



Universidad Tecnológica ECOTEC

Derecho y Gobernabilidad

Título del trabajo:

“Análisis del delito informático de suplantación de identidad, relacionado a los derechos constitucionales del Ecuador, período 2020-2021.”

Línea de Investigación:

Gestión de las Relaciones Jurídicas

Modalidad de titulación:

Trabajo de Investigación

Carrera:

Derecho con énfasis en Derechos Humanos y Ciencias Penales

Título a obtener:

Abogado

Autor (a):

Carlos Sergio Gómez Olvera

Tutor (a):

Ab. Mercedes Coronel Gómez, Mgtr.

Samborondón - Ecuador

2022



ANEXO N° 14

**CERTIFICADO DE APROBACIÓN DEL TUTOR PARA LA PRESENTACIÓN A
REVISIÓN DEL TRABAJO DE TITULACIÓN**

Samborondón, 9 de agosto de 2022

Magíster
Mgtr. Mario Cuví Santacruz
Decano de la Facultad
Derecho y Gobernabilidad
Universidad Tecnológica ECOTEC

De mis consideraciones:

Por medio de la presente comunico a usted que el trabajo de titulación TITULADO: "Análisis del delito informático de suplantación de identidad, relacionado a los derechos constitucionales del Ecuador, período 2020-2021.", según su modalidad Proyecto de Investigación, fue revisado, siendo su contenido original en su totalidad, así como el cumplimiento de los requerimientos establecidos en la guía para la elaboración del trabajo de titulación, Por lo que se autoriza a: Carlos Sergio Gomez Olivera , para que proceda a su presentación para la revisión de los miembros del tribunal de sustentación.

ATENTAMENTE,


MERCEDES
CECILIA CORONEL
GOMEZ

Firmado digitalmente
por MERCEDES CECILIA
CORONEL GOMEZ
Fecha: 2022.08.09
18:05:49 -05'00'

Mgtr. MERCEDES CECILIA CORONEL GÓMEZ

Tutora

CERTIFICADO DEL PORCENTAJE DE COINCIDENCIAS

Habiendo sido nombrado Ab. Mercedes Coronel Gómez, Mgtr, tutor del trabajo de titulación "Análisis del delito informático de suplantación de identidad, relacionado a los derechos constitucionales del Ecuador, período 2020-2021."

elaborado por Carlos Sergio Gomez Olivera , con mi respectiva supervisión como requerimiento parcial para la obtención del título de Abogado.

Se informa que el mismo ha resultado tener un porcentaje de coincidencias _ (%)__ mismo que se puede verificar en el siguiente link:

<https://secure.urkund.com/oid/view/130207587-321738-602075#Hoo7DsJQDETRvaQeIf3ebGoriAJFgFKQJIV70wojtyP7md6H8NyV'yHKSSlopqSjhrf+k/01cmKITJQU34IZLGADNsMSxpXhAle4wwQeRlI3QhEDkRIF0ZqFIUIFGm1o3rpbOrbXvi239b0vi2mRiSRUh41M6Urx+y4A>

Adicional se adjunta print de pantalla de dicho resultado.



Documento: [Tesis Final Carlos Gomez.docx](#) (D0427866)

Presentado: 2022-08-09 17:53 (-05:00)

Presentado por: mercoronel@ecotec.edu.ec

Recibido: mercoronel.ecotec@analisis.urkund.com

9% de estas 28 páginas, se componen de texto presente en 13 fuentes.

 Firmado digitalmente por
MERCEDES CECILIA
CORONEL GOMEZ
Fecha: 2022.08.09 18:04:41
-05'00'

FIRMA DEL TUTOR
Ab. Mercedes Coronel Gómez, Mgtr.

DEDICATORIA

A mis padres, Sr. Carlos Sergio Gómez Jaime y Sra. Carmen Aracely Olvera Avilés, porque son las personas más importantes de mi vida, al formarme en la persona que soy actualmente y ser pilares fundamentales en mi formación como profesional en el área de Derecho, gracias por apoyarme siempre en mi diario vivir, sin ustedes no hubiera logrado este título.

A mis hermanos, Andrés Gómez y Nery Gómez, por estar en cada momento importante de mi vida personal y estudiantil, gracias a ustedes por brindarme su ayuda cuando lo he necesitado dentro de este tiempo como estudiante de Derecho.

AGRADECIMIENTOS

Agradecimiento especial a la Universidad Tecnológica Ecotec y al personal docente de la Institución por ser de excelente guía dentro de mi período académico, y formarme como profesional con bases y herramientas metodológicas aplicables dentro de la Carrera de Derecho.

A los compañeros y amigos que logré conocer dentro de este período de estudios universitarios, por lo que llegaron a ser de gran ayuda para mi formación como profesional dentro de la Carrera de Derecho.

Resumen

El presente proyecto jurídico tiene como título: “Análisis del delito informático de suplantación de identidad, relacionado a los derechos constitucionales del Ecuador, período 2020-2021.”, de lo cual el objetivo general fue analizar los delitos informáticos de suplantación de identidad relacionado a los derechos constitucionales del Ecuador 2020-2021, ya que en la actualidad no existe en el Código Orgánico Integral Penal el delito informático de suplantación. La pregunta problemática que se empleó es la siguiente: ¿Cuáles son las alternativas legales que establece el marco normativo ecuatoriano para proteger la identidad de las personas en los medios digitales?.

En cuanto al capítulo de metodología se pudo implementar una investigación jurídica con un enfoque cualitativo y descriptivo, además se utilizó el método de entrevistas a expertos para lo cual se entrevistaron a los abogados: Ricardo Xavier Vanegas Cortázar, David Vergara Solís y Adela Alcívar. Para finalmente llegar a la conclusión de que es necesario realizar una reforma al Código Orgánico Integral Penal e insertar el delito informático de suplantación de identidad.

Palabras claves: suplantación de identidad, usurpación, delito, prevención e informática.

Asbtract

This legal project is entitled: "Analysis of the computer crime of identity theft, related to the constitutional rights of Ecuador, period 2020-2021.", of which the general objective was to analyze the computer crimes of identity theft related to the constitutional rights of Ecuador 2020-2021, since currently the computer crime of impersonation does not exist in the Comprehensive Criminal Organic Code. The problematic question that was used is the following: What are the legal alternatives established by the Ecuadorian regulatory framework to protect the identity of people in digital media?

Regarding the methodology chapter, it was possible to implement a legal investigation with a qualitative and descriptive approach, in addition, the method of interviewing experts was used, for which the lawyers were interviewed: Ricardo Xavier Vanegas Cortázar, David Vergara Solís and Adela Alcívar. To finally reach the conclusion that it is necessary to carry out a reform to the Comprehensive Criminal Organic Code and insert the computer crime of identity theft.

Keywords: identity theft, usurpation, crime, prevention and information technology.

Tabla de contenido

Introducción	1
Antecedentes	3
Contexto histórico	5
Planteamiento del problema científico	8
Objetivos	9
Objetivo general	9
Objetivos específicos	9
Justificación	9
Novedad científica	9
CAPÍTULO I: MARCO TEÓRICO	11
1.1. Teoría del delito	12
1.1.1. Concepto de infracción penal	13
1.1.2. Acción	14
1.1.3. Tipicidad	15
1.1.4. Antijuridicidad	16
1.1.5. Culpabilidad	17
1.2. Delitos informáticos	18
1.2.1. Conceptos	18
1.2.2. Tipos de delitos informáticos	19
1.3. Delito de suplantación de identidad	21
1.3.1. Definiciones	21
1.3.2. Características	22
1.3.3. Consecuencias	23
1.3.4. Tipo objetivo	24
1.3.5. Bien jurídico protegido	24
1.3.6. Sujeto activo	25
1.3.7. Sujeto pasivo	26
1.3.8. Verbo rector	26
1.3.9. Tipo subjetivo	26
1.4. Diferencia entre Suplantación y Usurpación de identidad	27
1.5. Delitos informáticos según el COIP	30
1.6. Delitos de suplantación de identidad según el COIP	34
1.7. Derecho comparado	36

1.7.1.	Argentina	36
1.7.2.	Colombia	37
1.7.3.	España	38
Capítulo II: Marco Metodológico		40
2.1.	Enfoque de la investigación	41
2.2.	Tipo de investigación	41
2.3.	Métodos de investigación	41
	Método documental	41
	Método comparado	42
	Método empírico	42
2.4.	Universo y muestra	42
Capítulo III: Análisis de resultados		43
3.1.	Entrevistas a expertos	44
3.2.	Análisis global de entrevistas	49
Capítulo IV: Propuesta		51
4.1.	Justificación de la propuesta	52
Conclusiones		53
Recomendaciones		55
BIBLIOGRAFÍA		56
Anexos		59

Índice de anexos

Anexo 1 Formato de entrevista a expertos

59

Introducción

La red de comunicación ha evolucionado constantemente, lo que ha permitido crear nuevas formas para comunicarse, como es el internet, que permite crear un intercambio de información constante, rápida y efectiva. Sin embargo, es necesario asegurar el correcto desenvolvimiento de la evolución tecnológica.

Internet es tan evolucionario que abrió paso a nuevas formas de delincuencia organizada que pone en riesgo la información privada, la seguridad en la navegación y de las instituciones públicas y privadas. La información ha obtenido un valor económico. El desarrollo tecnológico informático dio origen a la criminalidad informática o de los delitos informáticos que se vive en la realidad social actual. (Altamirano, 2017)

El abuso informático o la delincuencia informática es un conjunto de comportamientos de reproche penal que tienen por instrumento los sistemas o elementos de técnica informática. El delito informático es la realización de una acción que reúne ciertas características que delimitan el concepto de delito. Se materializa como un elemento informático que vulnera los derechos del titular de un elemento informático, sea hardware o software.

La emergente sociedad de la información es necesaria la incorporación de valores inmateriales y de la información como bienes jurídicos de protección. Es una protección necesaria al bien jurídico para evitar la penalización del principio de lesividad, en contra del valor intrínseco de la información, y los sistemas que procesan o automatizan la misma.

Las nuevas tecnologías y la falta de información para la protección a la misma, genera el conflicto a la delincuencia informática. Dado que, la faltan de protección facilita el trabajo de los ciber delincuentes. La suplantación de identidad es el fenómeno que consiste en hacerse pasar por otra persona para obtener un beneficio al que no se tiene derecho.

La suplantación de identidad es un problema que se escucha más seguido por el crecimiento del internet, redes sociales todo lo que engloba la era tecnológica esto deja una gran oportunidad para que ciber delincuentes puedan usurpar la identidad de otras personas. La importancia de la presente investigación es que la ciudadanía ecuatoriana conozca acerca de los diferentes delitos como es el caso de la suplantación de identidad Para así generar conocimiento de este tema. (Alvarez, 2015)

La suplantación de identidad en Internet es un delito según el uso que se realice. Por ejemplo, una persona se hace pasar por otra con el fin de obtener beneficios, por generar un fraude u ocasionar un daño. Las circunstancias concurren de forma independiente por el uso de la falsa identidad. El usurpador atenta contra el estado civil de la víctima al sustituir su verdadera identidad, ante las visualizaciones de otros usuarios en la red.

La suplantación de identidad vulnera la facultad de un tercero para relacionarse con otro, la seguridad de las relaciones jurídicas que se proyecta del estado civil vulnerado. Es una expresión informática que se emplea para referirse a los abusos informáticos cometidos por delincuentes para estafar, obtener información personal y contraseñas de forma ilegal.

