 1a ed. - Ciudad Autónoma de Buenos Aires: Erreius. https://www.pensamientopenal.com.ar/system/files/2018/09/doctrina46963.pdf

Parlamento Europeo y Consejo de la Unión Europea. (2016). Reglamento (UE) 2016/679, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos. *Diario Oficial de la Unión Europea, L 119, 1-88.* https://www.boe.es/doue/2016/119/L00001-00088.pdf

Parlamento Europeo y Consejo de la Unión Europea. (2016, 27 de abril). DIRECTIVA (UE) 2016/680 DEL PARLAMENTO EUROPEO Y DEL CONSEJO de 27 de abril de 2016 relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por parte de las autoridades competentes para fines de prevención, investigación, detección o enjuiciamiento de infracciones penales o de ejecución de sanciones penales, y a la libre circulación de dichos datos y por la que se deroga la Decisión Marco 2008/977/JAI del Consejo. *Diario Oficial de la Unión Europea.* https://www.boe.es/doue/2016/119/L00089-00131.pdf

Pedreira, F. y Escudero García, B. (2023). *La teoría jurídica del delito en un estado de derecho:* (1 ed.). J.M. BOSCH EDITOR. https://elibro-net.uta.lookproxy.com/es/ereader/uta/249527?page=24

Pérez, A. y Reyes, B. (2010). Una aproximación al ciberbullying. Ciberacoso: la tutela penal de la intimidad, la integridad y la libertad sexual en internet / coord. por Javier García

González, 2010, ISBN 978-84-9876-835-0, págs. 13-51. https://dialnet.unirioja.es/servlet/articulo?codigo=4812678

Pérez, L. Pérez, R. y Seca, M. V. (2020). *Metodología de la investigación científica:* (ed.). Editorial Maipue. https://elibro-net.uta.lookproxy.com/es/ereader/uta/138497?page=231

Peyrano, G. (2002). Datos sensibles: perfiles y regulaciones. El impacto del desarrollo tecnológico. *EL DERECHO- Boletín N° 10.651,* 511- 525. https://editorialjuris.com/administracion/frm-libros/pdf/1696600261_habeas_data.pdf#page=512

Pfeiffer, M. L. (2008). Derecho a la privacidad. Protección de los datos sensibles. *Revista colombiana de Bioética*, *3*(1), 11-36. https://www.redalyc.org/pdf/1892/189217248002.pdf

Pizarro Moreno, E. (2022). *El derecho a la intimidad de Warren y Brandeis, traduttore, traditore y notas:* (1 ed.). Dykinson. https://elibro-net.uta.lookproxy.com/es/lc/uta/titulos/217472

Plascencia, R. (2004). *Teoría del delito:* (1 ed.). Instituto de Investigaciones Jurídicas- UNAM. https://elibro-net.uta.lookproxy.com/es/ereader/uta/273711?page=45

Porcelli, A. (2019). La Protección de los Datos Personales en el Entorno Digital. Los Estándares de Protección de Datos en los Países Iberoamericanos. *Revista Quaestio Iuris, 12*(02), 465- 497. https://dialnet.unirioja.es/servlet/articulo?codigo=7751363#:~:text=A%20tales%20efectos%2C%20el%20objetivo%20del%20presente%20trabajo,de%20Protecci%C3%B3n%20de%20Datos%20en%20los%20Estados%20Iberoamericanos.

Posada, R. (2021). UNA APROXIMACIÓN A LAS DIFICULTADES EN LA INVESTIGACIÓN Y PERSECUCIÓN DE LOS CIBERCRÍMENES. *Revista Científica de Ciencias Jurídicas, Criminología y Seguridad FISCALÍA GENERAL DEL ESTADO,* 15- 33. https://www.fiscalia.gob.ec/pdf/politica-criminal/Ciberdelitos-Perfil-Criminologico.pdf

Presidencia de la República del Ecuador. (2023, 6 de noviembre). Reglamento General de la Ley Orgánica de Protección de Datos Personales. *Decreto Ejecutivo No. 904.*

https://www.telecomunicaciones.gob.ec/wp-content/uploads/2023/11/Decreto-Ejecutivo-No.-904.pdf

Ramos, F. (2024). Deepfake: Análisis de sus implicancias tecnológicas y jurídicas en la era de la Inteligencia Artificial. *Derecho Global. Estudios sobre Derecho y Justicia, 9*(27), 359-387. https://www.scielo.org.mx/scielo.php?script=sci_arttext&pid=S2448-51362024000200359

Real Academia Española y Consejo General del Poder Judicial. (2017). *Diccionario panhispánico del español jurídico* (DPEJ). Santillana.

Rebollo, L. y Serrano, M. (2019). *Manual de Protección de Datos*. Editorial Dykinson.

