UNIVERSIDAD INDOAMERICA

FACULTAD DE JURISPRUDENCIA, CIENCIAS POLITICAS Y ECONÓMICAS

CARRERA DE DERECHO

TEMA:

Ciberdelitos, y las dificultades que tiene la justicia para prevenir y sancionar estos actos delictivos.

Trabajo de titulación previo a la obtención del título de abogado/a de los tribunales y juzgados de la república del Ecuador.

AUTOR:

Alex Dario Zambrano Verdugo

Tutor(a): Abg. Victor Holguín. Mg.

QUITO-ECUADOR

2023

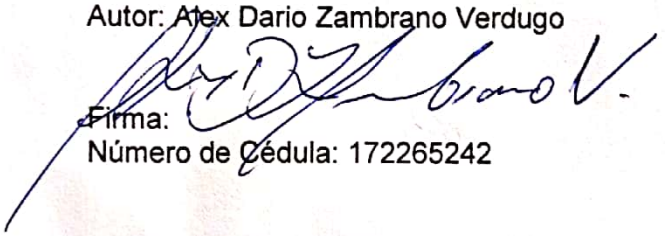
AUTORIZACIÓN POR PARTE DEL AUTOR PARA LA CONSULTA, REPRODUCCIÓN PARCIAL O TOTAL, Y PUBLICACIÓN ELECTRÓNICA DEL TRABAJO DE TITULACIÓN.

Yo, Alex Dario Zambrano Verdugo, declaro ser autor del Trabajo de Investigación con el nombre "Ciberdelitos, y las dificultades que tiene la justicia para prevenir y sancionar estos actos delictivos", como requisito para optar al grado de Abogado, autorizo al Sistema de Bibliotecas de la Universidad Tecnológica Indoamérica, para que con fines netamente académicos divulgue esta obra a través del Repositorio Digital Institucional (RDIUTI).

Los usuarios del RDI-UTI podrán consultar el contenido de este trabajo en las redes de información del país y del exterior, con las cuales la Universidad tenga convenios. La Universidad Tecnológica Indoamérica no se hace responsable por el plagio o copia del contenido parcial o total de este trabajo.

Para constancia de esta autorización, en la ciudad de Quito, a los 10 días del mes de A
Abril del 2023, firmo conforme:

Autor: Alex Dario Zambrano Verdugo



Firma:
Número de Cédula: 172265242

APROBACIÓN DEL TUTOR

En mi calidad de Tutor del Trabajo de Titulación **"CIBERDELITOS, Y LAS DIFICULTADES QUE TIENE LA JUSTICIA PARA PREVENIR Y SANCIONAR ESTOS ACTOS DELICTIVOS",** presentado por el autor ALEX DARIO ZAMBRANO VERDUGO para optar por el Titulo de Abogado

CERTIFICO

Que dicho trabajo ha sido revisado en todas sus partes y considero que reúne los requisitos y méritos suficientes para ser sometido a la presentación pública y evaluación por parte del Tribunal Examinador que se designe.

Quito, 6 de abril de 2023

Firmado electrónicamente por:
VICTOR HUGO HOLGUIN CARDENAS

Abg. Víctor Hugo Holguín Cárdenas

C.I. 1803807906

DECLARACIÓN DE AUTENTICIDAD

Quien suscribe, declaro que los contenidos y los resultados obtenidos en el presente trabajo de investigación, como requerimiento previo para la obtención del Título de Abogado, son absolutamente originales, auténticos y personales y de exclusiva responsabilidad legal y académica del autor.
Quito, 03 de Abril de 2023

CI: 172265242

UNIVERSIDAD TECNOLÓGICA INDOAMÉRICA
FACULTAD DE JURISPRUDENCIA, CIENCIAS POLÍTICAS Y ECONÓMICAS
CARRERA DE DERECHO

INFORME DE PAR LECTORES

FECHA: Quito, 10 de abril de 2023
CARRERA DE PREGRADO-ABOGADO MODALIDAD-SEMIPRESENCIAL

ESTUDIANTE:

Alex Dario Zambrano Verdugo

TEMA:

"Ciberdelitos, y las dificultades que tiene la justicia para prevenir y sancionar estos actos delictivos"

Una vez revisado el trabajo de titulación, y una vez que se han acogido las observaciones realizadas, encontramos que se enmarca dentro de los requerimientos establecidos en el reglamento respectivo, cumpliendo con los parámetros para la entrega de trabajos de titulación, razón por lo cual, se autoriza continuar con el trámite correspondiente para culminar el proceso de graduación

Ab. Germán Mosquera, MSc. **PAR LECTOR-**	**Ab. Jesús Portillo, Msc.** **PAR LECTOR**

DEDICATORIA

A mi madre y padre que durante toda su vida han creído en mí, que asumieron como proyecto mi educación, y que gracias a ese compromiso hoy me encuentro en este lugar, ejerciendo la defensa de conocimientos y monografía para ejercer mi profesión.

A mi amada esposa por impulsar lo mejor de mí, e inspirar el deseo de crecer y servir.

A mi familia y amigos por siempre estar y creer.

AGRADECIMIENTO

Agradezco a mis padres y familia por el mayor regalo que me han podido entregar, la educación como herramienta de progreso y superación.

Agradezco al Dr. Luigi Garcia Cano, que con sus enseñanzas, guía y confianza han despertado la pasión por esta hermosa profesión.

Agradezco también a toda la comunidad de la universidad Indoamérica que han inspirado mis conocimientos y decisión de ser un profesional del derecho, en especial al Dr. Victor Holguin y Dra. Estefanía Moreno, que con su ayuda me han guiado para la culminación de este proyecto.

TÍTULO: "Ciberdelitos, y las dificultades que tiene la justicia para prevenir y sancionar estos actos delictivos."

ÍNDICE GENERAL

LISTA DE TABLAS

RESUMEN

El presente proyecto investigativo, tiene el propósito de analizar los Ciber delitos, su tipificación en el Código Orgánico Integral Penal, los estudios doctrinarios, las modalidades, el perfil del ciber delincuente, y las dificultades que tienen los operadores de justicia para sancionar estos delitos. Podemos destacar que el Ecuador tiene avances en esta materia, sin embargo nos falta mucho camino por recorrer para poder prevenir, perseguir y sancionar estos actos, y estas dificultades no pasan únicamente por las deficiencias en la categorización de los delitos o la falta de capacitación técnica, sino que por la propia naturaleza de estos delitos, su detección y sanción es sumamente compleja, lo que incide directamente en que estos actos por lo general queden en la impunidad, especialmente porque su territorialidad no se encuentra definida, y más bien hablamos de actos transnacionales, sumado a la suplantación de identidades y alta complejidad técnica, lo que nos indica que hace falta ahondar mucho mas en esta materia a fin de prevenir activamente de forma conjunta con la sociedad.

Palabras claves:

Transnacional-Budapest-Informáticos-Prevención-Técnico

ABSTRACT

The purpose of this research project is to analyze Cybercrimes, their classification in the Comprehensive Organic Criminal Code, doctrinal studies, modalities, the profile of the cybercriminal, and the difficulties that justice operators have to sanction them. We can highlight that Ecuador has made progress in this matter, however we still have a long way to go to prevent, prosecute and punish these acts, and these difficulties do not only arise from deficiencies in the categorization of crimes or the lack of technical training, but due to the very nature of these crimes, their detection and punishment is extremely complex, which directly affects the fact that these acts generally remain unpunished, especially since their territoriality is not defined, and rather we speak of acts transnational, added to the theft of identities and high technical complexity, which indicates that it is necessary to go much deeper into this matter in order to actively prevent jointly with society.

Keywords:

Transnational-Budapest-IT-Prevention-Technician

INTRODUCCIÓN

En esta monografía, se fundamenta teóricamente los conceptos y categorías relativos a los ciberdelitos, ciberdelincuencia y las limitaciones existentes en el campo del Derecho Penal. Además, se presenta una comparación de la regulación de los ciberdelitos en la legislación penal de Ecuador con las de Colombia y Venezuela. También se identifican las características de las actividades ciberdelictivas y su tipificación en la legislación penal ecuatoriana vigente. Finalmente, se describe el perfil del delincuente informático, señalando sus características más importantes.

Entre los principales ciberdelitos están la suplantación de identidad, el acoso o la estafa. Con el empleo de las nuevas tecnologías, es posible ejecutar ataques cibernéticos en contra de gobiernos, negocios e individuos. En este sentido, ciertas palabras y frases que en años anteriores apenas eran conocidas, ahora son parte de la comunicación cotidiana. Estos delitos no conocen límites físicos ni virtuales, sino que ocasionan severos daños, e implican un peligro real para las víctimas a lo largo y ancho del mundo entero.