Esta suplantación de identidad es muy perjudicial para las víctimas ya que las personas malintencionadas al usar el nombre de otro estafan y hacen fraudes perjudicando la reputación y metiendo en problemas legales a las víctimas y se busca conocer si incrementó o disminuyó la suplantación de identidad en el Ecuador en los años 2017-2020 (Barrera, 2017).

Por qué debemos analizar la situación que se presentó y se sigue presentado de una manera pertinente para el momento tan delicado del país podemos investigar actos delictivos que pasaron. El derecho ha mantenido una colección de principios, preceptos y reglas que se someten a la convivencia de justicia y paz.

Las ciencias jurídicas mantienen una evolución tecnológica, que establece derechos y obligaciones dentro de una sociedad tangible que actúa ante los usuarios dentro de la internet.

Antecedentes

Las nuevas tecnologías que intermedian en la comunicación entre las personas que trae implícito el aprovechamiento indebido e ilícito de la información. Los delitos informáticos van a la par del desarrollo de las tecnologías de la información.

La sociedad por la falta de información y la falta del control de normativa para poder erradicar los actos delictivos. La sociedad ha tenido avance y desarrollo de todas sus áreas; y uno de los beneficios es que el uso de redes de comunicaciones les permite a los delincuentes cometer delitos (Carrillo, 2016)

Los sistemas informáticos establecieron un desarrollo social que se enfoca en el delito informático que se enfoca en el daño, perjuicio, frente a un delito informático. La criminalidad informática crece de manera exponencial por la falta de seguridad que permite a los ciber infractores abusar de la vulnerabilidad de la información.

El derecho y la tecnología contribuyeron a la sociedad y crearon una nueva ciencia jurídica como es el derecho informático. A su vez, se crearon inseguridades con los delitos informáticos que implican fraudes, perjuicios, estafas, uso indebido de las computadoras; por ello, trajo consigo regulaciones y controles.

Uno de los principales ataques en la historia de Internet se remonta al primer virus informático que afectó a una computadora que mostró un mensaje en los equipos infectados, el cual fue la base para el desarrollo de ataques de pérdidas millonarias en el sitio web de la Interpol (Davara, 2001).

Los delitos informáticos dentro de la sociedad son irreparables, ya que la investigación no es eficaz al momento de efectuarla, para llevar a

cabo el juzgamiento correcto, de acuerdo al derecho. La suplantación de identidad se asocia al uso público de un nombre y apellidos de un tercero ficticio, que puede existir o ser imaginario. Por ejemplo: aquella persona que abre una cuenta en una red social creando un perfil falso con la finalidad de enmascarar su identidad y con la intención de hacerse pasar por otro.

La presencia de nuevas formas delictivas informáticas y electrónicas de grandes magnitudes han sido un gran reto para la legislación vigente tanto a nivel nacional como a nivel internacional. Este tipo de delitos no cuenta con los medios y equipos adecuados para lograr una investigación eficaz que coadyuven al juzgamiento efectivo de los mismos.

Se suele referir a la apropiación de la identidad cuando otra persona para aparentar ser ella, asume su identidad frente a terceros con fines de obtener ganancias económicas o cualquier otro tipo de beneficio es denominado como robo de identidad. (García, 2015)

El robo de identidad es definido como aquella apropiación de identidad de una persona para hacerse pasar por ella, para asumir su identidad frente a terceros públicos o privados a fin de obtener ciertos recursos o beneficios a su nombre.

La identidad es un beneficio otorgado por el Estado para la ciudadanía, ya que corresponde a éste otorgar los recursos necesarios para generar documentos oficiales que acrediten los datos personales de los solicitantes, por ello es que cada integrante de las poblaciones cuenta con documentaciones que demuestren su nacionalidad, lugar de nacimiento, fecha de nacimiento, y número de control dentro de los registros de cada entidad.

Las actividades como la clonación de tarjeta, alteración y falsificación de documentos oficiales de identidad, envío de mensajes vía internet o celular anunciando supuestos sorteos o concursos, o hackeo de cuentas,

son tan solo algunas de las actividades derivadas de la suplantación de identidad.

Esta conducta antisocial permite favorecer ciertos delitos como el caso del tráfico de personas, terrorismo, usurpación de funciones, falsificación y alteración de documentos en general, lavado de dinero, entre otros, por ello debe atenderse con prontitud la problemática que afectó de manera indirecta gracias a la tecnología o de algunas artimañas de la delincuencia (Pino, Delitos Informáticos, 2016)

La delincuencia busca diversas situaciones que pueden ser bien aprovechadas para cometer delitos o simplemente para perjudicar a sus semejantes, como muestra de este acontecimiento, la suplantación de identidad, fenómeno que retoma fuerza por la vulnerabilidad y confianza de la población, este procedimiento sucede cuando simplemente a través de la telefonía la víctima acepta brindar cualquier información que le solicita el moderador, sin razonar plenamente que se puede tratar de un sujeto que utilice dicha confidencialidad para obtener beneficios económicos o patrimoniales que son fruto del esfuerzo del trabajo de la ciudadanía.

Contexto histórico

Los delitos informáticos tuvieron origen a finales de la segunda guerra mundial, tras eso investigaron nuevas formas de vulnerar a los estados que se encuentran en conflictos unos con otros. La investigación tecnológica empezó a atacar a los equipos de telecomunicaciones para limitarlos de pedir ayuda, refuerzos, o armamento para comunicarse o protegerse.

Posteriormente, el Internet se convirtió en una herramienta de fácil acceso y obtención, pero se ha tratado de imponer algunas normativas para regularlo. Por el crecimiento inminente de la tecnología, se ha dado un mal uso de la misma y ha aparecido una serie de actos ilícitos, a los cuales se conoce como delitos informáticos. (Somellera, 2010)

Durante los años 60, diferentes programadores o especialistas en informática intentaban boicotear el financiamiento gubernamental a la guerra de Vietnam mediante el uso gratuito del servicio telefónico. Posteriormente, el activismo político hippie de la época tuvo su costado informático a través de las llamadas blue box o cajas azules que establecían comunicaciones en forma gratuita simulando los tonos de llamadas utilizadas por la Bell Corporation y la ATT, básicamente para comunicaciones de larga distancia.

Con el correr del tiempo, estas técnicas de hacking alcanzaron un mayor grado de sofisticación, utilizadas también para las manipulaciones de transferencias de dinero por redes telefónicas vulnerables. En cuanto a la utilización de computadoras, la principal preocupación estaba dada por el manejo de la información a partir del almacenamiento y procesamiento de datos personales.

En 1970 se registraron una serie de casos que arrojan pérdidas cuantiosas para los sectores privados. El desarrollo de los delitos económicos como el espionaje informático, la piratería de software, el sabotaje y la extorsión por medio de los dispositivos informáticos, el robo directo de los mismos para la extracción de información.

Los objetivos de los delitos eran los programas de computación, los datos de investigación en el área de defensa, la información contable de las empresas y la cartera de direcciones de clientes corporativas. En relación a la piratería de software, la modalidad característica era la copia no autorizada de programas de computadora para su comercialización en el marco espionaje industrial. (Vallejo, 2010)

Las personas usan las máquinas electrónicas como instrumentos para efectuar los delitos electrónicos. El fenómeno informático ha sido incuestionable e irreversible para la sociedad. Los equipos tecnológicos se los usan como medios de almacenamiento, y procesamiento de datos que tienen la necesidad de regularse con una normativa que reglamente el uso de la red y el control de este servicio. En los casos de sabotaje y extorsión

informática, estos eran los delitos que más preocupaban a las administraciones gubernamentales y empresas ante la alta concentración de datos almacenados electrónicos.

Los objetivos eran tanto bienes tangibles; es decir, dispositivos físicos como intangibles, y datos e información que afectan tanto el hardware como de software de los dispositivos. En la década de 1980, los delitos informáticos adquieren mayor notoriedad a partir de un aumento exponencial de fraudes y el tratamiento de la problemática por parte de organismos internacionales.

Los casos típicos se realizaban mediante la manipulación de uso de tarjetas de débito en cajeros automáticos, fundamentalmente a través de la vulneración de las bandas magnéticas. Esto motivó la utilización por parte de las empresas emisoras de la adopción de chips en los plásticos como medida de seguridad. La cobertura legal de las bases de datos de las instituciones bancarias y empresas resultaba indispensable para la realización de negocios, fundamentalmente contra el robo de información comercial.

Los delitos de suplantación de identidad y el espionaje, utilizan la suplantación de personas para cometer otro delito informático. Para ello se basan de las artimañas y engaños tendientes a obtener, vía suplantación, el acceso a los sistemas o códigos privados de utilización de ciertos programas generalmente reservados a personas en las que se ha depositado un nivel de confianza importante en razón de su capacidad y posición al interior de una organización. (Carrillo, 2016)

La suplantación de identidad se asocia al uso público de un nombre y apellidos de un tercero ficticio, que puede existir o ser imaginario. Por ejemplo: aquella persona que abre una cuenta en una red social creando un perfil falso con la finalidad de enmascarar su identidad y con la intención de hacerse pasar por otro. Este tipo de acto en concreto que tienen como finalidad disfrazar su propia identidad, es un delito.

La difusión sobre el tema de robo de identidad y las medidas que deben de seguirse es una obligación para todos los usuarios de computadoras, tabletas, teléfonos celulares y extenderlo a los usuarios de las redes sociales como Facebook pues debido a la propia naturaleza de estas formas de comunicación, las personas son animadas a compartir información personal y de sus contactos por lo que un número cada vez mayor de usuarios se convierten en víctimas del robo de identidad.

Planteamiento del problema científico

Los delitos electrónicos son un tema muy concurrente diariamente sobre este delito informático que perjudica la seguridad jurídica y la identidad única de los ciudadanos y esto crea un problema económico, social y psicológico que perjudica a las instituciones que son usadas como puente para este delito informático y tienen que hacerse responsable en los gastos de las víctimas y afecta el prestigio de los sistemas informáticos perdiendo potenciales clientes por el miedo a ser víctimas del mismo.

Se puede confirmar teóricamente una de las causas favorables para los delitos electrónicos que perjudican los derechos de identidad y seguridad jurídica en los ciudadanos del Ecuador, es el desconocimiento de los usuarios de los sistemas informáticos los cuales no saben ni verificar si fueron afectados por este delito informático tendrán información necesaria de sus derechos y las maneras de evitar estos delitos y que hacer inmediatamente cuando eres perjudicado de estos delitos y como evitar ser afectado para que sus derechos no se vean vulnerados.

Pregunta problema

¿Cuáles son las alternativas legales que establece el marco normativo ecuatoriano para proteger la identidad de las personas en los medios digitales?

Objetivos

Objetivo general

Analizar los delitos informáticos de suplantación de identidad relacionado a los derechos constitucionales del Ecuador 2020-2021.

Objetivos específicos

- Realizar una revisión teórica respecto de los delitos informáticos de suplantación de identidad período 2020-2021
- Implementar una entrevista a un grupo de expertos acerca del tema del delito informático de suplantación de identidad.
- Proponer una reforma de ley al Código Orgánico Integral Penal en lo que respecta a los delitos de suplantación de identidad.

Justificación

La tecnológica ha provocado grandes desventajas, que dan oportunidad a que seres malintencionados vulneren los derechos de otras personas, por medio de delitos informáticos. Los usuarios de Internet cada vez son más víctimas de suplantación de identidad. El uso general de las redes sociales incrementa los riesgos que se extienden a anuncios y publicidad falsa.