Roca, A. (2020). El Derecho a la Protección de Datos Personales y su reflejo en el consentimiento del interesado. *Revista de Derecho Político, 1*(108), 165-194. https://doi.org/10.5944/rdp.108.2020.27998

Roca, A. (2021). Datos, datos, datos: el dato personal, el dato no personal, el dato personal compuesto, la anonimización, la pertenencia del dato y otras cuestiones sobre datos. *Estudios de Deusto: revista de Derecho Público, 69*(1), 211-240. https://dialnet.unirioja.es/servlet/articulo?codigo=7992306

Rodríguez, J. (2019). *Figuras y responsabilidades en el tratamiento de datos personales:* (ed.). J.M. BOSCH EDITOR. https://elibro-net.uta.lookproxy.com/es/ereader/uta/127035?page=27

Rojas, N. (2023). *Metodología de la investigación para anteproyectos:* (1 ed.). Universidad Abierta para Adultos (UAPA). https://elibro-net.uta.lookproxy.com/es/ereader/uta/229656?page=136

Roldán, F. (2021). Los ejes centrales de la protección de datos: consentimiento y finalidad. Críticas y propuestas hacia una regulación de la protección de datos personales en Ecuador. *USFQ Law Review. 8*(1), 175- 202. https://doi.org/10.18272/ulr.v8i1.2184

Salazar, D. (2021). EL ROL DE LA ADMINISTRACIÓN DE JUSTICIA Y LA COOPERACIÓN INTERNACIONAL EN LA LUCHA CONTRA LA CIBERDELINCUENCIA. *Revista Científica de Ciencias Jurídicas, Criminología y Seguridad FISCALÍA GENERAL DEL ESTADO,* 8-15.

https://www.fiscalia.gob.ec/pdf/politica-criminal/Ciberdelitos-Perfil-Criminologico.pdf

Sánchez, M. (2023). El derecho a la protección de datos personales en la era digital. *Revista Eurolatinoamericana de Derecho Administrativo. 10*(1), 1- 21. https://doi.org/10.14409/redoeda.v10i1.12626

Sentencia de 6.11.2003- Asunto C-101/01. Tribunal de Justicia (D.A.P. Edward). https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=ecli:ECLI%3AEU%3AC%3A2003%3A596

Sentencia T-405/07. (2007, 24 de mayo). Corte Constitucional de Colombia (Dr. Jaime Córdoba Triviño). https://www.corteconstitucional.gov.co/relatoria/2007/T-405-07.htm

Sentencia del Tribunal de Justicia (Sala Segunda) asunto C-434/16, Peter Nowak y Data Protection Commissioner. (2017, 20 de diciembre). Tribunal de Justicia (Sr. M. Ilešič). https://curia.europa.eu/juris/document/document.jsf;jsessionid=A47D5174285AF1E96BB6B8A2312112C4?text=&docid=198059&pageIndex=0&doclang=es&mode=lst&dir=&occ=first&part=1&cid=870432

Sentencia N° 048-13-SEP-CC. (2013, 13 de julio). Corte Constitucional del Ecuador (Dr. Antonio Gagliardo Loor). https://portal.corteconstitucional.gob.ec/FichaRelatoria.aspx?numdocumento=048-13-SEP-CC

Sentencia N° 292/2024. (2023, 02 de julio). Tribunal Superior de Justicia. Sala de los Civil y Penal. (Dra. María Teresa Chacón Alonso).

Sentencia N°. 1162-12-EP/19. (2019, 02 de octubre). Corte Constitucional del Ecuador (Dra. Daniela Salazar Marín). http://doc.corteconstitucional.gob.ec:8080/alfresco/d/d/workspace/SpacesStore/e8bb1c5a-4387-4f60-a8c8-3a87d1936bf1/1162-12-ep-sentencia.pdf?guest=true

Sentencia No. 176-14-EP/19. (2019, 16 de octubre). Corte Constitucional del Ecuador (Dr. Enrique Herrería Bonnet). http://doc.corteconstitucional.gob.ec:8080/alfresco/d/d/workspace/SpacesStore/0d994286-e791-428e-87ff-d72c2e258363/0176-14-ep-sen.pdf?guest=true

Sentencia No. 1868-13-EP/20. (2020, 08 de julio). Corte Constitucional del Ecuador (Dra. Karla Andrade Quevedo). https://esacc.corteconstitucional.gob.ec/storage/api/v1/10_DWL_FL/e2NhcnBldGE6J3RyYW1pdGUnLCB1dWlkOicyNzE4ZjljZC1hZjU4LTQxMTItYjBkYi01MjVlYmUwNDU2ZjgucGRmJ30=

Sentencia No. 77-16-IN/22. (2021, 27 de enero). Corte Constitucional del Ecuador. (Carmen Corral Ponce).