Las estrategias tradicionales de la delincuencia también evolucionaron. Las organizaciones delictivas emplean cada vez con mayor frecuencia las conexiones mediante Internet, facilitando así sus actividades e incrementando sus beneficios en el menor tiempo posible.

Estos delitos en realidad no son nuevos, considerando que se habla sobre el robo, fraude, juegos de azar ilícitos, venta de medicamentos falsificados, llegaron a una nueva dimensión, gracias a la comunicación en línea. La ciberdelincuencia, por tanto, crece a un ritmo acelerado. Así, entre 2017 y 2021, se tuvo un incremento del 29,11% de casos denunciados, según datos de la fiscalía general del Estado (FGE), como puede verse en la siguiente tabla:

Tabla 1. Estadística delitos cibernéticos denunciados a nivel nacional, período 2017-2021

ART. COIP	TIPO PENAL / ARTICULO	2017	2018	2019	2020	2021	TOTAL
103	Pornografía con utilización de niñas, niños o adolescentes	103	104	81	113	95	496
104	Comercialización de pornografía con utilización de niñas, niños o adolescentes	26	9	17	18	15	85

ART. COIP	TIPO PENAL / ARTICULO	2017	2018	2019	2020	2021	TOTAL
173	Contacto con finalidad sexual con menores de dieciocho años por medios electrónicos	158	202	165	152	152	829
174	Oferta de servicios sexuales con menores de dieciocho años por medios electrónicos	12	14	16	7	7	56
178	Violación a la intimidad	1660	2062	2038	1985	1346	9091
186	Estafa	13.911	14.268	16.918	18.415	16.272	79.784
188	Aprovechamiento ilícito de servicios públicos	102	130	194	99	72	597
190	Apropiación fraudulenta por medios electrónicos	959	1.448	1.744	2.280	3.962	10.393
192	Intercambio comercialización o compra de información de equipos terminales móviles	-	-	-	1	1	2
193	Remplazo de identificación de terminales móviles	4	2	-	3	-	9
194	Comercialización ilícita de terminales móviles	24	14	7	285	10	340
195	Infraestructura ilícita	-	5	7	-	-	12
229	Revelación ilegal de base de datos	22	44	34	30	23	153
230	Interceptación ilegal de datos	63	41	86	73	35	298
231	Transferencia electrónica de activo patrimonial	54	37	50	76	170	387
232	Ataque a la integridad de sistemas informáticos	85	86	111	95	86	463
233	Delitos contra la información pública reservada legalmente	14	12	5	5	4	40
234	Acceso no consentido a un sistema informático, telemático o de telecomunicaciones	218	236	242	295	274	1.265

ART. COIP	TIPO PENAL / ARTICULO	2017	2018	2019	2020	2021	TOTAL
366	Terrorismo	12	120	65	13	17	227
Total, general por años		17.480	18.914	21.834	23.968	22.569	104.765

Nota: (Fiscalía General del Estado, 2021, pág. 59).

Las instituciones relacionadas con esta problemática, deben actualizarse sobre las nuevas tecnologías, comprendiendo las posibilidades que crean para los delincuentes y su empleo como herramientas para luchar contra la ciberdelincuencia. Por tal motivo, es importante considerar la información sobre el tema, y tener consciencia de esta amenaza permanente (Fiscalía General del Estado, 2021).

Además, se toma en cuenta que la tipificación vigente de estos delitos, establecida en el Código Orgánico Integral Penal del Ecuador (COIP) es insuficiente, por cuanto no existe una adecuada coordinación y articulación de las acciones entre las instituciones vinculadas con esta problemática, siendo necesaria la creación de una Fiscalía especializada, además de los manuales, acuerdos, guías que reglamenten esta cooperación entre carteras de Estado, además de una constante actualización y preparación a Fiscales y Jueces, que debe ser coordinada entre la FGE y la Escuela de Función Judicial perteneciente al Consejo de la Judicatura (Cuenca, 2022).

Por ello, es necesario entender la naturaleza jurídica de estos ilícitos, así como la identificación de las falencias en las estructuras contenidas en la norma penal ecuatoriana, sobre todo en lo relacionado con las acciones típicas descritas en estos delitos. Además, se deben precisar apropiadamente los riesgos a los que se hallan expuestos los diferentes activos digitales de las instituciones y de particulares, profundizando así la comprensión de los bienes jurídicamente protegidos. Por tanto, de forma específica, se identifican los siguientes tipos penales en el COIP ecuatoriano:

> **Art. 229**, Revelación ilegal de Base de Datos, de 1 a 3 años y de 3 a 5 años cuando es en contra de servidores públicos.
>
> **Art. 230**, Interceptación ilegal de datos, de 3 a 5 años
>
> **Art. 231**, Transferencia electrónica de activo patrimonial, de 3 a 5 años
>
> **Art. 232**, Ataque a la Integridad de Sistemas Informáticos, de 3 a 5 años y cuando se comete a bienes informáticos destinados al servicio público públicos 5 a 7 años.

Art. 233, Delitos contra la información pública reservada bajo amparo de la ley, de 5 a 7 años y cuando esa información es sustraída por un servidor público la pena es de 3 a 5 años.

Art. 234, Acceso no consentido a un sistema informático, telemático o de telecomunicaciones, de 3 a 5 años.

En este sentido, para el interés de la presente investigación, se plantean las nociones básicas sobre ambos ejes temáticos, el Derecho Penal Informático en Ecuador, y las actividades ciber delictivas, con el interés fijo tanto en los conceptos principales como en la explicación teórica de ambos. En esta sección, se presentan la justificación, el problema y los objetivos, con los que se tiene una mejor visualización del tema de estudio.

1.1. Problema y finalidad del trabajo

Con base en los argumentos anteriores, se formula el problema de investigación en los siguientes términos:

¿Cuáles son las dificultades que tiene la justicia para prevenir y sancionar los ciberdelitos en el contexto ecuatoriano?

1.2. Objetivos

1.2.1. Objetivo general

Identificar las dificultades que tiene la justicia para prevenir y sancionar los ciberdelitos en el contexto ecuatoriano.

1.2.2. Objetivos específicos

- Fundamentar teóricamente el estudio, tomando en cuenta los conceptos y categorías relativos a los ciberdelitos, ciberdelincuencia y las limitaciones existentes en el campo del Derecho Penal.

- Comparar la regulación de los ciberdelitos en la legislación penal de Ecuador con las de Colombia y Venezuela.

- Identificar las características de las actividades ciberdelictivas y su tipificación en la legislación penal ecuatoriana vigente, contenidos en los Arts. 173, 174, 178, 190-195, 229-234 del COIP.

- Describir el perfil del delincuente informático, señalando sus características más importantes.

1.3. Justificación del tema elegido

Con esta monografía, se busca ampliar los conocimientos e identificar las debilidades del sistema relacionadas con las actividades ciber delictivas, cuya dinámica estadística refleja la falta de una acción efectiva de las instituciones públicas, como se menciona en el apartado correspondiente al problema. Además, se considera el crecimiento constante y diario del número de usuarios de las redes sociales y la telefonía móvil, fenómeno que cambió la comunicación humana, que entre 2022 y 2023 se incrementó en 1,9%. Esto, en valores absolutos, implica un crecimiento de 98 millones de personas, teniéndose, hasta enero de 2023, 5.160 millones de usuarios de internet y celulares. Esto representa el 64,4% de la población mundial (Galeano, 2023).

En la dimensión práctica, se busca entender las nuevas formas de comunicación y los factores que condicionan la aparición de acciones dirigidas a la comisión de los delitos informáticos en general, y cibernéticos en particular. Esto supone una comprensión más clara sobre el papel de la tecnología digital en la actualidad, su influencia en los individuos y la vulnerabilidad de estos frente a ataques que puedan sufrir sus sistemas y dispositivos. Así, se tendrá una visión clara sobre la problemática en el contexto actual.

En cuanto a la metodología, se aplicarán las herramientas existentes para la recolección de la información requerida por este estudio, como la observación documental o revisión bibliográfica, que posibilita la selección apropiada de la información relacionada. Además, se aplicó la legislación comparada, que permite ver las similitudes y diferencias de la legislación penal ecuatoriana con las de Colombia y Venezuela. Estos países fueron elegidos por su proximidad geográfica y cultural con Ecuador. De estas legislaciones, nos centraremos en la legislación colombiana, tomando en cuenta que dicho estado suscribió el Convenio de Budapest.