Dentro de las realidades actuales, la suplantación de identidad es considerada uno de los delitos informáticos más famosos por lo cual, en el presente trabajo de titulación se investigará y analizará los casos que sucedieron en Ecuador. Por lo que se demostrará dentro de un análisis comparativo el índice de incremento o disminución en el año 2020.

Novedad científica

La presente investigación busca establecer la realidad social sobre los delitos cibernéticos que pueden ser sujetos vulnerables las personas en todo el mundo, por ende, cada país debe de regular ese avance tecnológico que perjudica a los ciudadanos.

Los delitos informáticos son varios, pero en particular, la suplantación de identidad que es el principal delito que ha conmocionado a los ciudadanos en diversos países por el avance tecnológico y la Internet que avanza aceleradamente.

Ecuador ha sido un país cuya normativa trata de estar a la vanguardia al igual que la tecnología, pero la interrogante que se ha planteado es si los mecanismos que ofrece la ley son los suficientes para llevar a cabo una investigación previa.

CAPÍTULO I: MARCO TEÓRICO

1.1. Teoría del delito

La teoría del delito es una herramienta que sirve para resolver los problemas específicos de los delitos. Es un sistema categorial, clasificatorio y secuencial en el que se puede analizar los diferentes elementos esenciales comunes a todas las formas de aparición del delito (Calderón, 2010).

Los elementos como: acción, tipicidad, antijuricidad, culpabilidad constituyen los pilares desde los que se erige el sistema de la teoría del delito, que debe ser coherente para cumplir adecuadamente su función principal en la práctica jurídica: resolver problemas específicos de aplicación.

Por ello, la teoría del delito debe construirse desde los cimientos que proporcionan las mismas normas penales, pues de nada serviría el sistema si entrara en contradicción con lo expuesto en los textos legales. Por ello, no debe haber contradicciones internas al propio sistema, pues éstas podrían aniquilar el sistema.

El medio más útil y eficaz para conceptualizar la aplicación racional de la ley penal en cada caso en concreto. La teoría del delito, sigue un orden lógico para su aplicación, primero verifica que la conducta humana, es decir, la acción se encuentra adecuada a la descripción realizada por el tipo, lo que es la tipicidad.

Consecuentemente que dicha conducta sea contraria al ordenamiento jurídico como antijuricidad, y finalmente comprobar que el sujeto autor de esa conducta tiene las condiciones de conciencia y voluntad para poder imputarle dicho actuar, como culpabilidad.

Es un método sistemático que al reunir y estructurar todos los elementos del delito en un sistema dogmático permite interpretar y aplicar el Derecho penal; es decir, si concurre una acción, se examinará primero la tipicidad y luego la antijuricidad, culpabilidad y demás presupuestos de la punibilidad. (Antolisei, 2005)

La teoría del delito clasifica los elementos comunes de todos los delitos. Desde la óptica causal del delito, la acción es un hecho voluntario, bien sea de carácter físico o mecánico, que produce un resultado regulado por la norma penal sin tener en cuenta la finalidad de la acción cometida.

1.1.1. Concepto de infracción penal

El derecho penal es la ciencia que estudia las conductas humanas que se determinan como infracciones, como consecuencia, se establecen sanciones como una medida de protección social por parte del Estado. Los tipos de conductas humanas se pueden clasificar como infracciones penales, las misma que puede subdividirse en dos niveles: delitos y contravenciones. (Bacigalupo, 1996)

La infracción es una transgresión, quebrantamiento, violación, incumplimiento de ley, pacto o un tratado, lo cual, es toda denominación punible, que puede ser un delito o una falta. Es una violación a la norma jurídica, por parte del agente que actúa fuera de los parámetros de ley que rige para los ciudadanos en general.

No obstante, la definición doctrinaria no indica cual es sujeto a quien va dirigido el acto imputable, ya que solo las personas sujetas de imputación de infracción puede ser sujetos actores o victimarios de una conducta humana, típica, antijurídica, culpable. Toda infracción, tiene una sanción. En el código orgánico integral penal ecuatoriano, se define a la infracción como toda conducta típica, antijurídica y culpable cuya sanción se encuentra prevista en este Código Orgánico Integral Penal, estableciendo la composición esencial de los elementos para determinar un delito. (Torre, 1993)

La conducta previa a clasificarse, debe determinarse si es acción u omisión, para poder considerarla como una infracción, además de reunir los elementos que componen a la infracción penal: el primer elemento es tipicidad, que son los tipos penales que se encuentran tipificado en un cuerpo normativo, al momento de la comisión de la conducta.

Por otro lado, se encuentra la antijuricidad, es aquella que debe amenazar o lesionar sin justa causa, un bien jurídico protegido por el cuerpo legal. Por ende, se lo conoce por ser contraria al orden público o jurídico, lesiva y va en contra de los bienes jurídicos protegidos por el Derecho.

No existe una causa o una razón justa, sin embargo, a toda regla general, se aplica una excepción en los cuales se justifica la realización de una conducta sancionada de manera penal, en este caso aplicaría las causas de exclusión de la conducta, las causas de exclusión de antijuricidad y las causas de inculpabilidad.

1.1.2. Acción

La conducta humana es penalmente relevante sólo la que se exterioriza, no importa las características físicas de la persona, ni los hechos involuntarios. Conducta humana que ocasione un resultado dañino o ponga en peligro un bien jurídico tanto por Acción u Omisión. La conducta conformada por la acción u omisión de la persona que ponga en peligro su vida o de un tercero, mediante la producción de un acto que resulte lesivo. En conjunto con la tipicidad, antijuricidad, culpabilidad dan como resultado la pena. (Suarez, 2000)

La acción es un concepto básico en el derecho procesal, pero hay profundas diferencias entre materia penal y materia civil. En materia penal, la acción se encamina en la aplicación jurídica del derecho penal, para lo cual es necesario para que las personas víctimas de alguna violación de los derechos humanos puede ejercer la acción y exigir que se le repare integralmente por los daños ocasionados.

La acción penal es un instrumento del derecho, el cual da origen al proceso judicial en la jurisdicción penal cuando una persona natural o jurídica es víctima de un delito. Mediante la acción penal se lleva a las personas ante un juez para que juzgue los hechos imputables a determinada persona. (Rosal, 1999)

De forma general, la acción tiene tres acepciones; en primer lugar, el derecho, luego, la pretensión y finalmente, el poder público. La acción penal como derecho no puede ser considerada, dado que es una simple facultad del estado ejercer o no dicha acción. La regla general es que la ejerza siempre, pero existen ciertas excepciones.

Es la facultada de dar la iniciativa procesal y crear la obligación al juez o actividad su deber de comprobar que la situación concreta del hecho imputado se le declare si se constituye delito o no, determinar la culpabilidad y establecer la sanción adecuada dependiendo del daño ocasionado y la gravedad del acto.

La acción penal constituye un derecho de iniciativa, ya sea considerado como derecho o un poder, ya sea abstracto o concreto, una obligación o una potestad cuando el Estado es quien tiene el deber principal de asegurar que la norma jurídica sea cumplida por los ciudadanos y los funcionarios. (Molina, 1994)

De manera general, se podría indicar que la acción penal es el poder jurídico que se pone en conocimiento de una autoridad jurisdiccional competente acerca una noticia criminal, el cual origina el procesamiento de una o varias personas determinadas por medio de la formulación de los cargos, de esta forma, se inicia el proceso penal y se obliga al juez de que se pronuncie de forma motivada sobre el mismo.

1.1.3. Tipicidad

Es la adecuación del acto humano voluntario efectuado por el sujeto a la figura descrita por la ley como delito. La aplica el juez. Es la adecuación de un hecho cometido a la descripción que de ese hecho se hace en la ley penal.

La tipicidad es la conducta adecuada a los elementos que componen un determinado tipo penal, es decir, se componga por dolo, culpa o preterintención. El dolo es compuesto por el designio de causar daño, conocimientos de los hechos voluntad en un aspecto positivo y por una

conducta negativa es cuando no encaja la conducta en la descripción típica. (Pozo, 2005)

La tipicidad es un tipo de conducta que crea el legislador para hacer una valoración determinada en una conducta delictiva. Es una descripción abstracta de la conducta prohibida. Es un instrumento legal, lógica necesaria y de naturaleza descriptiva que tiene como función la individualización de las conductas humanas penalmente relevante.

Es la adecuación del acto humano voluntario ejecutado por el sujeto a la figura descrita por la ley penal como delito. Es la correlación, adecuación o la subsunción del acto humano voluntario al tipo penal. Si se adecua la conducta al tipo penal, es un delito. Si la adecuación no es compatible, no hay delito. La adecuación debe ser jurídica, mas no social.

La tipicidad penal es la criminalización de una norma de cultura realizada por el legislador y es establecida en la ley penal. La tipicidad es aplicada por el juez, mediante la calificación de un comportamiento como delito. Es la adecuación del acto humano voluntario que es ejecutado por el sujeto descrito por la ley penal como delito. Si la adecuación es completa, es indicio que es delito; si no es completa, no es delito. (Jakobs, 1996)

Son características y actividades que dependen del fuero interno del agente. Son tomados en cuenta para describir el tipo legal de la conducta, por eso estos elementos tienen que probarse. Se debe probar que sabía; se debe probar que actuó en calidad de titular, etc. e. Son tomados en cuenta para describir el tipo legal de la conducta, por eso estos elementos tienen que probarse. El juez no podrá enjuiciar como ilícitos aquellos comportamientos que no se adecuen a alguno de ellos, aun cuando parezcan manifiestamente injustos o contrarios a la moral.

1.1.4. Antijuridicidad

La antijuridicidad es la contradicción de la realización del tipo de una norma prohibida con el ordenamiento jurídico en su conjunto. Es un juicio

de valor objetivo, en tanto se pronuncia sobre la conducta típica, a partir de un criterio general, como un ordenamiento jurídico.

La adecuación de un acto a la descripción legal implica la violación de la norma prohibitiva o preceptiva implícita en una disposición penal. Es el acto voluntario típico que contraviene el presupuesto de la norma penal, lesionando o poniendo en peligro bienes e intereses tutelados por el Derecho. (Pineda, 1996)

La antijuridicidad es un juicio impersonal objetivo sobre la contradicción existente entre el hecho y el ordenamiento jurídico. La condición o presupuesto de la antijuridicidad es el tipo penal. El tipo penal es el elemento descriptivo del delito, la antijuridicidad es el elemento valorativo.

La contradicción entre la acción realizada y las exigencias del ordenamiento jurídico, es lo que se conoce como antijuridicidad. A diferencia de lo que sucede con otras categorías de la teoría del delito, la antijuridicidad no es un concepto específico del derecho penal, sino un concepto unitario válido para todo el ordenamiento jurídico, aunque tenga consecuencias distintas en cada rama del mismo. (Puig, 2002)

El ordenamiento jurídico está constituido por preceptos prohibitivos y preceptos permisivos. La violación de los primeros define una conducta típica, un indicio de antijuridicidad. Es necesario establecer si la conducta típica realizada tiene una causa de justificación para determinar su antijuridicidad. Es decir, si la acción típica se ha cometido en legítima defensa, estado de necesidad, cumplimiento de órdenes, consentimiento, entonces, la conducta siendo típica no es antijurídica y, por lo tanto, no hay delito.