Jove, D. (2021). *Tratamiento frente a dato. El problema de las categorías especiales.* [Tesis doctoral]. UDC. https://ruc.udc.es/dspace/bitstream/handle/2183/29853/Jove%20Villares_Daniel_TD_2022.pdf?sequence=2&isAllowed=y

Sentencia No. 77-16-IN/22. (2022, 27 de enero). Corte Constitucional del Ecuador (Dr. Enrique Herrería Bonnet). https://esacc.corteconstitucional.gob.ec/storage/api/v1/10_DWL_FL/e2NhcnBldGE6J3RyYW1pdGUnLCB1dWlkOiczMjdjNzdhMC0yNjMwLTRiNmItYmIyNi0wZjNjMDY3M2VlMmQucGRmJ30=

Sentencia No. SU-089/95. (1995, 01 de marzo). Corte Constitucional de Colombia (Dr. Jorge Arango Mejía). https://www.corteconstitucional.gov.co/relatoria/1995/su089-95.htm

Soler, E. (2023). Retos jurídicos derivados de la Inteligencia Artificial Generativa Deepfakes y violencia contra las mujeres como supuesto de hecho. *InDret*, 493- 515. https://indret.com/retos-juridicos-derivados-de-la-inteligencia-artificial-generativa/

Superintendencia de Industria y Comercio. (s.f.). *Misión y visión*. https://www.sic.gov.co/mision-y-vision

Tarrío, M. C. (2008). *Teoría finalista del delito y dogmática penal:* (ed.). Ediciones Cathedra Jurídica. https://elibro-net.uta.lookproxy.com/es/ereader/uta/76543?page=37

Touriño, A. (2014). *El derecho al olvido y a la intimidad en internet:* (1 ed.). Los libros de la Catarata. https://elibro-net.uta.lookproxy.com/es/ereader/uta/250019?page=57

Trejo Sánchez, K. (2021). *Fundamentos de metodología para la realización de trabajos de investigación:* (ed.). Editorial Parmenia, Universidad La Salle México. https://elibro-net.uta.lookproxy.com/es/ereader/uta/183470?page=32

Troncoso, A. (2010). *La protección de datos personales. En busca del equilibrio.* Tirant Lo Blanch.

UNESCO. (2003). *Declaración Internacional sobre los Datos Genéticos Humanos.* https://unesdoc.unesco.org/ark:/48223/pf0000136112_spa

Unión Europea. (s.f). *Supervisor Europeo de Protección de Datos (SEPD).* https://european-union.europa.eu/institutions-law-budget/institutions-and-bodies/search-all-eu-institutions-and-bodies/european-data-protection-supervisor-edps_es

UNODC Oficina de las Naciones Unidas contra la Droga y el Delito (2013). *Manual sobre los delitos relacionados con la identidad.* https://www.unodc.org/lpomex/uploads/documents/Publicaciones/Crimen/13-83700_Ebook.pdf

Vásquez, S. (2024). Las TIC, ciberdelitos, ciberdelincuencia y su impacto jurídico-social. *Voces y saberes.* (11) 37- 53. https://vocesysaberes.aragon.unam.mx/index.php/RAVS/article/view/86/86

Vidal, G. (2022). Enfoque cuantitativo: taxonomía desde el nivel de profundidad de la búsqueda del conocimiento. Llalliq, *2*(1), 13- 26. https://revistas.unasam.edu.pe/index.php/llalliq/article/view/936/997

Villagómez, B., Calle, R. y Garrido, V. (2022). La protección de datos personales en entornos digitales: Análisis de la sentencia 2064-14-EP/21. *Ius Constitutionale Revista de Derecho Constitucional*, (2), 100- 116. https://www.researchgate.net/profile/Karina-Tello-Toral/publication/359317885_El_desarrollo_pretoriano_de_la_consulta_prelegislativa_en_el_Ecuador/links/62349184d545b77294026225/El-desarrollo-pretoriano-de-la-consulta-prelegislativa-en-el-Ecuador.pdf#page=99

Villanueva, F. (2022). Metodología de la Investigación: (1 ed.). Ciudad de México, Klik Soluciones Educativas, S.A. https://www.google.com.ec/books/edition/Metodología_de_la_investigación/6e-

KEAAAQBAJ?hl=es-419&gbpv=1&dq=metodología+de+la+investigación+modalidades&printsec=frontcover

Villigua, H. (2022). *La Corte Constitucional del Ecuador y su facultad de interpretación.* [Tesis de maestría, Universidad San Gregorio de Portoviejo] *Repositorio Institucional de la Universidad San Gregorio de Portoviejo*. http://repositorio.sangregorio.edu.ec/handle/123456789/2546

Yanes, M. (2021). *El testimonio anticipado como medio de prueba en delitos de abuso sexual.* [Tesis de maestría, Universidad Andina Simón Bolívar Sede Ecuador]. Archivo digital. https://repositorio.uasb.edu.ec/bitstream/10644/8202/1/T3586-MDPE-Yanes-El%20testimonio.pdf

Zaffaroni, E. R., Alagia, A. y Slokar, A. (1998). *Manual de derecho penal* (p. 368). Ediciones Jurídicas.

