DOI: https://doi.org/10.56712/latam.v4i4.1202

# Las nuevas tecnologías frente al código orgánico integral penal

New technologies versus the comprehensive organic criminal code

***Pedro José García Brito***
pedrossd82@gmail.com
Universidad Católica de Cuenca
Cuenca – Ecuador

***Cesar Leonardo Arciniegas Castro***
carciniegasc@ucacue.edu.ec
Universidad Católica de Cuenca
Cuenca – Ecuador

Artículo recibido: 18 de septiembre de 2023. Aceptado para publicación: 04 de octubre de 2023.
Conflictos de Interés: Ninguno que declarar.

## Resumen

El internet ha experimentado un crecimiento exponencial desde su creación en 1969, brindando acceso ilimitado a información rápida y precisa. Este crecimiento desmesurado de las tecnologías, aplicaciones y redes sociales, también ha dado lugar a problemas como el aumento de delitos cibernéticos, lo que ha llevado al derecho a adaptarse, crear nuevas leyes para proteger a los usuarios. Este artículo científico analiza las acciones que el Código Orgánico Integral Penal de Ecuador debería incorporar para hacer frente a las nuevas tecnologías y proteger a los usuarios. Se utiliza una metodología que combina el estudio histórico del derecho y la informática (TIC), la investigación digital además de una normativa que regule de manera eficiente la protección de datos. Se debe de entender que el derecho y la información, de alguna manera se encuentran vinculados, ya que la información cumple un papel fundamental en la construcción de valores, principios en el ejercicio de los derechos humanos. El derecho de acceso a la información pública permite a las personas formar opiniones fundamentadas, pero también busca proteger la privacidad y evitar el daño a otros. En Ecuador dentro del (COIP), sanciona a varios de estos tipos, pero se considera a las sanciones como insuficientes para abordar la diversidad de delitos que se cometen a diario. Además, se busca incorporar nuevos delitos, como la falsificación de firmas electrónicas, la responsabilidad de los usuarios, sanciones en el metaverso, clonación de tarjetas y fraude electrónico. Además, se destaca la importancia de la Ley Orgánica de Protección de Datos Personales (LOPDP), promulgada en Ecuador el 21 de mayo de 2021. Esta ley garantiza el ejercicio del derecho en base a lo que es el derecho a la protección de datos y centrar una normativa en base a principios, deberes, que se rigen para amparar la protección de datos.

*Palabras clave:* legislación, información, derecho, datos, nuevas tecnológicas, protección

## Abstract

The Internet has experienced exponential growth since its creation in 1969, providing unlimited access to fast and accurate information. This excessive growth of technologies, applications and social networks has also given rise to problems such as the increase in cybercrimes, which has led the right to adapt and create new laws to protect users. This scientific article analyzes the actions that the Comprehensive Organic Criminal Code of Ecuador should incorporate to confront new technologies and protect users. A methodology is used that combines the historical study of law and information technology (ICT), digital research as well as regulations that efficiently regulate data protection. It must be understood that law and information are somehow linked, since information plays a fundamental role in the construction of values and principles in the exercise of human rights. The right of access to public information allows people to form informed opinions, but also seeks to protect privacy and prevent harm to others. In Ecuador within the (COIP), several of these types are sanctioned, but the sanctions are considered insufficient to address the diversity of crimes that are committed daily. In addition, it seeks to incorporate new crimes, such as forgery of electronic signatures, user responsibility, sanctions in the metaverse, card cloning and electronic fraud. In addition, the importance of the Organic Law on Personal Data Protection (LOPDP) is highlighted, enacted in Ecuador on May 21, 2021. This law guarantees the exercise of the right based on what is the right to data protection and center regulations based on principles and duties that are governed to protect data protection.

*Keywords:* legislation, information, law, data, new technologies, protection



Como citar: García Brito, P. J. & Arciniegas Castro, C. L. (2023). Las nuevas tecnologías frente al código orgánico integral penal. *LATAM Revista Latinoamericana de Ciencias Sociales y Humanidades 4(4), 116–127. https://doi.org/10.56712/latam.v4i4.1202*

***INTRODUCCIÓN***

El internet surge desde el año 1969 por primera vez, desarrollado por el gobierno de Estados Unidos específicamente su departamento de defensa bajo el nombre de ARPANET esto fue creado para una comunicación de Estados Unidos. Por otra parte, se liberó y se convirtió en libre acceso en 1982, y desde entonces internet se ha convertido en un elemento que no se ha detenido por lo que su creación llevo al mundo, a un mundo digital, donde la ciudadanía tuvo acceso a información ilimitada de manera rápida, exacta, sin restricciones, por lo que como existe lo bueno también surgió lo malo en este medio digital.