1.1.5. Culpabilidad

Es la culpabilidad es el juicio necesario para vincular en forma personalizada, y operar como principal indicador del máximo de poder punitivo que puede ejercerse sobre éste. Es la situación en que se

encuentra una persona imputable y responsable, que pudiendo haberse conducido de una manera no lo hizo, por lo cual el juez le declara merecedor de una pena. (Cabrera, 1999)

Es la situación en que se encuentra una persona imputable y responsable. Es una relación de causalidad ética y psicológica entre un sujeto y su conducta. Va dirigido a ver el furo interno de la persona y ver si es atribuible o no aquel delito. La culpabilidad se limita con la necesidad de prevención y juntas originan el nuevo concepto de responsabilidad, que es la base de la imposición de la pena

Es un concepto de carácter normativo, que se funda en que el sujeto podía hacer algo distinto a lo que hizo y le era exigible en esas circunstancias. El primero de los presupuestos de cualquier reproche de culpabilidad se halla en que el autor, al momento del hecho, haya sido siquiera capaz de actuar de modo responsable: de comprender lo ilícito del hecho y de dejarse determinar por esa comprensión, renunciando a su realización.

1.2. Delitos informáticos

1.2.1. Conceptos

Todas aquellas acciones u omisiones típicas, antijurídicas y dolosas, cometidos contra personas naturales o jurídicas, realizadas en uso de un sistema de tratamiento de la información y destinadas a producir un perjuicio en la víctima a través de atentados a la sana técnica informática, lo cual, generalmente, producirá lesiones a distintos valores jurídicos, un beneficio ilícito en el agente, sea o no de carácter patrimonial, actúe con o sin ánimo de lucro. (Castillo, 2018)

En derecho penal, la ejecución de la conducta punible supone la existencia de dos sujetos, a saber, un sujeto activo y otro pasivo. Estos, a su vez, pueden ser una o varias personas naturales o jurídicas; mientras que, el bien jurídico protegido será en definitiva el elemento localizador de los sujetos y de su posición frente al delito.

El titular del bien jurídico lesionado será el sujeto pasivo, quien puede diferir del sujeto perjudicado, el cual puede, eventualmente, ser un tercero. Por otra parte, quien lesione el bien que se protege, a través de la realización del tipo penal, será el ofensor o sujeto activo.

Los delitos informáticos son ciertas características que no presentan el denominador común de los delincuentes, esto es, los sujetos activos tienen habilidades para el manejo de los sistemas informáticos y generalmente por su situación laboral se encuentran en lugares estratégicos donde se maneja información de carácter sensible, o bien son hábiles en el uso de los sistemas informatizados, aún cuando, en muchos de los casos, no desarrollen actividades laborales que faciliten la comisión de este tipo de delitos. (Castro, 2008)

Con el tiempo se ha podido comprobar que los autores de los delitos informáticos son muy diversos y que lo que los diferencia entre sí es la naturaleza de los delitos cometidos. De esta forma, la persona que entra en un sistema informático sin intenciones delictivas es muy diferente del empleado de una institución financiera que “desvía fondos” de las cuentas de sus clientes.

Es un conjunto de comportamientos dignos de reproche penal que tienen por instrumento o por objeto a los sistemas o elementos de técnica informática, o que están en relación significativa con ésta, pudiendo presentar múltiples formas de lesión de variados bienes jurídicos.

1.2.2. Tipos de delitos informáticos

Los tipos de delitos informáticos, enfocados con la diversidad de comportamientos constitutivos de esta clase de ilícitos es inimaginable, el único límite existente viene dado por la conjugación de tres factores: la imaginación del autor, su capacidad técnica y las deficiencias de control existentes en las instalaciones informáticas.

En la clasificación se encuentran los delitos por fraudes: es decir, los datos falsos o engañosos, que son comúnmente conocidos como

introducción de datos falsos como una manipulación de datos de entrada al computador con el fin de producir o lograr movimientos falsos en transacciones de una empresa. Representa el delito informático que no requiere de conocimientos técnicos de informática y puede realizarlo cualquier persona que tenga acceso a las funciones normales de procesamiento de datos en la fase de adquisición de los mismos. (Maynez, 2009)

Por otro lado, el phishing es una modalidad de fraude informático que busca robar la identidad del sujeto pasivo, es decir, consiste en obtener información como número de tarjetas de créditos, contraseñas, información de cuentas u otros datos procesales por medio de engaños. El robo de identidad es uno de los delitos que más han aumentado y ocurre habitualmente a través de mensajes de correo electrónico o de ventanas emergentes.

Otro tipo de delito, se encuentra el sabotaje informático que consiste en el acto de borrar, suprimir o modificar sin autorización funciones o datos de computadora con intención de obstaculizar el funcionamiento normal del sistema. Las técnicas que permiten cometer sabotajes informáticos que son: virus informáticos y malware como elementos informáticos que tienden a reproducirse y a extenderse dentro del sistema al que acceden, se contagian de un sistema a otro, exhibe diversos grados de malignidad y son susceptible de destrucción con el uso de ciertos antivirus. (Pino, Delitos Informáticos: Generalidades, 2015)

El terrorismo informático es el acto de hacer algo para desestabilizar un país o aplicar presión a un gobierno, utilizando métodos clasificados dentro los tipos de delitos informáticos, especialmente de los tipos de sabotaje sin que pueda limitar el uso de los tipos de delitos informáticos con menos recursos humanos y financiamiento económico que permite un ataque terrorista común.

1.3. Delito de suplantación de identidad

1.3.1. Definiciones

La evolución humana tiene un proceso que se desarrolla en diferentes circunstancias, una de ellas se enfoca en la conducta y la colectividad, lo que conlleva la creación de nuevos delitos, y sobrepasan los límites de lo moral y legalmente permitidos

La identidad es un beneficio otorgado por el Estado para la ciudadanía, ya que corresponde a éste otorgar los recursos necesarios para generar documentos oficiales que acrediten los datos personales de los solicitantes, por ello es que cada integrante de las poblaciones cuenta con documentaciones que demuestren su nacionalidad, lugar de nacimiento, fecha de nacimiento, y número de control dentro de los registros de cada entidad. (Ramirez, 1989)

La delincuencia busca diversas situaciones que pueden cometer delitos o simplemente para perjudicar a sus semejantes, como muestra de este acontecimiento, la suplantación de identidad, es un fenómeno que retoma fuerza por la vulnerabilidad y confianza de la población.

La suplantación de identidad dentro de una red social es una nueva realidad y la misma no tiene como único y exclusivo blanco a personajes notorios como políticos o deportistas, pues también el usuario anónimo puede ser suplantado, generándose un pequeño terremoto en sus relaciones personales.

Es un proceso que se desarrolla en diferentes circunstancias, una de ellas es la conducta del hombre y la colectividad, este asunto alcanza en ocasiones a crear nuevos delitos, y esto sucede cuando el individuo se da cuenta que ha madurado emocionalmente y ha pasado la línea de superación y de superioridad, luego entonces se da cuenta que es necesario adquirir nuevos conocimientos y artimañas para sobrepasar los límites de lo moral y legalmente permitidos. (Salgado J. A., 2003)

La suplantación de identidad es el uso indebido de identificaciones personales e información confidencial y privada por medio de vías físicas, informáticas, electrónicas y de telecomunicaciones para ejecutar actividades ilícitas perjudiciales, como un aspecto que contempla diversas modalidades de la conducta antisocial y no parte únicamente de lo posiblemente tangible.

Es una actividad maliciosa en la que un atacante se hace pasar por otra persona para cometer fraudes, ciberacosar, sextorsión, etcétera. Se asocia al uso público de un nombre y apellidos de un tercero ficticio, que puede existir o ser imaginario.

1.3.2. Características

Suplantación es considerado como acción y efecto de suplantar, y éste último se precisa de la siguiente manera: Expresión que se define como ocupar con malas artes el lugar de alguien, defraudándole el derecho, empleo o favor que disfrutaba. Ser suplantado en internet puede provocar situaciones especialmente duras, sobre todo cuando se trata de sujetos especialmente sensibles, como pueden ser los menores de edad. (Valdez, 2004)

El robo de identidad, se ha convertido en la forma más común de fraude al consumidor en Internet, y la manera más corriente es mediante el abuso de información de tarjetas de crédito, esta actividad puede causar efectos depresivos en la economía, elevar los costes del crédito y reducir la confianza en el comercio electrónico.

La suplantación de identidad tiene un sin número de modalidades que son poco perceptibles o desconocidas por la autoridad competente, así como por víctimas, por ello es necesario realizar una clasificación de las modalidades derivadas de ésta conducta antisocial.

La suplantación de identidad es una nueva conducta antisocial que debe ser estudiada debidamente por un Criminólogo-criminalista, ya que se están pasando por desapercibido muchos factores que son de confort para

la delincuencia, y que si no es atendido en estos momentos se puede convertir en un verdadero problema de seguridad que no solo afectaría a la ciudadanía, sino que a la base de datos de las instituciones públicas y privadas. (Vasquez, 2005)

1.3.3. Consecuencias

Las consecuencias de la suplantación se basan en la pérdida económica directa del titular del derecho afectado, para comprometer su historia crediticia, su prestigio y hasta su identidad social. La atribución de una identidad permite establecer posibles conductas imputables de una persona. Es un hecho o conducta que une a varias personas mediante la identidad, es decir, tiene una significación fundamental sobre relaciones y atribuciones.

La defraudación es obtenida como una ganancia injusta a costa de la persona cuyo derecho de crédito se usurpa; y, por otro lado, la impostura de la identidad ajena con un propósito más amplio, que incluye, pero no se agota en la continuación de la defraudación, como podría ser el evadir responsabilidades penales o el desviar la atención sobre otras actividades ilícitas del impostor. (Zapater, 1986)

Las acciones que se llevan a cabo con este delito implica la obtención de un lucro indebido, lo cual recae en los operadores del delito cuando existe un cúmulo de bases de datos personales que no se alinean con las adquisiciones de medios legales.

Otros efectos son principalmente los daños económicos, como la imputación de ciertos gastos y operaciones comerciales que aparecen de forma injustificada en la cuenta o base de datos del titular, lo cual implica un pago que no se tenía conocimiento y por ende, hay negación al pago por dicha operación ilegal. Debido a ello, existe un daño patrimonial por la usurpación de identidad que sucede ante la invasión de la privacidad o la intimidad de las personas.

1.3.4. Tipo objetivo

La tipicidad objetiva en los delitos de mera actividad consiste en determinar si la conducta realizada se enmarca en la conducta antijurídica determinada en la normativa. El elemento objetivo abarca el lado externo de la conducta, y está integrado por un elemento normativo, sujeto activo, sujeto pasivo, bien jurídico lesionado y nexo causal entre acción y resultado.

Por otro lado, el elemento subjetivo pertenece a la parte psíquica del sujeto activo que realiza la acción, o de un tercero, y está conformado por el dolo y la culpa. Estos elementos presuponen la existencia de un presupuesto legal, que va a estar sujeto a una valoración que la realizará el juez que debe aplicar la ley. (Antolisei, 2005)

En este tipo de delito se refiere a la persona, que por su esencia busca sancionar a un individuo tangible de forma directa, por el acto cometido, para lo cual el legislador, lo definió de manera general sin hacer ningún tipo de distinción, sea de forma física como digital. La parte objetiva viene constituida por el aspecto externo de la conducta. Ahí se exterioriza el proceso humano por el agente contra realidades jurídicamente valoradas.

1.3.5. Bien jurídico protegido

De acuerdo a las opiniones doctrinales, el delito de suplantación de identidad se refiere al derecho a la identidad, que hace referencia al conjunto de rasgos propios de un sujeto o de una comunidad. Las cuales diferencian a un individuo o grupo, se encuentra vinculada en la conciencia de una persona que tiene sobre sí misma.