2. MARCO TEÓRICO

En este apartado, se presentan los hallazgos teóricos relacionados con el objeto de estudio, presentando los principales conceptos y categorías que permiten la comprensión clara de la temática elegida. Entre otros, se exponen las características de los ataques informáticos, los tipos más conocidos, así como las medidas de seguridad existentes para enfrentar tales amenazas, entre otros importantes aspectos, con especial énfasis en las limitaciones de la legislación penal vigente en el Ecuador.

2.1. Antecedentes

Para el desarrollo de este estudio, se revisaron distintas investigaciones, como la de Rodas y Loor (2018). Estos autores analizan el proceso de formación en tipificación en el Código Orgánico Integral Penal para los delitos cibernéticos. Además, definen los delitos informáticos como "toda actividad ilícita que tiene por esencia robo de información, contraseñas, fraude a cuentas bancarias, entre otros" (p. 4). Este concepto es orientador para desarrollar el presente estudio.

Por otra parte, se consultó el estudio de Mayer (2018), quien considera que los delitos informáticos presentan características distintas a otros, identificando la mayor dificultad en la recolección de evidencias. Además, recalca que la informática se caracteriza por una elevada preparación por parte del perpetrador, por cuanto tiene una marcada y complejidad técnica. Esto se refleja en el uso de términos y códigos particulares, tratándose de un campo semántico especializado en su área. Finalmente, afirma que se busca entender los rasgos esenciales de la persona que delinque oculto detrás de una pantalla, adecuando su propósito a un recurso tecnológico.

Frecuentemente, este tipo de delitos, tiene un carácter transfronterizo, y exige una respuesta instantánea. Por ello, es necesario establecer medidas de seguridad y normas para lograrlo, aunque el delito de fraude informático no se halla tipificado en algunas normas penales. A pesar de ello, se pudo establecer que el delito informático de mayor recurrencia es el espionaje y sabotaje informático, que se da mediante el robo de identidad, buscando acceder a fondos bancarios, la utilización de programas propios de hackers, a fin de incrustar malwares en los procesadores e infectar cualquier archivo, documentación o sistema informático de seguridad (Arellano, 2022).

Como se adelantó, con la técnica de derecho comparado se pretende ver las similitudes y diferencias de la legislación penal vigente en Ecuador, habiéndose elegido los casos de países de la misma región. Entonces, se puede apreciar, sobre todo en el caso de la legislación colombiana, que, al haber suscrito dicho Estado el Convenio de Budapest,

cuenta con una legislación penal más firme y efectiva en su lucha contra este tipo de delitos.

La ciberdelincuencia incluye aquellos delitos cometidos contra la seguridad de las computadoras y sistemas de información, buscando acceder de forma no autorizada a un dispositivo, o bloquear el acceso del usuario legítimo. Es decir, un cibercriminal es un individuo que identifica las vulnerabilidades de las redes y sistemas de información, buscando realizar actos tipificados en la normativa penal vigente: robo o destrucción de información, extorsión, divulgación de información confidencial, distribución de pornografía infantil, etc.

Asimismo, aprovechando la red de equipos conectados, sea de forma pública o privada, o por medio de un sistema informático, busque vulnerar todo lo relacionado con la confidencialidad, así como la integridad y también la disponibilidad de los sistemas informáticos, además del empleo de los sistemas, redes y datos de forma fraudulenta.

2.2. Delitos y ataques informáticos

Los ataques informáticos son los mecanismos empleados por algunas personas naturales para ocasionar daño a los sistemas informáticos de particulares, empresas o entidades gubernamentales. A continuación, se describen los principales tipos penales y ataques informáticos, con base en la normativa legal vigente en Ecuador.

Tabla 2. Principales tipos penales y ataques informáticos

ART. COIP	TIPO PENAL	DESCRIPCIÓN
103	Pornografía con utilización de niñas, niños o adolescentes	Involucramiento de menores de edad en fotografías, videos y otros productos comunicacionales y difundidos por medios digitales.
104	Comercialización de pornografía con utilización de niñas, niños o adolescentes	El mismo tipo descrito en el anterior artículo, pero que busca obtener un rédito económico para el o los autores, que difunden tales contenidos.
173	Contacto con finalidad sexual con menores de dieciocho años por medios electrónicos	Conjunto de acciones encaminadas a mantener contacto con personas menores de 18 años, con fines claramente sexuales, independientemente de que se lo haga, además, con el propósito de comercializar luego las imágenes y videos, de forma posterior.
174	Oferta de servicios sexuales con menores de dieciocho años por medios electrónicos	Este tipo de delito tiene que ver con la tradicional figura de proxeneta, consistente en contactar a adultos para que mantengan relaciones sexuales con

ART. COIP	TIPO PENAL	DESCRIPCIÓN
		niños, niñas o adolescentes, utilizando para ello los medios electrónicos.
178	Violación a la intimidad	Se trata de un tipo penal amplio, que incluye la intrusión en la comunicación digital de la víctima, por medio de distintas estrategias, como el phishing, y que buscan dañar de cualquier forma al propietario legítimo de la cuenta.
186	Estafa	Se trata del tipo de robo o delito contra la propiedad o el patrimonio, que a veces se asimila al fraude, el timo y el engaño (dolo), cometido con medios electrónicos.
188	Aprovechamiento ilícito de servicios públicos	Este tipo implica la alteración de los sistemas de control o aparatos contadores para aprovecharse de los servicios públicos de energía eléctrica, derivados de hidrocarburos, gas natural, gas licuado de petróleo, en beneficio propio o de terceros, empleando para ello los medios electrónicos.
190	Apropiación fraudulenta por medios electrónicos	Consiste en la alteración, manipulación o modificación el funcionamiento de redes electrónicas, programas, sistemas informáticos, telemáticos y equipos terminales de telecomunicaciones, con el propósito de facilitar la apropiación de un bien ajeno o que procure la transferencia no consentida de bienes, valores o derechos en perjuicio de esta o de una tercera, en beneficio suyo o de otra persona.
192	Intercambio comercialización o compra de información de equipos terminales móviles	Compra o venta de bases de datos que contengan información de equipos terminales móviles.
193	Remplazo de identificación de terminales móviles	Cambio intencional de las etiquetas o cualquier otro sistema de identificación de equipos móviles.
194	Comercialización ilícita de terminales móviles	Alude a la compra y venta por canales no oficiales o legalmente autorizados de terminales móviles.
195	Infraestructura ilícita	Se incluye a los equipos y tecnologías no autorizados para modificar o alterar la configuración o identidad de los terminales móviles.

Fuente: Código Orgánico Integral Penal, en sus respectivos artículos.

En la anterior tabla, se describen de forma resumida aquellas conductas que se constituyen en delitos informáticos, tomando en cuenta el fin que persiguen y la forma

en que se realizan. Por tanto, las formas más comunes de propagación de un malware son los correos electrónicos, las alertas emergentes o las descargas ocultas, tanto en equipos de computación como en teléfonos inteligentes, tabletas y otros dispositivos similares. Es decir, en todos los casos, se emplea un dispositivo de acceso a las redes, tanto internas como externas, constituyéndose así en los instrumentos empleados para cometer los ilícitos.

2.3. Convenio de Budapest

El Convenio No. 185, también conocido como Convenio de Budapest, o Convenio sobre la ciberdelincuencia, suscrito el 23 de noviembre de 2001. En el contexto latinoamericano, se tienen dos casos bastante próximos al Ecuador: Colombia y Perú, que, además, son también miembros de la Comunidad Andina de Naciones, al igual que Ecuador y Bolivia. En este caso, se considera necesario señalar a Colombia, en el apartado correspondiente a legislación comparada.

El caso de Perú, también debe ser considerado, por cuanto dicho estado tuvo un interesante desarrollo de normativa para encarar los desafíos que suponen las nuevas relaciones creadas a partir de las tecnologías de las TICs. Entre los años 80 e inicios de los 90, se expidieron muchas normas de organización interna para regular el uso de las computadoras y otros dispositivos electrónicos, que comenzaban a jugar un papel importante en la modernización del Estado. Asimismo, en 1991 se publicó el Decreto Legislativo N° 681, “Uso de Tecnologías Avanzadas en Materia de Archivo”, una norma pionera en la región que otorgaba validez legal a los archivos reproducidos por medios informáticos. En un claro signo del cambio de los tiempos, esta ley declaraba expresamente su intención de fomentar la inversión privada a partir del uso de la tecnología. En lo que respecta a Internet, la primera conexión estable se realizó también en 1991 gracias a la Red Científica Peruana (RCP) y en los siguientes años el acceso se expandió debido principalmente a un elemento adaptativo exitosamente aplicado: las cabinas públicas de Internet (Borgioli, y otros, 2018).