Que hasta la fecha es uno de los ejes principales para el mundo, a pesar de tratar de contenerlo y de genera formas de detener su progreso con los avances tecnológicos es cada día más complejo, en nuestro caso los delitos que se cometen tienen una repercusión lo cual deja vulnerable tanto a los derechos como a las obligaciones de los usuarios

Estas nuevas tecnologías han generado que el derecho tenga que actualizarse, crear nuevas normas, leyes y reglamentos con el fin de generar una seguridad, una protección a los datos de los usuarios eso es lo que venimos a dilucidar cuales son las acciones que debería incorporar el código orgánico integral penal ecuatoriano frente a las nuevas tecnologías.

Además de la implementación de una nueva ley que busca dar un mayor soporte y de cierta manera establecer una guía que sea de utilidad para que los delitos dentro de estos sistemas digitales se vean más controlados esto no solo se da en Ecuador, sino de manera internacional también.

Se considera un problema global por lo que se ha establecido un ranking mundial sobre la ciberseguridad y los esfuerzos del mundo por combatirlos sin dejar de lado la responsabilidad proactiva de los datos de cada usuario y la divulgación de los mismo es donde la seguridad busca hacer un hincapié frente a cada dato que el usuario permite que el mundo pueda llegar a ver es por esto que también hablaremos sobre las prestaciones por parte de los servicios de telecomunicaciones frente a las medidas que deberían adoptar para regular el tipo de información que se sube y la que se puede divulgar.

***METODOLOGÍA***

La metodología en este artículo inicia con la histórica como bien sabemos tanto el derecho como la informática al pasar los años han ido evolucionando debido a esta evolución tanto el derecho como la informativa han generado un vínculo tanto es así que se ha visto en la necesidad de implementación de nuevas normativas.

Tenemos la investigación digital que no es más que la recaudación de la información para dar un análisis eficiente con respecto a lo investigado, también tenemos la metodología de la protección de datos que es centrarnos en las leyes y la regulación que estas tienen con el fin de garantizar el correcto tratamiento de la información.

Para poder establecer una regulación a estas nuevas tecnologías en búsqueda de que estas no vulneren derechos, ya que la ley de protección de datos personales está vigente en Ecuador desde mayo del año anterior, es por esto que podemos decir que existe un crecimiento masivo de las nuevas tecnologías y que el derecho está buscando recién adecuarse a esta nueva realidad.

Por otra parte, el método cualitativo ya que lo que buscamos es darle una interpretación, darles un enfoque a las nuevas tecnologías y al derecho informático desde una base fundamentada que genera sucesos de crecimiento tanto al derecho y la sociedad con respecto a las nuevas tecnologías dando una seguridad y conocimiento de estas nuevas leyes que se darán en un futuro.

***RESULTADOS Y DISCUSIÓN***

**Derecho e información**

El derecho y la información están ligados en base a una naturaleza bifronte debido a que, en determinadas ocasiones, generan una mala interpretación entre lo individual y la libertad de expresión, ya que fomentan un espacio en donde el ser concibe un espacio de autonomía.

Es aquí donde surge el derecho de cada ser humano que no es más que el acceso a la información pública generando a las personas una forma propia de crear y formar tanto su crítica como una opinión fundamentada, como se conoce la información no está restringida a las personas y por otra parte el derecho busca restringe el daño que se puede ocasionar a los demás o que las personas no invadan tanto a la privacidad como la intimidad de otras personas.

**Clasificación en emisor y receptor**

Es indispensable reconocer a dos partes dentro del derecho y la información por una parte está el derecho a quien emite la información dentro este se puede señalar:

El derecho de buscar, recolectar, investigar.

Este es el derecho primordial de cada ser humano a divulgar su información en el medio que éste considere más eficaz y de igual manera la opinión sobre los asuntos públicos.

Derecho al acceso a la fuente donde surge la información

Esta surge más cuando se habla o se trata de información pública debido a que es un instrumentó vital para el progreso de la sociedad además este es un derecho adyacente como lo es también el derecho a saber de las actividades de nuestros representantes.