El ser humano tiene un sin número de derechos y obligaciones, entre ellos está el derecho a la identidad que tiene cada persona, al momento de tener un nombre o apellido debidamente registrado. Se compone por el conjunto de datos o referencias que hace a un individuo único, y puede ser diferenciado con amplia claridad.

1.3.6. Sujeto activo

En general, el sujeto activo es considerado toda persona, sea hombre o mujer quien ejecuta la acción delictiva, debido a que, en este caso no se podría determinar porque puede ser cualquier persona interesada en suplantar la identidad de otra persona para obtener beneficio para sí o para un tercero. (Ballesteros, 2006)

El sujeto activo es la persona que perpetra un hecho punible y a quien se le imputará responsabilidad penal por el cometimiento de ese hecho punible, pero esta responsabilidad sólo puede ser atribuida a seres humanos que son quienes pueden realizar conductas.

Este tipo de sujeto activo es cualquier persona por lo que no se determina edad o característica especial alguna para el sujeto activo quien, en este caso, incluso consideraría a los menores de edad como sujetos activos. Lo definen como la persona que está bajo la voluntad propia, sea por acción u omisión esperando el resultado que, de la fase interna, se lleve a cabo la fase de ejecución.

No se requiere que el sujeto enmarque alguna condición personal relacionada con la autoría, con excepción de algunos tipos agravados que exigen en el agente una cualificación especial, que antiguamente se determinaba para el *parricidio, en el caso de la antigua roma*, sin embargo, actualmente, existe la indeterminación del sujeto activo. (Barrera, 2017)

Es el agente que ejecuta el acto delictivo y que debe, en consecuencia, sufrir la pena correspondiente, es el enjuiciado en el proceso. Además de la individualidad, está en la cantidad, puede ser un solo individuo, pero en otros casos serán varios los que realizan el acto en conjunto o que cooperan a su realización, pero para ello, se debe determinar el grado de participación de cada sujeto que intervino en la ejecución del delito.

1.3.7. Sujeto pasivo

El sujeto pasivo es considerado el titular del bien jurídico protegido, y en el delito de suplantación de identidad, puede ser al igual que el sujeto activo, cualquier persona, sea hombre o mujer, la víctima del acto delictivo. Es cualquier persona menor o mayor de 18 años, de cualquier sexo, sea con o sin discapacidad.

Cabrera, (1999) considera al sujeto pasivo, es decir, al titular del derecho a la vida, como toda persona con existencia visible, dado que, si es aborto, no sería homicidio sino aborto, porque la interrupción de vida de un feto. Por ende, puede ser cualquier persona con vida independiente, pero debe tratarse de una persona distinta al autor, dado que, quien no mata a otro sino a sí mismo no realiza el homicidio, sino que se suicidio, lo cual no enmarca la figura delictiva.

1.3.8. Verbo rector

El delito es una acción determinada y expresada gramaticalmente por un verbo en cualquiera de sus formas. La realidad del delito recae en la acción típica. La realidad física, consiste en el objeto material del delito, pero considerada en su valoración jurídica al bien jurídico. (Pineda, 1996)

En este caso, el verbo rector es suplantar que se refiere a suplantar la identidad de un tercero o mediante el uso de una identidad falsa por medios electrónicos o telemáticos, y con ellos se establezca o se efectúen acciones ilegales perjudicando al propietario de dicha identidad, será sancionado con pena privativa de libertad de tres a cinco años.

1.3.9. Tipo subjetivo

En el tipo subjetivo o parte subjetiva del tipo se estudian los posicionamientos subjetivos que al entender del legislador son más peligrosos en abstracto, así por ejemplo un tipo doloso tendrá más pena que uno culposo. Es un escenario distinto como lo es la categoría dogmática de la conducta. (Molina, 1994)

La parte subjetiva se constituye a la voluntad que se dirige al resultado, a la conducta. García, (1952) anuncia a la producción del resultado dentro del fin o ámbito de protección de la norma infringida, por medio del cual, los resultados dentro del fin o ámbito de protección de la norma no pueden ser imputados a su autor, la provocación imprudente de un suicidio, la puesta en peligro de un tercero aceptada por este. El delito puede ser causado por cualquier medio, indiferente su naturaleza o poder letal del medio para provocar el resultado.

Casabona, (2016) define el homicidio simple como un delito doloso. El dolo se lo considera como la conciencia o la voluntad de realizar una conducta dirigida a la producción de la muerte de otra persona. La configuración subjetiva típica no requiere de ninguna motivación ni finalidad específica. Existen tres clases de dolo admisible: directo, indirecto y eventual.

El error de tipo, de algunos elementos del tipo objetivo, excluye el dolo, y la responsabilidad penal, si el error es invencible. En el caso, que el error es vencible, el autor deberá responder por el homicidio a título de culpa. Un error en la identidad, se considera un homicidio doloso, dado que no se protege a una persona en particular, sino a todos por igual. De igual forma, en caso de una desviación por error, no aplica, porque no es uniforme el delito, la subjetividad típica sigue siendo la misma.

1.4. Diferencia entre Suplantación y Usurpación de identidad

Para ser considerada usurpación depende si la cuenta es creada aleatoriamente o se utiliza una cuenta ya existente. Todas las modalidades implican generar un error sobre la identidad del titular, una forma de defraudar que se está extendiendo ampliamente en la era del comercio electrónico. (Zabaleezequiel, 2002)

Es una modalidad mediante la cual alguien suplanta a alguna otra persona en la titularidad de un derecho o una pretensión para obtener un bien o una prestación. Se puede distinguir entre hurto y fraude de identidad,

en el primer caso nos referimos a la suplantación de un titular y, en el segundo, a la creación de una identidad ficticia con el fin de defraudar

La usurpación de identidad es un modo particular de ejecución del delito de estafa, como la obtención indebida de bienes y servicios sin autorización del titular mediante el uso de tarjetas ajenas haciéndose pasar por su titular, o la alteración de instrumentos electrónicos de crédito o pago con el fin de obtener dichos beneficios que puede operar mediante la réplica de la información en otros instrumentos o mediante la incorporación de usuarios a registros informatizados.

La inserción de instrucciones falsas o fraudulentas para obtener el provecho injusto, distinción que reconoce una conducta directa e inmediata, en el tipo del hurto, y una indirecta y mediata en el de estafa, que pasa por el ardid para inducir la equivocación, en esta última, y que ha sido fuente de disputas doctrinarias y jurisprudenciales. (Zaffaroni R. E., 1986)

La suplantación y usurpación de identidad en Internet son dos conceptos análogos, aunque con una repercusión jurídica distinta. Tienen conceptos muy relacionados, en primer lugar, la suplantación hace referencia a la acción de suplantar, es decir, ocupar con malas artes el lugar de alguien, defraudándole el derecho, empleo o favor que disfrutaba y, en segundo lugar, la usurpación se comete por quien utiliza de forma estable el estado civil, nombre y apellidos de otra persona, suplantando su personalidad.

Se entiende por suplantación de identidad en internet, aquella acción por la cual una persona se hace pasar por otra en Internet. Se trata de la mera apropiación de derechos y facultades propias de la persona suplantada como podría ser la apropiación de redes sociales ajenas.

En este aspecto, debemos diferenciar entre el suplantador y el suplantado, siendo el primero la persona física o jurídica que realiza el acto de apropiarse de cuentas u elementos identificativos de otra persona, el suplantado.

Por otro lado, la usurpación de identidad en Internet, tiene lugar desde que el suplantador empieza a realizar actos desde el perfil del suplantado haciendo entender que actúa siendo el suplantado, propietario de los derechos y facultades. La suplantación de identidad se convierte en usurpación de identidad y, en consecuencia, el suplantador pasa a denominarse usurpador y el suplantado pasa a ser el usurpado.

En la usurpación de identidad en redes sociales, el usurpado es la persona física o jurídica cuya identidad ha sido apropiada por un tercero que tiene abierta una cuenta en una red social, y que la usa habitualmente, para fines personales o profesionales; mientras que, el usurpador es la persona física o jurídica que se apropia de la identidad de un tercero haciéndose pasar por él y realizando acciones como si de él se tratase, como podrían ser la publicación de contenidos inapropiados o el envío de mensajes a terceros. (Arrieta, 2016)

La diferencia entre suplantación y usurpación de identidad radica en que, mientras en la primera únicamente se lleva a cabo la apropiación de derechos y facultades de un perfil que pertenece e identifica a un tercero, en la segunda, además de dicha ocupación y apropiación, también se utilizan los datos del suplantado para actuar en su nombre.

Es imprescindible llevar a cabo esta diferenciación ya que en función de los hechos que tengan lugar, se incurrirá en una suplantación o usurpación de identidad; dos conductas subsumibles en diferentes tipos penales.

En el caso de suplantación de identidad, se debe tener en cuenta que no solo aplica en la acción o conducta de hacerse pasar por otro, sino que se apropie de los derechos y obligaciones del usurpado, apropiándose de sus datos y características que integran la identidad de la persona suplantada. (Carrillo, 2016)

En el caso de las redes sociales, se estaría cometiendo un delito de usurpación de identidad cuando el suplantador actuase como si fuese el

verdadero titular de la cuenta. Un ejemplo de ello, sería cuando el suplantador subiese fotografías o escribiese comentarios a otros perfiles actuando desde el perfil del suplantado y como si del mismo se tratase.

Es imprescindible llevar a cabo un análisis exhaustivo de la conducta del suplantador y llevar a cabo una correcta distinción entre la suplantación y usurpación de identidad, puesto que en función de que, si se trata de suplantación o usurpación de identidad, será delito o no.

En el caso de que estemos ante la comisión de un delito, según se trate del primer o el segundo tipo penal, estaremos ante un delito y, ante ellos, se establecerán las diferentes sanciones. El Delito de usurpación de identidad para la comisión de delitos contra los propios sistemas informáticos, se encuadra en el delito de daños y sabotaje informático del y el delito de descubrimiento y revelación de secretos del artículo, así como el Hacking.

Delito de usurpación de identidad en internet como medio para la comisión de otros delitos que atentan contra el patrimonio y el honor de las personas. Todo tipo de cibercrimen servido como instrumento para la comisión de otro tipo penal, podría ser el delito de estafa informática regulada en el Código Penal, delitos contra la propiedad industrial e intelectual. El delito la supresión o alteración de medidas de seguridad tecnológicas para proteger programas de software o ejecución de los mismos, sin autorización de los titulares de los derechos de propiedad intelectual.

1.5. Delitos informáticos según el COIP

Los delitos informáticos en Ecuador crecen de forma desmesurada y los más recurrentes son las estafas digitales con modalidades como suplantación de la identidad y la apropiación fraudulenta que se da por medios electrónicos. En el Código Orgánico Integral Penal se establecen sanciones por los tipos de delitos informáticos con penas de privación de libertad. (Salgado M. S., 2020)

Todas las actividades que contemplen grabaciones o fotografías sin consentimiento o autorización legal, entre otros actos, como intervención o violación en la intimidad de las personas, suplantación de claves, daños o pérdidas de información. (Torres, 2015)

Unos de los delitos tipificados es la revelación ilegal de base de datos, el cual establece que,

“la persona que, en provecho propio o de un tercero, revele información registrada, contenida en ficheros, archivos, bases de datos o medios semejantes, a través o dirigidas a un sistema electrónico, informático, telemático o de telecomunicaciones; materializando voluntaria e intencionalmente la violación del secreto, la intimidad y la privacidad de las personas, aquel acto será sancionado con pena privativa de libertad de uno a tres años.” (pág. 34) (Asamblea Nacional, 2018)

Además, establece que, si la revelación ilegal de base de datos se comete por una o un servidor público, empleadas o empleados bancarios internos o de instituciones de la economía popular y solidaria, será sancionada con pena privativa de libertad de tres a cinco años.