En cuanto a Colombia, el gobierno del vecino país, había avanzado desde el año 2009 con la expedición de la Ley 1273, donde se incorporaba en el Código Penal un nuevo bien jurídico tutelado denominado “de la protección de la información y de los datos”, por lo que se puede decir que el país ya se traía tarea adelantada por lo menos en relación con el capítulo del convenio que protege el CID de contera los datos personales (Cote, 2020).

2.3.1. Clasificación de los delitos informáticos

Este instrumento jurídico internacional clasifica a los delitos informáticos según el siguiente esquema (Suárez, 2016):

- Delitos contra la confidencialidad, la integridad y la disponibilidad de los datos y los sistemas informáticos;
- Delitos informáticos;
- Delitos relacionados con el contenido (como, por ejemplo, delitos relacionados con la pornografía infantil); y
- Delitos relacionados con infracciones a la propiedad intelectual.

El Convenio, por otra parte, señala la necesidad de sancionar estas conductas, así como las figuras de tentativa y complicidad. Además, establece que las sanciones deben ser efectivas, proporcionadas y disuasorias, y deben incluir las penas privativas de libertad (Suárez, 2016).

2.3.2. Protocolo Adicional

Este instrumento incluye un protocolo adicional, estableciendo la penalización de 58 actos de tipo racista y xenófobo, cometidos con el empleo de sistemas informáticos (Cires, 2022). Con él, se busca establecer mecanismos jurídicos efectivos en la lucha contra estos problemas, cometidos con los sistemas informáticos.

2.4. Delitos informáticos

2.4.1. Conceptualización

Para proseguir con la línea argumentativa de la presente investigación, sobre la base de las nociones de ataques informáticos, se procede a conceptualizar el delito informático, tomando en cuenta que esta figura abarca una gran cantidad de comportamientos que permiten construir un concepto más general.

Se debe visualizar al delito informático con la misma gravedad como cuando se enfrenta a un delincuente en la calle sosteniendo un arma blanca, con la diferencia que el delincuente ahora realiza sus acciones con la computadora como instrumento. Es necesario, entonces, entender que este tipo de comportamiento es punible y de difícil detección; aunque los primeros pasos para su cometimiento se realicen en el mundo físico y los otros se dan en el ciberespacio siendo su principal característica.

Los delitos informáticos deben ser sancionados con la normativa del mundo físico, puesto que sus consecuencias de forma efectiva se materializan en un medio o entorno físico y produce consecuencias en el mismo.

Las siguientes definiciones, aportadas por distintos autores, permiten clarificar la temática abordada:

> "Delincuencia informática es todo acto o conducta ilícita e ilegal que pueda ser tomada en cuenta como criminal, dirigida a alterar o socavar, destruir o manipular cualquier sistema informático o alguna de sus partes componentes que tenga como finalidad ocasionar una lesión o poner en peligro un bien jurídico cualquiera" (Acurio, 2016).

Es decir, es un conjunto de acciones dirigidas y ejecutadas por personas para dañar de cualquier forma un dispositivo informático, un sistema, o una red de los mismos. Existen diversos tipos de daños, como lo señala la cita anterior, y es actos con la intención de dañar u obtener algún beneficio como resultado de los mismos. Por ello, es importante considerar la clasificación de los mismos, de forma que el Derecho Penal tenga una acción eficaz frente a los mismos.

> "…. Son aquellas actividades ilícitas que se cometen por medio del empleo de computadoras, sistemas informáticos u otros dispositivos de comunicación (la informática es el medio o instrumento para realizar el delito) o tienen por objeto ocasionar daños, provocar pérdidas o impedir el empleo de sistemas informáticos…". (Sánchez, 2015, pág. 2).

Esta otra cita, nos recuerda que, como todo delito, los informáticos requieren instrumentos para su ejecución. Mientras en el asesinato el instrumento puede ser un cuchillo, un arma de fuego, o veneno, en el caso de los delitos informáticos, es cualquier computadora u otro dispositivo que pueda ser manipulado para acceder a otro y cometer el delito. Este equipo, como se señaló, requiere que el operador tenga ciertos conocimientos y un objetivo claro de dañar a otro, u obtener cualquier tipo de beneficio.

> "Los delitos informáticos son infracciones de oportunidad especial, es decir, el delincuente informático, espera la oportunidad en la que las posibilidades de impunidad sean las mayores posibles; como en todos los delitos de cuello blanco, por lo general es delincuentes primarios, no lo que no implica que sea la primera vez que no logra evadir la acción de la justicia" (Hurtado, 2018).

En esta cita, en cambio, se resalta el hecho de contar con una oportunidad que tenga el delincuente. Es decir, es cualquier circunstancia que posibilite al delincuente acceder a un dispositivo, sea cercano o remoto, y manipularlo, gracias a sus conocimientos, destrezas y habilidades, para ocasionar el daño pretendido.

En base a estos conceptos mencionados de forma anterior, se concluye que las conductas realizadas por el sujeto activo en esta clase de delito abarcan diferentes tipos de atentados en contra de diferentes bienes jurídicos protegidos según el caso. Por ejemplo, en primera instancia al patrimonio, también esta conducta puede afectar a la intimidad personal, y; otro bien jurídico al que puede afectar de forma directa es la seguridad nacional.

Son entonces actos dirigidos contra la confidencialidad, integridad y disponibilidad de los sistemas informáticos, redes o datos, así como el abuso de esos sistemas. A ello, se debe agregar una característica esencial de los delitos informáticos, tomando en cuenta que los mismos son una forma conductual de crimen transnacional, es decir que puede ser cometido en cualquier parte del mundo y afectar a una persona a un grupo de personas o países diferentes y lejanos del lugar del cometimiento físico del mismo.

Por tanto, se puede afirmar que “Los delitos informáticos son las conductas típicas, antijurídicas y culpables en que se tienen a las computadoras y redes como instrumentos para lograr los fines deseados y que afectan a una persona o grupo de personas determinados” (Acurio, 2016)

En el caso ecuatoriano, la Ley No. 67/2002 regula el Comercio Electrónico, Firmas y Mensajes de datos. En dicha norma, dentro del Capítulo I del Título V, titulado "DE LAS INFRACCIONES INFORMÁTICAS". El art. 57 de la referida norma establece que "se deberán tomar como infracciones informáticas, las de carácter administrativo y las que se tipifican, mediante reformas al Código Penal, en la presente ley" (Congreso Nacional, 2002). Así, se incorporan diferentes figuras de delitos informáticos.

Entre las reformas que se realizaron al Código Penal de entonces, se positivaron los siguientes comportamientos, en el primer artículo innumerado después del Art. 202:

> “… el que, empleando cualquier medio electrónico, informático o afín, violentare claves o sistemas de seguridad, para acceder u obtener información protegida, contenida en sistemas de información; para vulnerar el secreto, confidencialidad y reserva, o solo vulnerar la seguridad, será reprimido con prisión de seis meses a un año y multa de quinientos a mil dólares de los Estados Unidos de Norteamérica. Si la información obtenida se refiere a seguridad nacional, o a secretos comerciales o industriales, la pena será de uno a tres años de prisión y

> multa de mil a mil quinientos dólares de los Estados Unidos de Norteamérica. La divulgación o la utilización fraudulenta de la información protegida, así como de los secretos comerciales o industriales, será sancionada con pena de reclusión menor ordinaria de tres a seis años y multa de dos mil a diez mil dólares de los Estados Unidos de Norteamérica. Si la divulgación o la utilización fraudulenta se realiza por parte de la persona o personas encargadas de la custodia o utilización legítima de la información, éstas serán sancionadas con pena de reclusión menor de seis a nueve años y multa de dos mil a diez mil dólares de los Estados Unidos de Norteamérica…" (Congreso de la República, 2010).

En un artículo posterior, se tipifica otro comportamiento nocivo en las redes la obtención y utilización no autorizada de información, estableciendo sus características, y la sanción respectiva. Este tipo también contempla conductas como el acceso ilícito y violación de la intimidad.

Después describe el atentado contra la integridad de datos, en los siguientes términos:

> "… Serán reprimidos con tres a seis años de reclusión menor, todo empleado público y toda persona encargada de un servicio público, que hubiere actuado de forma maliciosa y fraudulenta, destruyendo o suprimiendo documentos, títulos, programas, datos, bases de datos, información o cualquier mensaje de datos contenido en un sistema de información o red electrónica, de que fueren depositarios, en su calidad de tales, o que les hubieren sido encomendados en razón de su cargo." (Congreso de la República, 2010).