**Derecho a que no exista la censura previa**

No se puede restringir la información de manera previa antes de la emisión de la información de ninguna manera por parte del estado, de privados, de manera directa o indirecta.

Por otra parte, tenemos al receptor de la información y sus derechos que son:

- Receptar la información y las opiniones que se han emitido
- Elegir la información que desea recibir, también está vinculado al derecho a la información
- Derecho a contar con una información que sea tanto oportuna como válida. (AGUADO LOPEZ & FENOLL, 2013)

**Derecho a preservar su honra**

Derecho a solicitar una sanción en caso de buscar proteger el honor la autonomía personal la privacidad la entidad de las personas como puede ser el derecho a la imagen esta puede ser proteger la información o a su difusión o el abuso de la misma.

**El derecho a la información**

La información es uno de los primeros eslabones de la construcción de valor debido a esto es constituido como un derecho inherente al ser humano, por eso surge la expresión de la soberanía popular y la información da un derecho a la igualdad, ya que esta nos iguala dando el mismo plano, aunque esto no surge en todos los casos puede chocar derechos fundamentales, acciones y ser tergiversados.

**Los nuevos fraudes, amenazas y consecuencias en la era digital.**

**Los fraudes electrónicos**

Este es un fenómeno que empieza a tener una mayor trascendencia debido a que se basa en técnicas que explotan la ingenuidad de las víctimas hasta la utilización de metodologías más complejas que son más conocidos como códigos maliciosos.

Como primera parte tenemos las amenazas silenciosas que son conocidas como malware que son inadvertidas por los usuarios esto facilita a los estafadores que logran ejecutar las acciones sin que la víctima de su consentimiento generando pequeños fraudes como para que puedan pasar desapercibidos.

Por lo que los ciberdelincuentes en un inicio eran organizaciones unipersonales o de pocos integrantes debido a que en la actualidad el internet ha generado un gran avance estas personas han formado organizaciones enfocadas en cometer ciberdelitos poseen una estructura firme y determinada para la actividad que les competa mediante la cual generan el fraude en el internet, esta situación vulnera los derechos de los individuos por lo que genera un conflicto con el derecho (AGUADO LOPEZ & FENOLL, 2013)

Lo que a la final conlleva a buscar una solución por parte del derecho con el fin de erradicar o establecer sanciones a quien cometa este tipo de delitos y fomentando reglas o normativas que la sociedad deberá de seguir con el fin de generar una seguridad a la población, es por esto que existen elementos que integran el fraude en internet y es igual que en el mundo real una personas que se lucra que se convierte en el delincuente y el perjudicado que es la víctima; los delitos más frecuentes son:

**Falsas ofertas de empleo**

La mayoría de estos fraudes tienen una aportación inicial para gastos de materiales o certificaciones que jamás llegan a su destino, por lo que el supuesto empleo certificación que jamás existió en la mayoría de estos ataques se crearon o diseñaron por páginas para extraer información bancaria y extraer dinero de los usuarios. (AGUADO LOPEZ & FENOLL, 2013))

**Venta de objetos nuevo o de segunda mano**

En 2008 y 2009 surgieron muchas estafas por estas compras, dando lugar al timo de la Thermomix, donde se ofertan productos a costos económicos, por lo que la gente enviaba dinero y su ubicación, lo que generó robos tanto del dinero enviado como de sus hogares, por que revelaban su ubicación aumentando así la información personal obtenida ilegal por los ciberdelincuentes dando lugar a amenazas y fraudes a estas personas.

**Cartas nigerianas**

Se trataba de un fraude por correo electrónico en donde se establecía que recibirías la herencia de un familiar en donde se utilizaba sellos y firmas falsificadas de manera electrónica de las autoridades correspondiente del país de donde surgía la información esto lo que pedía eran cuentas bancarias para el depósito lo que a largo plazo género una lista de datos bancarios de millones de personas que se podían vender generando un delito o infracción de la información privada de cada persona.

**Phishing**

La estafa es conocida como pesca y cosecha de claves, el término se relaciona con la captura de claves y firmas electrónicas silenciosa para realizar operaciones fraudulentas o pago de internet, es uno de los métodos que hasta ahora no tienen sanción establecida, su función era

generar un link de internet donde el usuario ingresa a la supuesta página de su banco y al ingresar esta guardaba sus claves para ocuparlas y extraer el dinero de esas cuentas.