Otro delito es la interceptación ilegal de datos, la cual se sanciona con pena privativa de libertad de tres a cinco años, si se cumplen las siguientes condiciones:

“1. La persona que, sin orden judicial previa, en provecho propio o de un tercero, intercepte, escuche, desvíe, grabe u observe, en cualquier forma un dato informático en su origen, destino o en el interior de un sistema informático, una señal o una transmisión de datos o señales con la finalidad de obtener información registrada o disponible.

2. La persona que diseñe, desarrolle, venda, ejecute, programe o envíe mensajes, certificados de seguridad o

páginas electrónicas, enlaces o ventanas emergentes o modifique el sistema de resolución de nombres de dominio de un servicio financiero o pago electrónico u otro sitio personal o de confianza, de tal manera que induzca a una persona a ingresar a una dirección o sitio de internet diferente a la que quiere acceder.

3. La persona que a través de cualquier medio copie, clone o comercialice información contenida en las bandas magnéticas, chips u otro dispositivo electrónico que esté soportada en las tarjetas de crédito, débito, pago o similares.

4. La persona que produzca, fabrique, distribuya, posea o facilite materiales, dispositivos electrónicos o sistemas informáticos destinados a la comisión del delito descrito en el inciso anterior.” (pág. 34) (Asamblea Nacional, 2018)

La transferencia electrónica de activo patrimonial, es otro delito informático que establece que:

“La persona que, con ánimo de lucro, altere, manipule o modifique el funcionamiento de programa o sistema informático o telemático o mensaje de datos, para procurarse la transferencia o apropiación no consentida de un activo patrimonial de otra persona en perjuicio de esta o de un tercero, será sancionada con pena privativa de libertad de tres a cinco años.” (pág. 35)

Posteriormente, indica que, serán sancionadas con igual pena la persona que facilite o proporcione datos de su cuenta bancaria con la intención de obtener, recibir o captar de forma ilegítima un activo patrimonial a través de una transferencia electrónica producto de este delito para sí mismo o para otra persona.

Por otro lado, establece como delito al ataque a la integridad de sistemas informáticos, el cual indica que:

“La persona que destruya, dañe, borre, deteriore, altere, suspenda, trabe, cause mal funcionamiento, comportamiento no deseado o suprima datos informáticos, mensajes de correo electrónico, de sistemas de tratamiento de información, telemático o de telecomunicaciones a todo o partes de sus componentes lógicos que lo rigen, será sancionada con pena privativa de libertad de tres a cinco años.” (Pág. 35) (Asamblea Nacional, 2018)

Con igual pena, sancionará a las personas que ejecute las siguientes acciones:

“1. Diseñe, desarrolle, programe, adquiera, envíe, introduzca, ejecute, venda o distribuya de cualquier manera, dispositivos o programas informáticos maliciosos o programas destinados a causar los efectos señalados en el primer inciso de este artículo.

2. Destruya o altere sin la autorización de su titular, la infraestructura tecnológica necesaria para la transmisión, recepción o procesamiento de información en general.” (pág. 35) (Asamblea Nacional, 2018)

Sin embargo, se establece una pena superior que oscile entre 5 a 7 años de privación de libertad, si la infracción se comete sobre bienes informáticos destinados a la prestación de un servicio público o vinculado con la seguridad ciudadana.

El Delito contra la información pública reservada legalmente es un delito que consiste en:

“La persona que destruya o inutilice información clasificada de conformidad con la Ley, será sancionada con pena privativa de libertad de cinco a siete años.

La o el servidor público que, utilizando cualquier medio electrónico o informático, obtenga este tipo de información,

será sancionado con pena privativa de libertad de tres a cinco años.

Cuando se trate de información reservada, cuya revelación pueda comprometer gravemente la seguridad del Estado, la o el servidor público encargado de la custodia o utilización legítima de la información que sin la autorización correspondiente revele dicha información, será sancionado con pena privativa de libertad de siete a diez años y la inhabilitación para ejercer un cargo o función pública por seis meses, siempre que no se configure otra infracción de mayor gravedad.” (pág. 35) (Asamblea Nacional, 2018)

Por otro lado, se encuentra el acceso no consentido a un sistema informático, telemático o de telecomunicaciones, el cual establece que:

“la persona que sin autorización acceda en todo o en parte a un sistema informático o sistema telemático o de telecomunicaciones o se mantenga dentro del mismo en contra de la voluntad de quien tenga el legítimo derecho, para explotar ilegítimamente el acceso logrado, modificar un portal web, desviar o redireccionar de tráfico de datos o voz u ofrecer servicios que estos sistemas proveen a terceros, sin pagarlos a los proveedores de servicios legítimos, será sancionada con la pena privativa de la libertad de tres a cinco años.” (pág. 35) (Asamblea Nacional, 2018)

1.6. Delitos de suplantación de identidad según el COIP

La supresión, alteración o suposición de la identidad y estado civil, es un delito de la identidad, el cual establece que:

“La persona que ilegalmente impida, altere, añada o suprima la inscripción de los datos de identidad suyos o de otra persona en programas informáticos, partidas, tarjetas índices, cédulas o en cualquier otro documento emitido por la

Dirección General de Registro Civil, Identificación y de Cedulación o sus dependencias o, inscriba como propia, en la Dirección General de Registro Civil, Identificación y de Cedulación a una persona que no es su hijo, será sancionada con pena privativa de libertad de uno a tres años.

La persona que ilegalmente altere la identidad de una niña o niño; la sustituya por otra; entregue o consigne datos falsos o supuestos sobre un nacimiento; usurpe la legítima paternidad o maternidad de niña o niño o declare falsamente el fallecimiento de un recién nacido, será sancionada con pena privativa de libertad de tres a cinco años. (pág. 35) (Asamblea Nacional, 2018)

Finalmente, la normativa penal ecuatoriana tipifica el delito de suplantación de identidad, estableciendo que:

“La persona que de cualquier forma suplante la identidad de otra para obtener un beneficio para sí o para un tercero, en perjuicio de una persona, será sancionada con pena privativa de libertad de uno a tres años.” (pág. 35) (Asamblea Nacional, 2018)

La suplantación de identidad es aquella acción por la que una persona se hace pasar por otra para llevar a cabo actividades de carácter ilegal, como pueden ser pedir un crédito o préstamo hipotecario, contratar nuevas líneas telefónicas o realizar ataques contra terceras personas. (Torres, 2015)

Existen varias formas de suplantar la identidad de una persona. Resulta de gran utilidad para esclarecer los hechos que se buscan demostrar la inocencia de las partes implicadas. Se produce cuando se apropian indebidamente de otra identidad digital y la usa para conseguir información personal, para publicar y desprestigiar, extorsionar o chantajear.

1.7. Derecho comparado

1.7.1. Argentina

Se estableció como sanción en el Código Penal la conducta delictiva, para tipificar el delito de suplantación de identidad digital, conocido comúnmente como, robo de identidad, el cual ocurre cuando una parte adquiere, transfiere, posee o utiliza información personal de una persona física o jurídica de forma no autorizada, con la única intención de causar fraude u otro delito relacionado. (Antolisei, 2005)

Sin embargo, se mantiene en un proyecto de ley para que sea aprobado y se amplió la regulación jurídica de la suplantación de identidad digital. En virtud del aumento exuberante de las bases de datos ilegales con información privada de las personas, ha ocasionado que los delincuentes accedan con facilidad a los detalles de la información, que son materia prima para facilitar la usurpación de una identidad, con la cual el autor encontrará el camino para realizar diversas conductas maliciosas. (Natalia Soledad Villa, 2020)

La víctima en este tipo de delitos, se trata de personas naturales y jurídicas, por los cuales los delincuentes se hacen pasar como empleados de empresas, bancos o financieras, con la finalidad de extraer datos de terceras personas, y de la mano con otras técnicas de captación ilegítima de datos confidenciales.

El derecho a la identidad es considerado como un derecho humano fundamental y, por ende, se ha consagrado en diversos tratados internacionales. En Argentina, se registran al menos 180 al mes, los cuales consisten en ataques de Facebook que terminan en justicia criminal o correccional, por denuncias penales y civiles que llevan adelante los afectados. (Centro de Estudios en Libertad de Expresión y Acceso a la Información, 2018)

Se consuma el delito simplemente con la suplantación o apoderamiento de identidad ajena, y, en consecuencia, se actúa causando

un perjuicio a la misma o a terceros. Entendemos que, no es un requisito necesario demostrar que la suplantación o apoderamiento de identidad se realiza con los fines de cometer otro delito, sino que, en la tipificación se da a conocer utilizando para tal fin las Tecnologías de la Información y la Comunicación.

1.7.2. Colombia

La conducta delictiva de la suplantación de identidad, que es realizado por el ataque informático, de ingeniería social que tiene por finalidad la adquisición de información confidencial de la víctima mediante el uso de ardid o engaño, pudiendo provocar perjuicios patrimoniales, como es la afectación del derecho de propiedad y también, regulado en la normativa de derecho penal colombiano, en el cual se establece que la protección de la información y de los datos del sistema informático busca capturar una figura específica que proteja los datos personales. (Cabrera, 1999)

El objeto ilícito de esta conducta está facultado a diseñar, desarrollar, traficar, vender, ejecutar, programar, o enviar páginas electrónicas, enlaces o ventanas emergentes que incurra en pena de prisión y multa económica como una sanción por una infracción lenta.

Adicionalmente, se ha configurado el sistema de resolución de dominio, que permite al usuario de una IP que acceda a instituciones como banco u otro sitio personal o de confianza, siempre que la conducta no constituye con una pena más grave.

La suplantación ha obligado a tomar acciones legislativas que permitan establecer una serie de conductas típicas, antijurídicas y sancionadas en las legislaciones sustantivas penales; mediante instrumentos jurídico-penales, otorgando seguridad jurídica a los ciudadanos. (Calderón, 2010)

Esta figura tiene una serie de agravantes en la pena antes mencionada, si se incurre en ciertas circunstancias tales como: si la conducta se ejecuta

sobre redes o sistemas informáticos o de comunicaciones estatales u oficiales o del sector financiero, nacionales o extranjeros; en el caso de servidores públicos en el ejercicio de sus funciones; si se aprovecha de la confianza que fue depositada en el poseedor de la información o quien tiene un vínculo contractual.

La modalidad de suplantación de identidad de la persona, se regula en un tipo específico de delitos informáticos que atenta contra la información personal que se encuentra en el cuidado y custodia de los datos personales.

1.7.3. España

El ordenamiento jurídico español respecto al tratamiento jurídico de los delitos informáticos, se mantiene con dos perspectivas. El primero es que entre los juristas se discute la existencia jurídica de los delitos informáticos, para estos eventos que ocurren mediante medios tecnológicos. Por otro lado, a diferencia de los delitos tradicionales, los informáticos no tienen un tratamiento diferenciado por una regulación diferente. (Soler, 1929)

El legislador español no cuenta con una regulación autónoma de modo que, no tiene una sesión de delitos informáticos que se encuentre como parte de los delitos tradicionales. El phishing está dentro del cuerpo normativo, pero de una forma genérica porque se lo considera en el grupo de defraudación o estafa, un delito de naturaleza económica que afecta el patrimonio de las personas.