Zambrano Pasquel, A. (2023). *Teoría del delito:* (1 ed.). Ediciones Olejnik. https://elibro-net.uta.lookproxy.com/es/ereader/uta/251035?page=27

Anexos

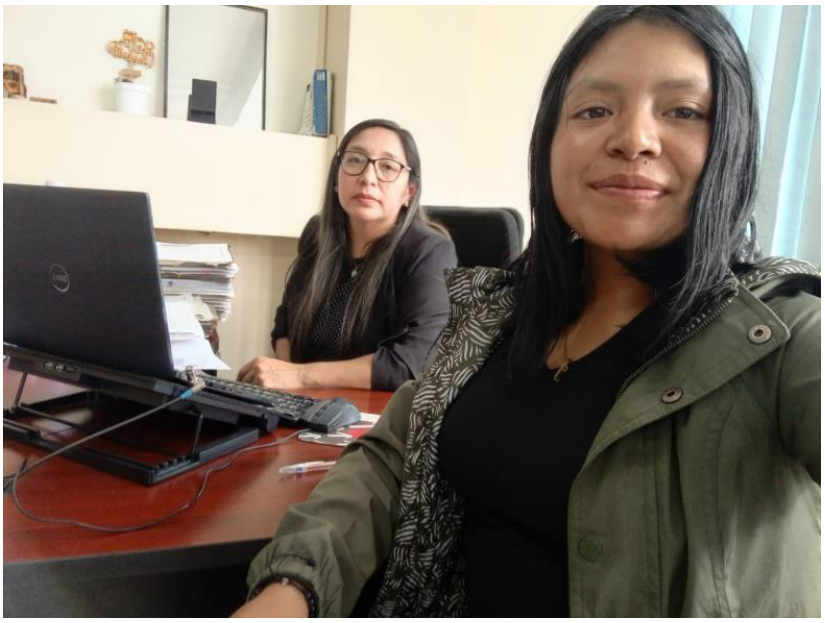


Figura 1: *Dra. Amparo Tasipanta- Fiscal Multicompetente en el cantón Latacunga.*



Figura 2: *Dra. Maricela Yánez- Fiscal de violencia de género en el cantón Latacunga.*



Figura 3: *Verónica Altamirano Guerra- Asistente de Fiscalía en el cantón Latacunga.*



Figura 4: *Dr. Jorge Nagales- Asistente de Fiscalía en el cantón Latacunga.*

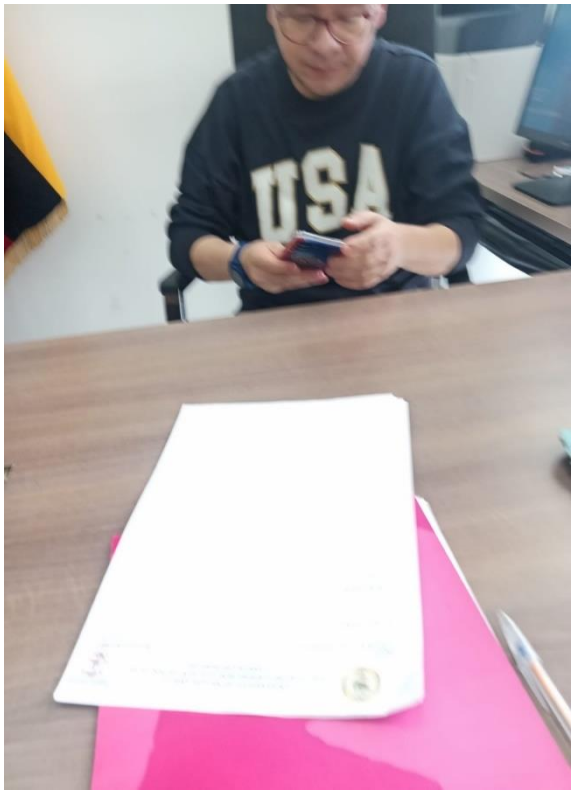


Figura 5: *Dr. Fabián Altamirano - Juez de Garantías Penales en el cantón Ambato*

Nota: Dos profesionales no dieron el consentimiento para usar fotografías personales como parte de los anexos.