**Pharming**

Es una versión más actual o sofisticada de phishing y del farming en donde el tráfico de datos que se encuentra en un sitio web, este sistema aprovecha los principios en donde cambian los archivos de la computadora generando un web falso, suplantando la identidad de los sitios como son los bancos y redes sociales robando los datos personales de los usuarios.

**Rogueware**

Este es un software que genera una infección falsa del sistema con la finalidad de vender antivirus que para el sistema vuelva a funcionar de la manera más adecuada pero lo que en realidad se está produciendo es un pago por el virus que ya infectó el equipo este se ha convertido en una nueva forma de estafa que está tomando un gran auge dentro de la sociedad.

En base a todos los tipos expuesto y la creación de nuevas maneras de delinquir de manera informática la normativa actual en el Ecuador no ha generado un gran aporte a la solución de estos conflictos por lo que la estafa, la violación de los derechos personales, la falsificación de documentos y el fraude están tomando un mayor auge, lo que produce una complejidad para la ciudadanía frente a la seguridad de su información. (AGUADO LOPEZ & FENOLL, 2013)

**El código orgánico integral penal en el ámbito tecnológico**

Dentro de Ecuador en su normativa (COIP) El Código Orgánico Integral Penal emite diversas sanciones que regulan a este tipo de Delitos, de una manera muy resguardada dejando de lado el gran espectro que es, por lo que se encuentra demasiado reducida y no puede

abarcar todos los tipos de delitos que en la actualidad se están generando, dentro de nuestra legislación se sanciona la pornografía infantil artículo 103, la transgresión del derecho a la privacidad, contemplado en el art. 178, revelación legal de información de base de datos, establecido por medio del art. 229; las comunicaciones interceptadas. contempladas en el art. 476; el ataque a la Integridad de los sistemas de información, dispuesto en el art. 232, los delitos en contra de la información pública que se encuentra reservada de forma legal por medio del art. 233: el ingreso no autorizado a un sistema informático o telemático de telecomunicaciones. Establecido por medio del art. 234 estos son todos los tipos penales que constan dentro del mismo cuerpo legal. (Asamblea Nacional, COIP, 2023)

Debemos tomar en consideración que la última reforma se realizó en agosto de 2021, por lo que hasta ahora se han creado nuevos delitos que deberán ser considerados, dentro de estos tenemos la falsificación de firmas electrónicas, la responsabilidad de los usuarios, sanciones en el metaverso, clonación de tarjetas, fraude electrónico.

**La incorporación de la normativa dentro de la protección de datos personales y la ciberseguridad**

Debemos tener en cuenta que desde el auge que tuvo las nuevas tecnologías el derecho se ha visto en una etapa de formación apresurada ya que está se vio forzada a la creación de nuevas normativas.

Frente a este ámbito dentro del Ecuador se vio la necesidad de la implementación y de la creación de una nueva ley orgánica que es la ley orgánica de protección de datos personales (LOPDP) se fue promulgada y aceptada el seis de mayo de dos mil veinte y tres esta ley se ha generado con una finalidad como lo establece dentro de artículo 1 dispone que, el motivo y propósito de esta

ley se centra en asegurar el pleno ejercicio del derecho a la privacidad de los datos personales, además de que se abarca la capacidad de acceder a ellos, controlarlos y por ende, garantizar una seguridad adecuada, siendo así que , para lograr este fin, se define; anticipan y desarrollan los principios, derechos, deberes y medidas de protección relevantes. (Asamblea Nacional, LOPDP, 2022)

Dicho esto, se abre la puerta a la protección de la información y por otra se hace reflexionar sobre los límites que surgen y la existencia de nuevas fuentes de derecho, por este hecho debería de coexistir una responsabilidad sobre la utilización, difusión y pertenencia de los datos personales, como establece la LOPDP ecuatoriana en su capítulo VIII la responsabilidad proactiva, dentro de este mismo cuerpo normativo establecer el artículo 78, en donde se expresa que , las empresas que ofrecen servicios de telecomunicaciones tiene la responsabilidad de aplicar medidas adecuadas de índole técnica y organizativa para garantizar la seguridad de su infraestructura, con el objetivo de proteger la confidencialidad de los datos personales. (Asamblea Nacional, LOPDP, 2022)

La falta de seguridad de estas plataformas, por ejemplo; uno de los elementos externos serían los hackers de sombrero blanco y negro o también conocidos como éticos y maliciosos; en el caso de los hackers de sobrero blanco pretende buscar las vulneraciones que existen dentro de una red o de un sistema, y reforzar para evitar la vulneración de estos.