Lo consideran un grupo tan habitual, puesto que engloba varias conductas delictivas, como técnica de ingeniería social avanzada con sistemas de información con un grado de tentativa o programas maliciosos que constituyen este tipo de delitos. (Pozo, 2005)

Por ende, en España no se cuenta con una normativa que regule de manera específica y determina los delitos informáticos y sea protegidos los derechos vulnerados por las personas en un código penal y de esta forma

se garantice y proteja a las víctimas de aquellos abusos informáticos que son sometidas.

Todo ello, porque no consideran a la suplantación de identidad digital un delito de carácter permanente puesto que el uso fraudulento de un sitio web o un perfil en redes sociales no persigue la apropiación permanente sino un mal uso puntual.

Para que se sancione estas acciones, se debe probar que se han incumplido los delitos de: acceso no autorizado a equipos y programas informáticos, suplantación de estado civil, injurias, calumnias, amenazas, etc., delitos todos ellos recogidos en el Código Penal. (Zabaleezequi, 2002)

En el caso de que sólo se hubiera producido uno de los delitos arriba mencionados, la suplantación tendrá la consideración de delito leve y por lo tanto será complicado probar y sancionar el delito. Los ciudadanos no disponen aún de la seguridad jurídica necesaria para protegerse en el mundo digital, dado que ni el delito está contemplado en la Ley.

Capítulo II: Marco Metodológico

Para el presente proyecto de investigación científica se empleó en primer lugar el enfoque cualitativo, además de los métodos de recolección de datos tales como el documental, comparativo y una entrevista a expertos, los cuales se desarrollan a continuación:

1.1. Enfoque de la investigación

En cuanto al enfoque de esta investigación se implementó el enfoque cualitativo, debido a que no se tiene data respecto del tema, además este enfoque se basa en el estudio de las principales características de determinado fenómeno social.

1.2. Tipo de investigación

Respecto del tipo de investigación se empleó la investigación jurídica debido a que este proyecto es netamente basado en el análisis del derecho como un fenómeno social de las especificaciones que componen el delito electrónico de suplantación de identidad.

Además, esta investigación es de tipo descriptiva toda vez que lo que se buscó fue analizar las características y la naturaleza jurídica del delito informático de suplantación de identidad y su posible implementación en el Ecuador.

1.3. Métodos de investigación

Método documental

En este proyecto se ha implementado el método documental, ya que esta es una investigación jurídica y se ha podido revisar información de doctrina tanto en medios físicos como libros y digitales como la web.

Método comparado

El método comparado se implementó en esta investigación para realizar un análisis sucinto en derecho comparado respecto de los delitos electrónicos de suplantación de identidad en países como Argentina, Colombia y España.

Método empírico

Se utilizó el método empírico para recolectar datos de un grupo de expertos mediante una entrevista con un cuestionario de preguntas respecto de los delitos electrónicos de suplantación de datos.

1.4. Universo y muestra

Debido a que esta es una investigación de corte jurídico y netamente documental, además no existen mayores estudios estadísticos respecto al tema y lo que al autor busca es tener una opinión experta de personas que tengan experiencia en lo relacionado a delitos informáticos de suplantación de identidad, en tal sentido para el universo y muestra se implementaron entrevistas a grupos de expertos los cuales brindaron su opinión a este proyecto con la finalidad de buscar una solución al tema planteado.

Los expertos consultados para esta investigación fueron:

- Abogado Ricardo Xavier Vanegas Cortázar.
- Abogado David Vergara Solís.
- Abogada Adela Liseth Alcivar Holguin.

Capítulo III: Análisis de resultados

En este capítulo se va a realizar el análisis de las entrevistas al grupo de expertos con la finalidad de obtener directrices de los abogados.

2.1. Entrevistas a expertos

Experto 1: Abogado Ricardo Xavier Vanegas Cortázar

Preguntas:

1. ¿Cuál es su opinión acerca del delito informático de suplantación de identidad?

En mi opinión el delito informático de suplantación de identidad no creo que esté tipificado en el Código Orgánico Integral Penal como tal, lo cual sin duda alguna debe ser implementado.

2. ¿De acuerdo a su criterio cuál es la diferencia entre suplantación y usurpación de identidad?

La suplantación es cuando una persona se quiere hacer pasar por otra y si se hace a través de medios telemáticos es cuando accede a sus redes sociales, cuentas bancarias y otras con la finalidad de apropiarse de valores y de publicar en las redes información que no pertenece al titular.

La usurpación es cuando una persona se apropia de la identidad de otra persona e incluso llega a adquirir obligaciones de la persona usurpada.

3. ¿Cree Ud. que la normativa ecuatoriana tiene procedimientos adecuados para detectar los posibles delitos informáticos de suplantación de identidad?

La suplantación digital de identidad es muy común en el internet, y no creo que tenga un procedimiento adecuado.

4. ¿De acuerdo al Código Orgánico Integral Penal en su artículo 212, cree Ud. que las penas para el delito de suplantación de identidad son idóneas?

Creo que las penas no son idóneas, creería que se necesita un ajuste, ya que suplantar la identidad es tan común en nuestros días, cualquiera puede falsificar una firma.

5. ¿Cree Ud. que es necesario implementar penas más rigurosas para sancionar el cometimiento de los delitos de suplantación de identidad?

Si creería que es necesario ajustar las penas.

6. ¿Cuál sería su recomendación para evitar que se cometan los delitos informáticos de suplantación de identidad en el Ecuador?

Creo que se deberían ajustar medidas de seguridad en los medios informáticos, al momento de solicitar datos personales.

Experto 2: Abogado David Vergara Solís

Preguntas:

1. ¿Cuál es su opinión acerca del delito informático de suplantación de identidad?

Opino según lo que dice el artículo 212 del Código Orgánico Integral Penal que el delito básicamente consiste en su modalidad informática en apropiarse de la identidad de otra persona, para que pueda ser catalogado como un delito informático esta suplantación de identidad esta conducta tiene que realizarse a través de medios electrónicos ya sea suplantar identidad de una red social, de un correo electrónico, de un perfil, en eso consiste básicamente, es un delito que hoy en día tiene mayor importancia por el hecho de que muchas de las estafas ya sea por phishing o pharming se realizan a través de esta modalidad delictual.

2. ¿De acuerdo a su criterio cuál es la diferencia entre suplantación y usurpación de identidad?

Es una diferencia doctrinaria, menos aquí en el Ecuador ya que sólo tenemos el artículo 212 que habla de suplantación de identidad en el Código Orgánico Integral Penal, la suplantación sería el mero acto de apropiarse de un perfil mientras que la usurpación sería apropiarse pero además realizar algún tipo de acto que perjudique ya sea que se apropie

económicamente de una clave para poder hacerse una transferencia o sacarle provecho a esa apropiación.

Entonces la suplantación es un acto por así decirlo inicial y la usurpación ya bien cuando se utiliza el perfil para comunicarse con otras personas, para comunicarse con el banco, para realizar algún tipo de acto secundario que perjudique aún más a la víctima de este delito, de allí en el Código Orgánico Integral Penal no existen otras diferencias, solo está tipificado el delito de suplantación de identidad pero más bien debería ser categorizado como usurpación si nos acogemos a esta diferencia doctrinaria.

3. ¿Cree Ud. que la normativa ecuatoriana tiene procedimientos adecuados para detectar los posibles delitos informáticos de suplantación de identidad?

La suplantación digital de identidad es muy común en el internet, y no creo que tenga un procedimiento adecuado.

4. ¿De acuerdo al Código Orgánico Integral Penal en su artículo 212, cree Ud. que las penas para el delito de suplantación de identidad son idóneas?

Considero que el problema no radica específicamente en la normativa, sino en la falta de criterios en la seguridad informática de los usuarios y consumidores, entonces por más que la ley le otorgue al fiscal facultades investigativas en concordancia con la policía judicial, eso va a hacer bastante difícil llevarlo a la práctica, porque los delitos informáticos son de difícil detección porque las pruebas son fácilmente borrables y dificultades de poder establecer la autoría, el problema es en la parte de la seguridad informática.

5. ¿Cree Ud. que es necesario implementar penas más rigurosas para sancionar el cometimiento de los delitos de suplantación de identidad?

Insisto en que el problema del derecho penal informático no está relacionado del todo con las penas ni con los tipos penales, el problema

con los delitos informáticos radica que por su naturaleza son de difícil detección y juzgamiento, claro está que uno de los efectos del endurecimiento de las penas es la prevención general, es decir que todas las personas al saber que es un delito con una pena grave no están tan tentados a delinquir, yo considero que si se realiza un acto perjudicial es posible que la pena de uno a tres años para este tipo de delitos deba aumentarse.

6. ¿Cuál sería su recomendación para evitar que se cometan los delitos informáticos de suplantación de identidad en el Ecuador?

La recomendación en primer lugar es no poner tantos datos en el internet, no dejar huellas ni registros en páginas que no sean confiable, manejar fotografías comentarios o videos de manera mínima y para un círculo reducido de usuarios, también se debe cambiar de claves cada tres o seis meses, se debe tratar de no utilizar tanto estas herramientas así sea por ocio.

Además, habría que estudiar la posibilidad de aumentar las penas actuales que se encuentran estipuladas en el artículo 212 del Código Orgánico Integral Penal.

Experto 3: Abogada Adela Liseth Alcivar Holguin

Preguntas:

1. ¿Cuál es su opinión acerca del delito informático de suplantación de identidad?

Este tipo de delito ha venido aumentando dentro de nuestro país, y cada vez están aumentando los casos de personas que son víctimas de este tipo de práctica irregular usada para cometer ilícitos por medio del mundo digital y redes sociales, usando este tipo de mecanismo con intención clara de beneficiarse o algún tercero de algo que le pertenece a otra persona o producir algún tipo de daño.

2. ¿De acuerdo a su criterio cuál es la diferencia entre suplantación y usurpación de identidad?

La diferencia es que la suplantación de identidad es cuando una persona se hace pasar por otra buscando un fin que es la obtención de un beneficio generando un fraude u ocasione algún tipo de daño, en cambio la usurpación de identidad es cuando una persona se apropia de todas las cualidades de una persona (nombre, estado civil, profesión, nacionalidad, etc.) simulando ser esa persona en diferentes actos jurídicos.

3. ¿Cree Ud. que la normativa ecuatoriana tiene procedimientos adecuados para detectar los posibles delitos informáticos de suplantación de identidad?

Dentro de la normativa ecuatoriana existen procedimientos escasos para tratar estos tipos de delitos, y es muy complejo efectuar mecanismo que permitan sancionar estos tipos de delitos.

4. ¿De acuerdo al Código Orgánico Integral Penal en su artículo 212, cree Ud. que las penas para el delito de suplantación de identidad son idóneas?

Por tratarse de delitos contra la identidad de las personas, considero que sí debería ser más inflexibles las sanciones para estos tipos de delitos.

5. ¿Cree Ud. que es necesario implementar penas más rigurosas para sancionar el cometimiento de los delitos de suplantación de identidad?

Es necesario incrementar las sanciones dentro de estos tipos de delitos, considerándose los agravantes que pudieran desarrollarse dentro del tipo penal.

6. ¿Cuál sería su recomendación para evitar que se cometan los delitos informáticos de suplantación de identidad en el Ecuador?

En esta era digital que estamos viviendo actualmente, la mayoría de actividades las realizamos por medio de las plataformas digitales, redes

sociales y de telecomunicaciones, así mismo como consecuencia tenemos que han surgidos los nombrados “delincuentes cibernéticos”.