También está el fraude o estafa informática cuando dice: "… Son reos de falsificación electrónica la persona o personas que con ánimo de lucro o bien para ocasionar un perjuicio a un tercero, empleando cualquier medio, alteren o modifiquen mensajes de datos, o la información incluida en éstos, que se encuentre contenida en cualquier soporte material, sistema de información o telemático" (Congreso de la República, 2010)..

Luego el atentado contra la integridad de sistemas, describiendo así esta conducta: "… el que, de forma dolosa, de cualquier modo, o empleando cualquier método, destruya, altere, inutilice, suprima o dañe, de forma temporal o definitiva, los programas, datos, bases de datos, información o cualquier mensaje de datos contenido en un sistema de información o red electrónica …" (Congreso de la República, 2010)..

Por último, describe el acceso ilícito, identificando a quienes emplearen de forma fraudulenta sistemas de información o redes electrónicas, para facilitar la apropiación de un bien ajeno, o los que procuren la transferencia no consentida de bienes, valores o derechos de una persona, en perjuicio de ésta o de un tercero, en beneficio suyo o de otra persona alterando, manipulando o modificando el funcionamiento de redes

electrónicas, programas informáticos, sistemas informáticos, telemáticos o mensajes de datos (Congreso de la República, 2010)..

Una vez que el Código Penal fue derogado, el COIP establece los delitos informáticos tipificados en el mismo. La prevención, por tanto, debe tomarse en cuenta como la primera acción a tomar en contra de los delitos informáticos. En relación con la prevención, tipificación y sanción, el “Convenio sobre la ciberdelincuencia” o Convenio de Budapest, ya señalado anteriormente, permite contar con un catálogo de delitos informáticos, que el Estado ecuatoriano podría adaptar para mejorar la regulación de estas conductas punibles.

2.4.2. Caracterización básica

La ciberdelincuencia puede ser definida como el fenómeno delictivo de rápida propagación, bajo el cual se incluyen los diversos delitos susceptibles de ser cometidos, empleando un dispositivo (computadora, celular o Tablet) conectado a una red informática (Ortiz, 2013). Por tanto, se da el uso del ciberespacio como ámbito en el que se cometen varias actividades ilícitas, o como medio de ataque a los archivos o programas de los sistemas informáticos (Ortiz, 2013).

2.4.3. Especificación de los delitos informáticos en la legislación ecuatoriana en el COIP.

En primer lugar, se describen los delitos informáticos tipificados en el COIP de Ecuador. En este sentido, el Art. 173, establece la descripción del tipo penal correspondiente al Contacto con finalidad sexual con menores de 18 años por medios electrónicos. La corrupción de menores por parte de un adulto, encontró en la comunicación vía internet una fuente propicia para desarrollarse. Los pedófilos aprovechan el anonimato y la invisibilidad para contactar a sus potenciales víctimas. Este artículo determina las características del acto como tal, a la vez que describe cómo se daría tal situación. El límite de edad es fundamental, tomando en cuenta que los 18 años marcan la mayoría de edad de una persona, y, por tanto, define la capacidad de decidir de una persona sobre sus actos y sobre su cuerpo.

Por otra parte, se tiene el Art. 174, que establece la oferta de servicios sexuales con menores de 18 años por medios electrónicos. Este tipo penal intenta controlar la conocida prostitución en las redes que en la actualidad se dan con mayor frecuencia. Así, se pretende consolidar la protección de los derechos de los niños y adolescentes en de la normativa penal ecuatoriana.

Asimismo, se tiene el Art. 178, que establece el delito de violación a la intimidad. En este artículo, además, se identifica los “datos personales”, mencionando que los mismos pueden estar en mensajes de datos, voz, audio y video, objetos postales, información contenida en soportes informáticos, comunicaciones privadas o reservadas de otra persona por cualquier medio. Las implicaciones de la violación a la intimidad de las personas en el ciber espacio van desde las comunicaciones personales, información sensible, contenido íntimo, y más, el cual puede ser obtenido por personas de nuestro entorno o del ciber espacio, provocando daños no solo a la intimidad, sino que puede vulnerar la integridad sexual, datos privados de salud o secretos profesionales, por lo que no debe ser tomado a la ligera ya que sus daños se producen en varios bienes jurídicos.

Por otra parte, en relación con la apropiación fraudulenta por medios electrónicos, el Art. 190 hace referencia a la estafa, que se basa en el engaño y el aprovechamiento de la ingenuidad de las personas para apropiarse de sus bienes, por lo general el dinero, aunque también es posible que se beneficien de otros activos.

En cuanto a la reprogramación o modificación de equipos terminales móviles, este delito se halla tipificado en el Art. 191 del COIP. Este tipo penal fue una novedad en esta codificación. Esto se debe al desarrollo que experimenta el derecho de acuerdo a los comportamientos nuevos que tenga la población. Si bien la penalización de esta conducta no será suficiente para disminuir este delito, es importante su tipificación, como una forma de visibilizar la problemática, medida que podría complementarse con campañas de concienciación respecto a la compra de dispositivos celulares de segunda mano, casi siempre sin contar los comprobantes o respaldos respectivos. Es de amplio conocimiento que el robo de celulares, “equipos terminales” se generalizó en las diferentes sociedades, tomando en cuenta que resulta un equipo indispensable en la interacción social, laboral, comercial y personal. Entonces, el legislador observó necesario incluir este tipo de conducta.

Asimismo, el Art. 192 establece la sanción con pena privativa de libertad de uno a tres años, para la persona que intercambie, comercialice o compre bases de datos que contengan información de identificación de equipos terminales móviles. Según se observa en este artículo, el intercambio, la comercialización o compra de información de equipos terminales móviles es una conducta pasible a una sanción privativa de libertad, al ser una práctica prohibida de forma expresa por la ley. Este artículo hace referencia y ampara a los datos personales.

Por otra parte, el Art. 193 establece la pena privativa de libertad de uno a tres años para la persona que reemplace las etiquetas de fabricación de los terminales móviles que contienen información de identificación de dichos equipos y coloque en su lugar otras etiquetas con información de identificación falsa o diferente a la original. El reemplazo de identificación de terminales móviles que contienen identificación, este es con el fin de que no se comercialicen otra vez los equipos terminales robados, y penaliza este comportamiento de forma exclusiva.

En cuanto a la Revelación ilegal de bases de datos, el Art. 229 penaliza en particular la conducta de revelar en provecho propio o de un tercero la información privada registrada en: ficheros, archivos, bases de datos, a través o dirigidas a un sistema informático, electrónico, telemático o de telecomunicaciones.

Además, sobre la interceptación ilegal de comunicaciones, el Art. 230 establece la pena privativa de libertad de tres a cinco años, tipificando como delito el hecho de interceptar, escuchar, desviar, grabar y observar datos informáticos con la intención de obtener información privada o personal disponible.

En cuanto a la transferencia electrónica de activo patrimonial, el Art. 231 resguarda los activos de la empresa o compañía, salvaguardando los bienes económicos de la víctima.

En relación con el ataque a la integridad de sistemas informáticos, el Art. 233 tipifica esta conducta como delito, considerando que abarca aún más comportamientos que tienen que son complementarios para la comisión del objetivo del mismo. Sobre los delitos contra la información pública reservada bajo protección legal, el Código Orgánico General Integral Penal menciona también los delitos más peligrosos que se pueden cometer desde las redes y su sanción de libertad, esto puesto que un ataque contra la información calificada, de conformidad con la ley, como clasificada o reservada, podría resultar en estafas masivas o ataques económicos.

En cuanto al acceso no consentido a un sistema informático, telemático o de telecomunicaciones, el Art. 234 describe a quién sin consentimiento y/o autorización acceda de forma ilegal en todo o en parte a un sistema informático y más adelante describe el objeto de la acción, mencionado para explotar de manera ilegítima el acceso logrado.

Siendo el universo de posibilidades para cometer este tipo de acciones entre la red, también esta disposición describe otras posibilidades diciendo: “… modificar un portal web, desviar o re direccionar el tráfico de datos o voz u ofrece servicios que estos

sistemas proveen a terceros, sin pagarles a los proveedores de servicios legítimos…". Estos comportamientos también tienen ánimo doloso tomando en cuenta que implica un daño a quien de forma efectiva provee el servicio de telecomunicaciones.