**Ley de protección de datos personales en ecuador las brechas legales y medidas en curso**

Por otra parte, en Ecuador existe la normativa sancionadora como en la (LOPDP) Ley Orgánica de Protección de Datos Personales y el COIP (Código Orgánico Integral Penal), tomando en cuenta que la existencia de esta normativa es limitada frente a la gran cantidad de delitos tecnológicos que han surgido el sistema jurídico está teniendo una gran carencia.

Por esta carencia en el sistema jurídico los hackers de sombrero negro dentro del Ecuador se han convertido en un problema y se está buscando una manera de prevenir estos ataques a través del (MINTEL) conocido como el Ministerio De Telecomunicaciones Y De La Sociedad De La Información.

La UIT (Unión Internacional De Telecomunicaciones) la seguridad jurídica de las redes se basa en cinco pilares dentro de estos tenemos: técnicas organizativas, medidas jurídicas, operaciones y creación de capacidades, en base a esta organización y al estudio que realiza se manifiesta que; El Ecuador se halla en una etapa de fortalecimiento, ya que está comprometido en llevar a cabo acciones complejas que se encuentran orientadas a prevenir estos delitos, a mejorar y a salvaguardar las actividades tecnológicas de la sociedad en general. Esto significa que deben involucrarse en proyectos y programas vinculados a la seguridad y en el entorno digital, siendo así que, a nivel global, el país ocupa la posición 66 en el ranking de ciberseguridad, siendo el 9no en América del Norte y el 6to en América del Sur. Además, según el informe emitido en 2016 de la DEA, Ecuador ha experimentado avances notables durante los últimos años en la consolidación de sus capacidades para prevenir y responder ante amenazas informáticas. Entre las medidas sobresalientes se incluyen la implementación del COIP para combatir las actividades delictivas en línea y el desempeño del Centro de Respuesta a incidentes Informáticos de Ecuador (ECUCERTI). (MINTEL, 2021)

**La falta de normativa en Ecuador**

Para la realización de esta comparación hemos buscando uno de los países que más desarrollo ha tenido dentro de este tipo de casos, Chile en la actualidad ha sido un país que ha tomado a las nuevas tecnologías como un pilar fundamental para la creación de nuevas normativas y que

en base a este estudio hemos visto las normativas que Ecuador pudiera incorporar con la finalidad de mejorar la seguridad y crear precedentes dentro de nuestra legislación.

La legislación de Chile estableció la "Ley 21459" con la finalidad de establecer normas frente a los delitos informáticos derogando a la anterior ley además de la modificación de algunos cuerpos legales.

Esta ley fue promulgada el 09 de junio de 2022 y fue publicada el 20 julio de 2022 es la ley más actual que esta legislación tiene con referencia a los nuevos delitos.

El primer delito que podemos identificar es el de ataque, que llega a poner en peligro a la integridad de un sistema, en el cual mediante su art. 1 señala que, el atentado a la integridad de un sistema informático es aquel que interrumpa o dificulte el funcionamiento normal, ya sea en su totalidad o parcialmente, de un sistema de computación al introducir, transmitir, dañar, degradar, modificar o eliminar datos informáticos, estará sujeto a ser condenado a una pena de prisión de oscila entre un nivel medio y máximo. (Ley 21459, 2022)

Como podemos ver dentro de la normativa de Chile existe esta figura de atacar a un sistema informático mientras que en Ecuador en su artículo 190 nos dice: En los casos de apropiación fraudulenta de un sistema informático, con el objetivo de facilitar la apropiación indebida de propiedades ajenas o de promover el traspaso no autorizada de derechos, bienes o valores, causando un daño a la víctima o a terceros, ya sea en su propio beneficio o en beneficio de terceros, al inferir, manipular o modificar la operación de redes electrónicas, software, sistemas informáticos, plataformas telemáticas o dispositivos de telecomunicaciones, enfrentará una condena de prisión que variará entre uno y tres años. (Asamblea Nacional, COIP, 2023)

En base a esto vemos la inexistencia de una sanción en Ecuador frente a la Integridad de un sistema informático lo que deja en una vulneración que esta forma lo que son las nuevas tecnologías y la promulgación de una gran cantidad de sitios que están en una forma vulnerable.