Por tal motivo unas de las recomendaciones necesarias para evitar estos tipos de delitos es incrementar políticas públicas de educación y prevención para reducir los riesgos y casos que puedan afectar la reputación de las personas y así mismo provocar pérdidas económicas, además es necesario una propuesta de reforma de ley al Código Orgánico Integral Penal y crear un nuevo tipo penal de especialidad que abarque el delito informático de suplantación de identidad y con penas considerables.

2.2. Análisis global de entrevistas

Ahora bien, respecto del delito de delito informático de suplantación de identidad los expertos indican que es una situación que ha venido aumentando en los últimos años, más sin embargo el abogado Vanegas indica que este delito “informático de suplantación de identidad” no se encuentra tipificado como tal, sino más bien existe el artículo 212 de suplantación de identidad.

Se indica también que existe una diferenciación entre suplantación y usurpación de identidad desde el punto de vista doctrinario, siendo la suplantación es el acto de sustraer la identidad y la usurpación es sacar provecho de este acto ilícito.

En cuanto a la revisión de penas del artículo 212 del Código Orgánica Integral Penal existen posturas similares, por una parte se indica que en efecto sería necesario una reforma para aumentar los años de penas por este tipo de delitos y de esta manera también ampliar el poder punitivo del estado pero también el experto abogado Vergara indica que si bien es cierto se pueden aumentar las penas para evitar que se cometan estos actos delictivos, indica que otra arista del problema radica en que los usuarios no toman las precauciones del caso para evitar ser posibles

víctimas de estos actos delictivos, y que los delitos informáticos son muy complejos de detectar y que la autoridad competente los pueda proceder a juzgar.

Finalmente, los expertos indican que es posible realizar una reforma al Código Organico Integral Penal para aumentar las penas por el delito de suplantación de identidad o crear un tipo penal especial para este acto ilícito específico, además es necesario implementar políticas públicas en relación a la educación de la ciudadanía y prevención para mitigar riesgos que afecten la reputación de las personas y puedan provocar pérdidas económicas.

Capítulo IV: Propuesta

4.1. Justificación de la propuesta

Mi propuesta de reforma de ley va encaminada a prevenir y contener los actos delictivos de suplantación de datos de manera digital, ya que no existe en el Código Orgánico Integral Penal el delito informático de suplantación de identidad.

La propuesta gira en torno a adicionar a continuación del artículo 212 del Código Orgánico Integral Penal el siguiente artículo el cual contiene el delito informático de suplantación de identidad:

“Art...- Delito informático de suplantación de identidad.- La persona que mediante medios digitales o informáticos suplante la identidad de otra para obtener un beneficio para sí o para un tercero, en perjuicio de una persona, será sancionada con pena privativa de libertad de uno a tres años..”

Conclusiones

- Finalmente se pudo analizar lo que respecta a los delitos de suplantación de identidad en Ecuador, lo cual es un acto delictivo que con las nuevas tecnologías, también se lo realiza en el campo informático o digital, es por esto que se debe prevenir y normar este tipo de acto delictivo para evitar que se vulneren derechos constitucionales como el derecho a la intimidad personal y familiar, el derecho a la propiedad, el derecho a la identidad personal.
- En lo que respecta a la revisión teórica del presente proyecto se pudo evidenciar que el Código Orgánico Integral Penal establece en su artículo 212 el delito de suplantación de identidad, más sin embargo no existe una directriz específica, sólo se ha tipificado este delito de manera general.
- Respecto de las entrevistas realizadas a los expertos se pudo evidenciar su consenso en lo que respecta a una reforma de ley al Código Orgánico Integral Penal en donde se adicione el delito informático de suplantación de identidad. Cabe destacar que el Mgs. David Vergara hizo mucho énfasis en que también se debe trabajar en la prevención de estos delitos tomando medidas de seguridad adecuadas tales como implementar contraseñas difíciles de rastrear, cambiar contraseñas periódicamente, limitar las publicaciones en redes sociales.

- Finalmente, de la revisión teórica implementada en esta investigación, y del análisis de las entrevistas al grupo de expertos, se ha podido evidenciar que es necesaria la inserción de un tipo penal específico para el delito informático de suplantación de identidad, lo cual se implementó en este mentado proyecto jurídico.

Recomendaciones

- La primera recomendación va dirigida al gobierno central para que realice campañas de concientización de las posibles consecuencias de no tomar precauciones de seguridad al momento de hacer uso de medios tecnológicos.
- La segunda recomendación va dirigida a la Universidad Ecotec para que se implementen estudios respecto del delito informático de suplantación de identidad, ya que al momento este delito no se encuentra tipificado en el Código Orgánico Integral Penal, y así desde la academia se realice un aporte científico al presente tema de estudios.
- La tercera recomendación se relaciona con las precauciones que deben tener todas las personas que usan habitualmente medios tecnológicos para realizar sus transacciones bancarias, o para ocio, o para el fin que fuere, es necesario cambiar las contraseñas periódicamente y utilizar contraseñas fuertes.
- La cuarta recomendación se dirige a la Asamblea Nacional para que se realice un estudio acerca de los actos de suplantación de identidad por medios informáticos y que se realicen las reformas de ley pertinentes.

BIBLIOGRAFÍA

- Altamirano, S. (2017). *Manuel Jurídico Informático. Universidad Regional Autónoma de los Andes.*
- Alvarez, J. L. (2015). *Delitos Informáticos. Editorial Temis S.A.*
- Antolisei, F. (2005). *Manual de Derecho Penal: Parte General.* Argentina: Ediar.
- Arrieta, H. V. (2016). El análisis gramatical del tipo penal. *Revista de Derecho*, 24.
- Asamblea Nacional. (2018). *Código Organico Integral Penal.* Quito: Corporación de Estudios y Publicaciones .
- Bacigalupo, E. (1996). *Manual de derecho penal.* Bogotá: Temis.
- Ballesteros, L. A. (2006). *La privacidad electrónica-internet en el centro de protección.* Valencia: Tirant Lo Blanch.
- Barrera, S. (2017). *Claves de la Investigación en Redes Sociales, (2da Ed.)* . España: Círculo Rojo.
- Cabrera, R. P. (1999). *Tratado de derecho penal. Parte general 3ra edición.* Lima: Grijley.
- Calderón, L. A. (2010). *Delitos Informáticos y derecho penal.* México: Ubijus.
- Carrillo, M. (2016). *Sociedad de la informática y los derechos fundamentales.* Editorial La Roca.
- Castillo, R. B. (2018). Teoría del delito, evolución, elementos integrantes. *Revista de derecho.*
- Castro, J. G. (2008). *Programa de formación inicial de la defensa pública.*
- Centro de Estudios en Libertad de Expresión y Acceso a la Información. (2018). Obtenido de <https://observatoriolegislativocele.com/argentina-proyecto-de-ley-suplantacion-de-la-identidad-digital-2722-18-2018/>
- Davara, M. (2001). *Manual de Derecho Informático (4ta ed).* Madrid: Arazandi S.A.
- García, A. D. (2015). *Derecho Informático, elementos de informática jurídica.* Editorial Leyer.
- Gomez, E. A. (2011). *Manual de derecho penal ecuatoriano Parte Especial.* Quito: Ediciones Legales.

- Jakobs, G. (1996). *Sociedad, norma y persona en una teoría de un derecho penal funcional*. Madrid: Civitas.
- Lascano, J. C. (2002). *Manual de Derecho Penal*. Córdoba: Advocatus.
- Maurizio, T. (2012). *Suplantación de identidad digital como delito informático en Argentina*. Argentina: Trotta.
- Maynez, E. G. (2009). *Introducción al estudio del Derecho*. México: Editorial Porrúa .
- Molina, A. G. (1994). *Introducción de Derecho Penal*. España.
- Natalia Soledad Villa. (2020). Obtenido de <https://www.diputados.gov.ar/proyectos/proyecto.jsp?exp=0121-D-2020#:~:text=Art%C3%ADculo%20139%20ter%3A%20Ser%C3%A1%20reprimido,como%20tal%2C%20utilizando%20para%20tal>
- Palazzi, P. (2016). *Delitos Informáticos*. Buenos Aires : Abeledo Perrot .
- Pineda, B. M. (1996). *Filosofía del derecho*. Bogotá: Temis.
- Pino, S. A. (2015). *Delitos Informáticos: Generalidades*. Editorial Astrea.
- Pino, S. A. (2016). Delitos Informáticos. *Revista del PUCE*.
- Pozo, J. H. (2005). *Manual de derecho penal*. Lima: Grijley.
- Puig, S. M. (2002). *Derecho Penal. Parte General 6ta edición*. Barcelona.
- Ramirez, J. B. (1989). *Manual de derecho penal*. Barcelona: Ariel.
- Rosal, M. C. (1999). *Derecho Penal*. Valencia.
- Roxin, C. (1997). *Derecho Penal. Parte General*. España, Madrid: Civitas Ediciones.
- Salgado, J. A. (2003). *Delitos y otros ilícitos informáticos* . México: Editorial Porrúa.
- Salgado, M. S. (2020). *Análisis Conceptual del delito informático en Ecuador*. Ecuador: Universidad Regional Autónoma de los Andes.
- Sanchez, J. S. (2001). *La expansión del derecho penal*. Madrid: Civitas.
- Soler, S. (1929). *Teoría del delito*. Buenos Aires: Valerio.
- Somellera, R. (2010). Delitos Informáticos. *Revista Instituto Tecnológico de Estudios Superiores de Monterrey*.
- Suarez, R. B. (2000). *Manual de derecho penal*. Lima: Santa Rosa.
- Torre, I. B. (1993). *El contenido del tipo penal*. Lima: Cuzco.

- Torres, V. A. (2015). *Manual de Derecho Penal*. Lima: Editorial San Marcos.
- Valdez, J. T. (2004). *Derecho Informatico*. México: Editorial McGraw-Hill.
- Vallejo, V. (2010). *El Delito Informático en la Legislación Ecuatoriana*. Corporación de Estudios y Publicaciones .
- Vasquez, M. A. (2005). *Derecho Penal Económico*. Chile.
- Vitoria, G. (2008). *El tipo basico de aborto*. Pamplona: Editorial Bellavista.
- Zabaleezequiél, M. (2002). *Derechos Informaticos*. Buenos Aires: Juris.
- Zaffaroni, E. R. (2002). *Derecho Penal - Parte General*. Buenos Aires: Ediar.
- Zaffaroni, R. E. (1986). *Manual de Derecho Penal*. México: Cádernas.
- Zapater, E. B. (1986). *Lineamientos de la teoría del delito*. Buenos Aires.

Anexos

Anexo 1 Formato de entrevista a expertos



Facultad de Derecho y Gobernabilidad

Tema: Análisis del delito informático de suplantación de identidad, relacionado a los derechos constitucionales del Ecuador, período 2020-2021.”

Entrevista a experto

Preguntas:

- 1. ¿Cuál es su opinión acerca del delito informático de suplantación de identidad?**
- 2. ¿De acuerdo a su criterio cuál es la diferencia entre suplantación y usurpación de identidad?**
- 3. ¿Cree Ud. que la normativa ecuatoriana tiene procedimientos adecuados para detectar los posibles delitos informáticos de suplantación de identidad?**
- 4. ¿De acuerdo al Código Orgánico Integral Penal en su artículo 212, cree Ud. que las penas para el delito de suplantación de identidad son idóneas?**

5. **¿Cree Ud. que es necesario implementar penas más rigurosas para sancionar el cometimiento de los delitos de suplantación de identidad?**

6. **¿Cuál sería su recomendación para evitar que se cometan los delitos informáticos de suplantación de identidad en el Ecuador?**