2.4.4. Legislación comparada

En la siguiente tabla, se presenta la comparación de las legislaciones penales de Colombia y Venezuela, con la ecuatoriana.

País / Conducta penalizada	Ecuador	Colombia	Venezuela
Norma legal que tipifica los delitos informáticos	Código Orgánico Integral Penal, Arts. 173, 174, 178, 190-195, 229-234.	Código Penal, Arts. 192-197	Ley especial contra los delitos informáticos, Arts. 6-26
Conductas tipificadas	Contacto con finalidad sexual con menores de dieciocho años por medios electrónicos, Oferta de servicios sexuales con menores de dieciocho años por medios electrónicos, Violación a la intimidad, Revelación ilegal de base de datos, interceptación ilegal de datos, transferencia electrónica de activo patrimonial, ataque a la Integridad de sistemas informáticos, delitos contra la información pública, acceso no consentido a un sistema informático, telemático o de telecomunicaciones	Acceso abusivo a un sistema informático, obstaculización ilegítima del sistema informático o red de telecomunicaciones, intercepción de datos informáticos, daño informático, uso de software malicioso, hurto por medios informáticos, violación de datos personales, suplantación de sitios web para capturar datos personales y trasferencia no consentida de activos	Acceso indebido, sabotaje o daño a sistemas, favorecimiento culposo del sabotaje o daño, acceso indebido o sabotaje a sistemas protegidos, Posesión de equipos o prestación de servicios de sabotaje, espionaje infromatico, falsificación de documentos, hurto, fraude, obtención indebida de bienes o servicios, manejo fraudulento de tarjetas inteligentes o instrumentos análogos, apropiación de tarjetas inteligentes o instrumentos análogos, entre otros.
El Estado suscribió el Convenio de Budapest	NO	SÍ	NO

Elaboración propia, 2023.

Esta tabla permite ver de forma resumida los alcances y contenidos de las diferentes normas legales que tiene cada país. A continuación, se describen los hallazgos más relevantes en cada caso.

2.4.4.1. Colombia

La Constitución Política de Colombia de 1991, establece en el artículo 15 que: "Todas las personas tienen derecho a su intimidad personal y familiar y a su buen nombre, y el Estado debe respetarlos y hacerlos respetar. De igual modo, tienen derecho a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en bancos de

datos y en archivos de entidades públicas y privadas” (Asamblea Nacional Constituyente, 1991).

En consecuencia, y para lograr darle operatividad al derecho garantizado en el artículo descrito anteriormente de la Constitución Política de Colombia, en el año 2009 se expide la Ley de Delitos Informáticos (1.273), que completa y permite que el Código Penal colombiano incorpore el bien jurídico: “protección de la información y de los datos”.

Esta legislación también obligó al gobierno colombiano a diversificar sus relaciones internacionales en lo relacionado a la protección de recursos informáticos, y modifique sus leyes a fin de integrarse al Convenio. Colombia decide entonces comenzar el proceso de adhesión al Convenio de Budapest sobre Ciberdelincuencia. Además, se debe mencionar que el estado colombiano cuenta con el COLCERT, equipo nacional de respuestas a incidentes de seguridad digital, dependiente de la Policía Nacional, y que coordina las diferentes tareas y actividades nacionales de seguridad informática (https://www.colcert.gov.co/).

La implementación y adecuación de la legislación colombiana, facultaron al Consejo de Europa a invitar al estado colombiano a adherirse al Convenio de Budapest en 2013, disponiendo de 5 años para encaminar su adhesión al Convenio. Así, el congreso colombiano aprobó el convenio de Budapest en 2018, mediante Ley No 1.928, finalizando su adhesión el 16 de marzo del 2020.

La Ley 1273 del 2009 modifica el Código Penal, creando un nuevo bien jurídico tutelado, denominado “De la protección de la información y de los datos…”. Con esta incorporación, se agrega el Capítulo I, titulado "De los atentados contra todo lo relacionado con la confidencialidad, así como la integridad y también la disponibilidad de los datos y de los sistemas informáticos…".

Por otra parte, se tiene la Ley 1273 que, anexada al Código Penal Colombiano, regula las sanciones que recibirán los autores de delitos contra la confidencialidad, la integridad, la disponibilidad de los datos y los sistemas informáticos. De forma puntual, se tiene los artículos agregados 269, desde el A hasta el J, que establecen:

> Art. 269 A) Acceso abusivo a un sistema informático. El acceso abusivo se produce cuando un agente externo, que puede ser cercano o no a la organización se introduce en su sistema informático, con el fin de extraer, sacar, copiar, dañar o borrar, información de la empresa u organización y al hacerlo sacar provecho de ese acto. Para realizar este tipo de conducta en la gran mayoría de los casos son los mismos “colaboradores” o trabajadores de la organización o empresa quienes realizan este tipo de conducta tomando en

cuenta que suele ser información específica y que solo atañe o importa a ese tipo de línea de negocio.

Art. 269 B) Obstaculización ilegítima de sistema informático o red de telecomunicaciones, a cerca de este tema y con el objeto de explicarlo está lo siguiente: "…esta conducta consiste en impedir u obstaculizar el acceso normal a un sistema informático o a los datos informáticos contenidos en el mismo, puede llevarse a cabo por medio de la instalación de un software malicioso, que contenga virus o spiware, a fin de atacar los controles informáticos y producir la propagación de código maliciosos. En este caso aquella conducta también se concreta, la destrucción, daño, borrado o alteración, de los datos informáticos o del sistema de tratamiento de la información…" (Suárez, 2016, pág. 278).

Art. 269 C) Intercepción de datos informáticos.

En lo que respecta a este comportamiento también el mismo autor al referirse a ello dice:

"… La conducta del delito de interceptación de datos informáticos se tipifica cuando la misma se da respecto de dichos datos en su origen, destino o en el interior de un sistema informático, o las emisiones electromagnéticas. Como este delito tiene como objeto material los datos, se puede realizar mediante interceptación de los mismos…" (Suárez, 2016, pág. 317)

De lo transcrito, se puede inferir que es una conducta con la cual el fin último es el impedir o interceptar cierta información que resulte relevante o importante para la propia organización, otra vez esta conducta se notará o se expondrá con agente internos de las organizaciones tomando en cuenta que siendo particulares los intereses son en absoluto peculiares.

Art. 269 D) Daño informático, para hablar sobre este tipo de comportamiento, se debe acotar que en el confluyen otros comportamientos anteriores con el fin de hacer efectivo el daño que se quiera ocasionar.

Este comportamiento como otros en la red están ligados y se debe hacer el uno para lograr la comisión del otro. Así para realizar "daño informático", primero es necesario acceder al sistema. Entonces, surge el primer cuestionamiento: ¿el mero ingreso no autorizado a un sistema no es por sí mismo ya un daño informático? La respuesta lógica es que sí, tomando en cuenta que el acceso no consentido a un sistema informático mismo constituye por sí solo una conducta punible, tomando en cuenta que obedece a intereses propios del giro o la línea del negocio, y un ingreso no autorizado equivale a una intrusión.

Art. 269 E) Empleo de software malicioso. Esta conducta se hace efectiva una vez que un tercero desde el interior de la organización (insider) o por medios remotos instala un programa con el objeto de ocasionar un daño inminente o a futuro, este comportamiento puede tener variables como son acceso abusivo o daño informático.

En muchas conductas delictivas informáticas esta unas ligadas o supeditadas a otras es decir que para conseguir el fin último se deber realizar varias conductas delictivas, hay concurso de delitos.

> Art. 269 F) Violación de datos personales, la conducta que describe la violación de datos personales hacen referencia a la conducta de modificar, transformar o alterar los datos que ya tiene una persona u organización.

En este caso, se debe anotar que los datos personales tienen una característica especial puesto que individualizan y singularizan a una persona en específico.

> Art. 269 G) Suplantación de sitio web para capturar datos personales, es también conocido como phishing, este tipo conducta intenta por medio de la estafa, obtener los datos personales de un tercero con fines ilícitos.

Es entonces por medio de una estafa robar información confidencial de forma fraudulenta, la información buscada, consiste en obtener coordenadas o claves bancarias, números de tarjeras de crédito, contraseñas y datos personales por medio de correos electrónicos, mensajes de texto, llamadas telefónicas; realizando cualquiera de estas acciones, que además parecen reales, solicitando claves o pidiendo otra vez información sensible.

En la actualidad esta forma de estafa se ha diversificado, y se produce entre las redes sociales más grandes y conocidas como lo son Facebook o Instagram, en donde te envían invitaciones para que te bajes e instales aplicaciones de dudosa procedencia con el fin de realizar copia o respaldo de toda la información personal.