Otra de las normativas que Ecuador no contempla dentro de su legislación es Interceptación ilícita que es un elemento de gran importancia ya que interferir o interrumpir la información de una o más personas deja en vulneración sus datos personales que pueden ser contraseñas, firmas electrónicas lo que puede llegar a generar un conflicto de qué tan seguro o que tan seguros están mis datos; si existe este tipo de sucesos dentro de la legislación chile existe el artículo 3 que abarca estas situaciones: 1. Quien, de manera Inapropiada, intervenga o interfiera de manera técnica en la transmisión de información que no es pública en un sistema informático o entre varios sistemas similares, enfrentará una condena de prisión de grado intermedio: .2 Del mismo modo, aquel que, sin la autorización adecuada, acceda a datos almacenados en sistemas informáticos mediante la captura de emisiones electromagnéticas emitidas por estos sistemas, será condenado a una pena de prisión que puede variar desde un nivel intermedio hasta el máximo permitido por la ley. (Ley 21459, 2022

Dentro de nuestra legislación tenemos el art. 230 numeral 1, en donde se habla acerca de la Interceptación ilegal de datos, por lo que, la persona que realice este tipo de actos llegará a ser sancionada con una pena privativa de libertad de entre tres y cinco años, por las actuaciones siguientes: si la persona que, sin una autorización judicial previa, intercepte de alguna manera un dato informático en su punto de inicio, destino o en el interior de un sistema informático, así como en una señal o transmisión de datos o señales con el propósito de obtener información almacenada o accesible para su propio beneficio o el beneficio de terceros. (Asamblea Nacional, COIP, 2023)

Por otra parte, dentro de la legislación chilena existe la sanción por el delito de receptación de datos informáticos a través de su art. 6, en el cual se manifiesta que: la persona que, teniendo

pleno conocimiento de su procedencia o sin poder evitar conocerla, comercie, transfiera o guarde datos informáticos con el mismo objetivo o con un propósito ilícito diferente en cualquier contexto, enfrentará una penalización equivalente a la establecida para las infracciones indicadas en los artículos 2, 3 y 5 reducida en un grado. (Ley 21459, 2022)

Este es uno de los artículos que dentro de la legislación de Ecuador no existe, es decir, no existe una sanción para quienes que realicen este tipo de actos delictivos lo que genera un vacío que debería ser subsanado.

Dentro de otros países como Colombia y El Salvador lo que han buscado es una regulación a este tipo de nuevas tecnologías, por lo que estas iniciativas se debería de fomentar dentro de Ecuador, por su parte en El Salvador existen las siguientes normativas el art. 4 expone que, en el caso de acceso indebido a los sistema informáticos, quien de manera deliberada y sin consentimiento, o excediendo el otorgado, ingrese, intercepte o emplee total o parcialmente un sistema informático que haga uso de Tecnologías de la Información o Tecnologías de la Comunicación, enfrentará una pena de privativa de libertad de 1 a 4 años. (Asamblea Legislativa de la República del Salvador, 2022)

Por otro lado, el artículo 8 nos habla acerca de la posesión, el uso de equipos o la prestación de servicios que pueden vulnerar la seguridad, en donde, aquel que cuente con, fabrique, proporcione, venda dispositivos, códigos maliciosos. programas informáticos, virus informáticos, contraseñas o claves de acceso diseñados para la manipulación indebida de sistemas o programas Informáticos utilizando tecnologías para la Información y comunicación, o que preste servicios con la intención de lograr los mismos propósitos en la comisión de cualquiera de los delitos establecidos en esta Ley, estará sujeto a una pena privativa que variará entre 3 y 5 años. (Asamblea Legislativa de la República del Salvador, 2022)

La legislación salvadoreña señala a través de su art. 11-A, en relación con a la falsificación de documentos y firmas, aquella persona que altere, des encripte, decodifique o de cualquier forma descifre, revele o comercie con documentos, firmas o certificados, ya sean de naturaleza digital, digitalizada o electrónica, vinculados a registros públicos o privados, se enfrentará a una pena de prisión que variará entre 3 y 6 años. (Asamblea Legislativa de la República del Salvador, 2022)

Así también la normativa que se da está dando en Colombia y que en Ecuador no ha sido considerada por el momento es:

Se puede indicar que, por medio del art. 269F, acerca de la violación de datos personales, señala que, quien, sin contar con la debida autorización y con el propósito de obtener beneficio propio o en favor de una tercera persona, obtenga, o recopile, quite, prometa, transfiera, comercie, envíe, adquiera, obstaculice, divulgue, altere o utilice códigos o datos personales alojados en archivos, ficheros, bases de datos u otros medios similares, se verá sujeto a una condena de prisión que abarcará desde 48 hasta 96 meses, además de estar sujeto a una multa que variará entre 100 y 1000 salarios mínimos legales mensuales vigentes. (República de Colombia, 2023)

De la misma manera, el art. 269G, manifiesta que, en situaciones donde se produzca la suplantación de sitios web con la finalidad de obtener datos personales de manera ilegal y sin la autorización adecuada, aquella persona que elabore, cree, venda, active, programe o transmita páginas electrónicas, enlaces o ventanas emergentes estará involucrada en dichas actividades, se verá sujeto a una pena de prisión que oscila entre 48 y 96 meses, además de una multa que variará entre 100 y 1.000 salarios mínimos legales mensuales vigentes, a menos que esta acción esté calificada como un delito con una pena más grave. (República de Colombia, 2023)

Por otro lado, la misma legislación colombiana sustenta por medio de su art. 269j, para los casos de transferencia de activos sin el consentimiento correspondiente, que, quien con la intención de

obtener ganancias económicas y haciendo uso de manipulaciones Informáticas o artificios similares, logre llevar a cabo el traspaso no autorizado de cualquier activo en menoscabo de una tercera persona, a menos que esta acción sea tipificada como un delito con una pena más severa, será sentenciado a un periodo de prisión que oscila entre 48 y 120 meses, además de enfrentar una multa que variará entre 200 y 1.500 salarios mínimos legales mensuales vigentes. La misma penalización se aplicará a aquellos individuos que creen, introduzcan, posean o faciliten programas de computadora diseñados con la finalidad de cometer el delito mencionado anteriormente, o con el propósito de llevar a cabo un acto de estafa. (República de Colombia, 2023)

Como lo hemos establecido anteriormente dentro de estas nuevas tecnologías existe una gran variedad de situaciones en donde el sistema ecuatoriano reflejado en el (COIP) CODIGO ORGANICO INTEGRAL PENAL, no está abarcando todo lo que las nuevas tecnologías están generando es por ello que se ha traído a colación estos artículos de otras legislaciones en donde se abarca temas que resultar ser de suma importancia y que lo que buscan es mejorar estos tipos de delitos.

***CONCLUSIÓN***

En el Ecuador, el marco legal actual, el COIP y al LOPDP, ha intentado abordar estos delitos, pero se enfrenta a desafíos debido a la rapidez con la que evolucionan las tecnologías y surgen nuevas formas de delincuencia informática. Es necesario que la legislación se actualice constantemente para abarcar todos los tipos de delitos cibernéticos y proporcionar sanciones adecuadas. La implementación de la LOPDP en Ecuador es un paso importante para de esta forma poder asegurar la posibilidad de ejercer el derecho a la privacidad y preservar la seguridad de la información personal.

Sin embargo, aún existen brechas legales y así también la necesidad de fortalecer la protección de las redes y sistemas informáticos. Es fundamental que las instituciones y organismos gubernamentales trabajen en conjunto para desarrollar estrategias y políticas de ciberseguridad eficaces, además, es esencial fomentar la educación y concienciación sobre las amenazas cibernéticas y promover buenas prácticas en el uso de la tecnología.

Por último, la colaboración entre el sector público, el sector privado y la sociedad en general es esencial para enfrentar los desafíos inherentes a la era digital y garantizar la protección de los derechos individuales en un mundo cada vez más interconectado. El Código Orgánico Integral Penal (COIP) debería considerar como imperativo establecer regulaciones y normativas actualizadas que aborden las amenazas cibernéticas y protejan la privacidad y a la seguridad de la información personal. La cooperación y la sensibilización desempeñan un rol fundamental en la preservación de un entorno digital seguro y en la salvaguardia de los derechos individuales en la era de la información.