> Art. 269 I) Hurto por medios informáticos, este delito hacer referencia al apoderamiento de la cosa mueble ajena, por medio de la manipulación del sistema informático por medio de la superación de medidas de seguridad informática, aquí también se produce la modalidad de hurto por medio de la suplantación del usuario.

Este delito está ligado muy de cerca con el de “violación de datos personales”, tomando en cuenta que son conductas que describes estos tipos penales.

> Art. 269 J) Transferencia no consentida de datos, al respecto el código penal colombiano prevé en el artículo 269J la figura típica de “transferencia no consentida de activos y tenencia de software destinado al fraude”.

Este tipo penal además de la seguridad de la información informatizada, protege el patrimonio económico.

En cuanto a Ecuador, el país no forma parte del Convenio de Budapest y el gobierno no ha realizado acciones en ese sentido.

2.4.4.2. Venezuela

El bien jurídico protegido en la República Bolivariana de Venezuela, en relación con los delitos informáticos, es la protección de los sistemas informáticos, los mismos que incluyen, tratan, protegen y transfieren la respectiva información. Están tomados en cuenta en la Ley Especial contra los Delitos Informáticos desde el año 2001. Esta norma legal tipifica cinco tipos de delitos:

- Contra los sistemas que emplean tecnologías de información.
- Contra la propiedad.
- Contra la privacidad de las personas y de las comunicaciones.
- Contra los niños y adolescentes.
- Contra el orden económico.

De esta comparación, se puede destacar el esfuerzo que el legislativo ha realizado al ver reflejada la realidad acorde a los avances del sistema informático plasmada en la sociedad actual, respecto a la conducta dentro del ciberespacio y en vista a la complejidad de este delito por sus características tan "atípicas" donde es vulnerable toda la información incluyendo la reservada y confidencial, la que tiempo atrás era inaccesible e inalcanzable, logrando por medio de la norma responder a la realidad contemporánea.

A esto, se suma la coyuntura actual, con la pandemia del Covid 19, observándose que varias actividades productivas se realizan en el ciberespacio. También se pudo observar cómo la transformación digital se produce de forma vertiginosa en vista de la inminencia que tiene la sociedad de poder producir, por medio del acceso a la información e innovarse en áreas como el teletrabajo, educación online, y un sinnúmero de servicios que se ofertan, que aportan de manera sustentable, fomentando el desarrollo y avance de la sociedad desde otro enfoque, en pro de la transformación.

Se hace imperioso entonces el conocer acerca de la realidad que nos atañe en la actualidad y que echa mano del recurso digital para que la sociedad siga funcionando con relativa normalidad.

2.4.5.- Conclusiones del estudio comparativo

- Podemos concluir que el desarrollo en materia de ciber delitos es bastante similar, y en general protege los mismos bienes jurídicos como propiedad, privacidad o intimidad, niños o adolescentes, orden económico, y sistemas

informáticos, es decir se tiene una tipicidad común en contra estos actos delictivos.

- Podemos resaltar que ambos países tienen un mayor desarrollo en esta materia, debido a que existen mayor numero de conductas tipificadas de forma bastante especifica lo que ayuda a los operadores de justicia a poder hacer cumplir con la ley y que se cierre la brecha con la impunidad que es característica de estos tipos penales.

- El desarrollo integral de las leyes respecto de estas conductas penales permite que la cooperación internacional tan necesaria para perseguir estos actos, sea mucho más eficiente, que con países que desde las legislaturas no se desarrolla las definiciones y diferenciación de las conductas, por lo que los ciber delincuentes encuentran mayor facilidad para cumplir sus objetivos, en la mayoría de casos transnacionales.

2.5. Perfil del delincuente informático

En este apartado, se presentan los principales rasgos del delincuente informático, tomando en cuenta las características personales del mismo, de forma particular sus conocimientos y empleo que hacen de los diferentes dispositivos electrónicos, con acceso a la comunicación en la red. Con base en estas consideraciones, el perfil del delincuente informático va desde el de un joven obsesionado por el medio informático e Internet, muy hábil y consciente de su potencial, o es un empleado descontento con su empresa. Todo, además, sin fines lucrativos inmediatos, tomando en cuenta que, en determinadas oportunidades, estos actos pueden ser los más cuantiosos hablando en términos económicos, por lo que demuestran una gran paciencia, hasta lograr su propósito. Por lo general, los sujetos activos, son varones cuya edad oscila entre 15 y 40 años, con habilidad para el manejo de los sistemas informáticos. Además, por su situación laboral, sobre todo, se desempeñan en instituciones y sectores estratégicos donde se maneja información sensible (Maza, 2021).

La siguiente tabla, ilustra las características principales del perfil del delincuente informático.

Tabla 3. Perfil del delincuente informático

Psico-ciberdelincuente		**Normo-ciberdelincuente**	
Ciber-psicópata	**Integrado** Ciberdelincuente exitoso **No integrado** Ciberdelincuente realizor	Ciber-oportunista	Ciberdelincuente ventajista
Ciber-neurótico	Ciberdelincuente manipulable	Ciber-frecuente	Ciberdelincuente pandillero Ciberdelincuente rebelde
Ciber-psicótico	Ciberdelincuente enajenado Ciberdelincuente salvador	Ciber-habitual	Ciberdelincuente neo profesional Ciberdelincuente profesional Ciberdelincuente a sueldo
Ciber-sociópata	Ciberdelincuente inadaptado		

Fuente: (Fanjul, 2018)

No es frecuente el empleo de estupefacientes o de bebidas alcohólicas entre los *hackers*, decantándose, en la mayor parte de los casos, por el consumo de las denominadas drogas “blandas” (cannabis). La excepción la constituyen los menos cualificados entre los *hackers*, quienes abusan de estas sustancias, tomando en cuenta que la falta de claridad mental les impide realizar un ataque sin cometer errores y evita que alcancen los niveles más altos de sus capacidades técnicas (Cámara, 2020).

3. NECESIDAD DE ACTUALIZAR LA NORMATIVA PENAL ECUATORIANA SOBRE DELITOS INFORMÁTICOS

La ciberdelincuencia campea en el Ecuador, y esto es en gran medida por la falta de acción efectiva por parte del estado ecuatoriano, las acciones se han limitado únicamente a tipificar ciertos tipos de actos delictivos, dejando de lado el estableciendo de políticas públicas tendientes a educar, informar, prevenir, invertir, y sobre todo perseguir al ciber delincuente.

El primer paso urgente que debe tomar el estado ecuatoriano es la suscripción de los tratados internacionales necesarios que nos permitan vincularnos con la comunidad internacional a fin de perseguir estos delitos que no miran fronteras, solo objetivos.

El segundo paso es vincular el sector privado y público, a fin de establecer estrategias conjuntas para el tratamiento de los datos de usuarios clientes y ciudadanos y la política que nos permita educar y prevenir desde sector que es el más vulnerable.

El tercer paso es invertir tanto el sector público como privado en la protección de los datos, ya que estos sectores manejan información sensible, como información bancaria, datos personales, registros públicos, etc.

En este punto podemos recordar los últimos ataques informáticos, realizados en contra del Registro de la Propiedad de Quito y la Corporación Nacional de Telecomunicaciones (CNT), así como el Banco de Pichincha.

Es decir, se necesita una acción conjunta para que las políticas tengan los resultados deseados.

Y, por último, se necesita de forma urgente que se eduque e informe a los servidores públicos; sean estos principalmente agentes investigadores, fiscales, jueces y funcionarios que están relacionados con el tratamiento de datos. También a los empleados privados y empresarios que por el giro de negocio tienen relación con sistemas informáticos y tratamientos de datos personales o comerciales. Y por último la ciudadanía en general. Todas estas acciones van a influir directamente en la prevención de estos delitos ya que una población preparada e informada es menos vulnerable, ya que muchos de los delitos que se cometen se hubieran podido prevenir simplemente con un ciudadano informado.

4. CONCLUSIONES

El desarrollo del presente estudio, permitió formular las siguientes conclusiones:

- Se fundamentó teóricamente el estudio, considerando los conceptos y categorías relativos a los ciberdelitos, ciberdelincuencia, perfil del delincuente informático, así como las limitaciones existentes en el campo del Derecho Penal. Por ello podemos concluir que existen múltiples amenazas a los sistemas informáticos tanto públicos como privados, al ser una técnica sumamente especializada su detección es compleja y la impunidad de estos actos es casi una garantía, a esto podemos sumar la falta de información respecto de estos delitos que dificulta la toma de acciones preventivas y acciones emergentes ante un ataque, esta falencia dificulta el accionar judicial, posicionando a la ciudadanía como una potencial víctima, y sin la garantía de que se sancione al victimario.

- Se identificaron los desafíos globales resultantes del ciberdelito, lo que representa uno mayor para las legislaciones latinoamericanas, como el caso ecuatoriano, teniéndose diversas dificultades para los gobiernos y las instituciones involucradas en esta problemática, como la Fiscalía y la Policía Nacional para enfrentar al ciberdelito. Pese a existir una normativa que regule el cibercrimen, no es suficiente en la mitigación de este tipo de delitos. Es necesario, para mejorar los niveles en ciberseguridad, desarrollar políticas públicas enfocadas en la especialización de unidades de investigación de delitos informáticos, en programas de educación y cultura digital dirigidos a toda la ciudadanía, en capacitación de operadores de justicia y una serie de estrategias que se van actualizando al corto y al largo plazo dentro de sus planes de ciberseguridad.

- Se presentó una comparación de la regulación de los ciberdelitos en la legislación penal de Ecuador con las de Colombia y Venezuela. En general, si bien Ecuador cuenta con un esquema actualizado que permite la penalización de las conductas típicas en relación con la era digital, también adolece de ciertas falencias, como la no suscripción del Convenio de Budapest, que provee un importante catálogo de conductas punibles y articulación internacional, que serían un gran avance en la materia dentro de la legislación nacional. Así mismo podemos destacar el gran avance que tiene la legislación colombiana, tanto en

prevención, profesionalización del sistema judicial, y en la subscripción de convenios internacionales para perseguir los ciberdelitos.

- También se identificaron las características de las actividades ciber delictivas y su tipificación en la legislación penal ecuatoriana vigente, contenidos en los Arts. 173, 174, 178, 190-195, 229-234 del COIP. Además, se presentaron las nociones básicas de los ataques informáticos más comunes, que permiten llevar adelante la lucha contra este flagelo del siglo actual, y podemos categorizar los bienes jurídicos protegidos, como Propiedad, Intimidad, Integridad Sexual, y Delitos contra la seguridad de los activos de los sistemas de información y comunicación.

- Por último, se describió el perfil del delincuente informático, señalando sus características más importantes, así como las variantes del mismo, ya que no existe un solo perfil del referido delincuente. Esta perfilación es importante para identificar a los sujetos que afectan los sistemas informáticos de particulares, así como de instituciones públicas y privadas, comprometiendo y afectando la información y seguridad informática de las mismas. Podemos concluir que existen perfiles motivados por la curiosidad, descontento o por incentivos económicos, y generalmente se encuentran en posiciones empresariales o publicas donde manejan información sensible esto debido a su alta cualificación profesional en esta área. Además, que sus relaciones interpersonales son deficientes por un alto desarraigo y desestructuras familiares, induciendo a estas personas a refugiarse en el ciberespacio.

5. Bibliografía

Acurio, S. (2016). *Delitos Informáticos: Generalidades.* Quito: PUCE. Recuperado el 13 de Junio de 2021, de https://www.oas.org/juridico/spanish/cyb_ecu_delitos_inform.pdf

Arellano, G. (2022). *Deficiencias Legislativas en el Tratamiento de la Ley N° 30096, Ley de Delitos Informáticos – Fraude Informático, Lima 2019 – 2021.* Lima: Universidad César Vallejo. Recuperado el 16 de Enero de 2023, de https://repositorio.ucv.edu.pe/handle/20.500.12692/102672

Asamblea Nacional Constituyente. (1991). *Constitución Política de Colombia*. Recuperado el 30 de Octubre de 2022, de Corte Constitucional: https://www.ramajudicial.gov.co/documents/10228/1547471/CONSTITUCION-Interiores.pdf

Borgioli, M., Guerrero, C., Frati, S., Hernández, L., Morales, D., Castañeda, J. D., . . . Samaniego, M. (2018). *Perú: análisis sobre el proceso de implementación del convenio de ciberdelincuencia. Impacto en el corto, mediano y largo plazo.* Lima: Derechos digitales. Recuperado el 1 de Abril de 2023, de https://www.derechosdigitales.org/wp-content/uploads/minuta_hiperderecho.pdf

Cámara, S. (2020). Estudios criminológicos contemporáneos (IX): La Cibercriminología y el perfil del ciberdelincuente. *Derecho y Cambio Social*, 470-512.

Cires, C. (2022). *La Falta de tipificación penal sobre los delitos informáticos en el Ecuador.* Guayaquil: Universidad Tecnológica ECOTEC. Recuperado el 25 de Octubre de 2022, de https://repositorio.ecotec.edu.ec/bitstream/123456789/425/1/CIRES%2c%20CRISTOPHER.pdf

Congreso de la República. (2010). *Código Penal*. Recuperado el 26 de Enero de 2023, de https://www.secretariadelamazonia.gob.ec/wp-content/uploads/downloads/2014/05/CODIGO-PENAL-act.pdf

Congreso Nacional. (2002). Ley de comercio electrónico, firmas electrónicas y mensajes de datos . *Ley No. 2002-67. Registro Oficial 557-S, 17-IV-2002*. Quito: Registro Oficial. Recuperado el 19 de Julio de 2021, de https://www.gob.ec/sites/default/files/regulations/2018-10/Documento_Ley-Comercio-Electr%C3%B3nico-Firmas-Mensajes-Datos.pdf

Cote, L. (22 de Enero de 2020). *Colombia y el convenio de Budapest contra el cibercrimen*. Recuperado el 1 de Abril de 2023, de https://www.redipd.org/es/tribuna/colombia-y-el-convenio-de-budapest-contra-el-cibercrimen

Cuenca, H. (2022). *Articulación de la Fiscalía General del Estado para la persecución de delitos cibernéticos.* Quito: Instituto de Altos Estudios Nacionales. Recuperado el 24 de Enero de 2023, de https://repositorio.iaen.edu.ec/bitstream/handle/24000/6045/TRABAJO%20DE%20TITULACI%c3%93N%20HUGO%20CUENCA%20ESPINOSA.pdf?sequence=1&isAllowed=y

Fanjul, M. (2018). *Conceptualización, evolución y clasificación del ciberdelito empresarial. Definición del ciberdelincuente. Implicaciones estratégicas.* Madrid: AMEC Ediciones.

Fiscalía General del Estado. (2021). Perfil criminológico. *Revista Científica de Ciencias Jurídicas, Criminología y Seguridad*, 1-62. Recuperado el 5 de Enero de 2023, de Quito https://www.fiscalia.gob.ec/pdf/politica-criminal/Ciberdelitos-Perfil-Criminologico.pdf

Fundación Telefónica. (18 de Octubre de 2022). *Ciberseguridad: 4 tipos de ataques informáticos*. Recuperado el 6 de Febrero de 2023, de https://www.fundaciontelefonica.com/noticias/ciberseguridad-4-tipos-de-ataques-informaticos/

Galeano, S. (26 de Enero de 2023). *El número de usuarios de internet en el mundo crece un 1,9% y alcanza los 5.160 millones (2023)*. Recuperado el 26 de Enero de 2023, de Marketing 4 e-commerce: https://marketing4ecommerce.net/usuarios-de-internet-mundo/

Hurtado, L. (2018). *Manual de Derecho Informático.* Guayaquil: Biblioteca Jurídica.

Mayer, L. (2018). Elementos criminológicos para el análisis jurídico - penal de los delitos informáticos. *Ius et Praxis, 24*, 159-206. doi:http://dx.doi.org/10.4067/S0718-00122018000100159

Maza, P. (14 de Enero de 2021). *El perfil del delincuente informático*. Obtenido de Pablo Maza Abogado: https://pablomazaabogado.es/penal-tecnologico/el-perfil-del-delincuente-informatico/#%C2%BFComo_es_el_delincuente_informatico

Ortiz, J. (2013). *Problemas procesales de la Ciberdelincuencia.* Madrid: Cólex.

Rodas, P., & Loor, E. (2018). Proceso de formación en tipificación en el código orgánico integral penal para los delitos cibernéticos. *Revista Iberoamericana de educación*. doi:https://doi.org/10.31876/ie.v1i1.4

Sánchez, L. (2015). *Ética y Legislación Informática.* Recuperado el 3 de Julio de 2021, de www.aniei.org.mx/paginas/uam/CursoEtica/Delincuencia_Informatica.pdf

Suárez, A. (2016). *Manual de delito informático en Colombia.* Bogotá: Universidad El Externado de Colombia.