***RECOMENDACIONES***

La rama de las nuevas tecnologías cada día están en aumento en la época que vivimos los avances en tecnología se ve como el futuro pero no porque sea un futuro estas deben estar sin control, es por ello que a través de este artículo se buscó dar una normativa que pueda contener en cierta parte este tipo de delitos y que en Ecuador, no se está viendo una reforma o una manera de que este tipo de sucesos no queden en la impunidad; como todos sabemos Ecuador es un estado democrático que debería de proteger la integridad de las personas y de su información, es por ello que debería de dar reformas con la finalidad de implantar nuevas normativas con respecto a las nuevas tecnologías y buscar reducir esta brecha digital existente de dentro de la legislación Ecuatoriana, la Informática (TIC) y el Código Orgánico Integral Penal.

***REFERENCIAS***

Accessnow. (11 de enero de 2023). Disrupciones de internet en Ecuador: cómo ocurrieron y cómo eludirlas. Obtenido de https://www.accessnow.org/disrupciones-de-internet-en- ecuador-como-ocurrieron-y-como-eludirlas/

Ana, C. (13 de diciembre de 2021). www.cnnespanol.com. Obtenido de https://cnnespanol.cnn.com/2021/12/13/eeuu-narcotrafico-ecuador-orix/

Argoti, M. (2022). La estrategia contra las amenazas híbridas. Revista de la Academia de Guerra del Ejército Ecuatoriano, 15(1), Obtenido de: https://dx.doi.org/10.24133/age.n15.2022.12,

Bello, E. (10 de noviembre de 2022). Siete ejemplos de empresas y marcas que ya han abrazado el metaverso. Obtenido de https://www.iebschool.com/blog/ejemplos- empresas-metaverso-tecnologia/

Benavides, M. &. (20 de eneros de 2023). Seguridad y crimen transnacional: La geopolítica del narcotráfico como amenaza a la seguridad del estado. Obtenido de: http://repositorio.puce.edu.ec/bitstream/handle/22000/20366/SEGURIDAD%20Y%20CRIMEN%20TRANSNACIONAL_%20LA%20GEOPOL%C3%8DTICA%20DEL%20NARCOTR%C3%81FICO%20COMO%20AMENAZA%20A%20LA%20SEGURIDAD.%20.pdf?sequence=1&isAllowed=y

Colombia, r. d. (2009). Ley 1273. Recuperado el 11 de mayo de 2015. Obtenido de Ley 1273. Recuperado el 11 de mayo de 2015: http://www.secretariasenado.gov.co/senado/basedoc/ley_1273_2009.html ECUADOR, G. D. (s.f.). Ecuador trabaja en medidas preventivas para evitar los “ciberdelitos”. Obtenido de https://www.telecomunicaciones.gob.ec/ecuador-trabaja-en-medidas-preventivas-para-evitar-los-ciberdelitos/

HUMANOS, M. D. (2022). ESTABLECE NORMAS SOBRE DELITOS INFORMÁTICOS, DEROGA LA LEY N° 19.223 Y MODIFICA OTROS CUERPOS LEGALES CON EL OBJETO DE ADECUARLOS

AL CONVENIO DE BUDAPEST. Chile: navegar norma.

Martínez, A. A. (2004). Derecho y nuevas tecnologías. Catalunya: UOC.

Mundial., B. (10 de enero de 2022). Personas que usan internet en el Ecuador. Obtenido de https://datos.bancomundial.org/indicator/IT.NET.USER.ZS?locations=EC&name_desc=true

Nacional, A. (26 de marzo de 2021). LEY ORGÁNICA DE PROTECCIÓN DE DATOS. Obtenido de https://www.finanzaspopulares.gob.ec/wp-content/uploads/2021/07/ley_organica_de_proteccion_de_datos_personales.pdf

Nacional, P. (14 de enero de 2023). Delitos informáticos o Ciberdelitos. Obtenido de https://www.policia.gob.ec/delitos-informaticos-o-ciberdelitos/

NAVARRO, S. A. (2013). FRAUDE ELECTRONICO PANORAMICA ACTUAL Y MEDIOS JURÍDICOS PARA COMBATIRLO. ESPAÑA: ARANZADI, SA.

Ortiz, A. I. (2002). El derecho a la intimidad en la Nueva Ley Orgánica de Protección de Datos Personales. Madrid: Librería-Editorial Dykinson.

Penal, C. O. (2021). Código Orgánico Integral Penal, COIP. Ecuador.

SALVADOR, L. A. (12 de enero de 2022). DECRETO No. 260.-. Obtenido de DECRETO No. 260. https://www.jurisprudencia.gob.sv/DocumentosBoveda/D/2/2010- 2019/2016/02/B6B74.PDF