



Universidad Tecnológica Ecotec
Facultad de Derecho y Gobernabilidad

Título del trabajo:

Estudio de la apropiación de datos a través de medios electrónicos para tutelar los derechos de los usuarios de banca virtual, en Guayaquil año 2022.

Línea de investigación:

Gestión de las relaciones jurídicas

Modalidad de titulación:

Proyecto de investigación

Carrera:

Derecho con énfasis en derechos humanos y ciencias penales

Título a obtener:

Abogado de los Tribunales de la República del Ecuador

Autor:

Gary Marlon Soria Contreras

Tutor:

Abg. Fabián Orellana Batallas

Guayaquil-Ecuador

2023

Dedicatoria

Se lo dedico a Dios por que el ha sido mi fortaleza y quien me ha guiado a través de su palabra, teniendo consejos para que me pueda levantar en los momentos más duros, luego a mi madre que estuvo conmigo en mi proceso de formación profesional, que dedico arduos esfuerzos para que pueda prepararme en este camino tan importante, inculcándome valores importantes para mis prácticas y desempeños académicos en cada adversidad que me encontraba atravesando. A mi Tío Silvio Devoto Passano , que gracias a su rol de padre que fue importante en mi vida, el que me impulso a continuar luchando hasta el final y fue mi sustento día a día, en poder continuar siempre enamorado de que ahora será mi profesión. A mi tía Janneth Contreras, que ha sido una segunda madre, estando también pendiente de mi en que pueda continuar hacia el éxito con sus consejos y admirables atenciones para que el camino pueda continuar con mucha seguridad. A mi hermano Ricardo en el que estuvo siempre guiándome en esta profesión e impartíendome sus conocimientos y el amor a la profesión; sabiendo que con honestidad y transparencia se puede honrar cada parte de las ciencias jurídicas con impecable devoción, dándome a conocer un mundo nuevo que es la jurisprudencia, siendo un sustento importante en mi vida. Y quiero agradecer también mucho a mi Padre que en paz descansa que siempre creyó en mi y que estuvo aconsejándome para que pueda ser un hombre de bien, para que siga sus pasos y pueda alcanzar muchos éxitos más como fue el en vida, que sabiendo que, aunque no este físicamente, su espíritu fue impartido en mi para que siga adelante y buscando superar los desafíos que se me presente en este grandioso camino que es la vida. También dedico este logro a mi mejor amigo y compañero de batallas, en las que estuvo en mi vida para aconsejarme y disciplinarme como buen amigo a Eduardo Rendon, que siempre estuvo conmigo presto a escuchar y dar su milla extra para que pueda ser un hombre de bien, dándome consejos precisos y acercándome mucho más a Dios y dando su tiempo para que yo pudiera conocer a ese ser Soberano y cuanto es real y fundamental en nuestras vidas. Gracias Totales

Agradecimiento

Quiero agradecer a la Abogada Diana Ramos, quien me impartió e impulso a seguir con este tema, para que pueda comenzar con este proyecto de investigación, siendo ella la pionera en darme las herramientas necesarias para poder desarrollar en mi campo de investigación, además; de la Abogada Carla Carrera, en que ella fue el pilar base de mi formación como un profesional tanto como en el área laboral como en lo personal, y apporto mucho sus conocimientos para poder seguir adelante en mis proyectos académicos, haciendo que pueda desenvolverme mas en la materia del derecho. Quiero agradecer también a la Abogada Zoila Urgiles, por ser una excelente profesional conmigo, dándome sus dotes creativos en el desarrollo de mi carácter, añadiendo también, que fue una pieza clave en el desarrollo de mis proyectos, cumpliendo con las bases legales que necesitaba para valer de mi trabajo.

Y quiero agradecer al Abogado Manuel Avegno, siendo la persona muy importante en mi vida que me enseñó mucho en esta profesión, siendo mi mentor y amigo, llegándolo a considerar demasiado en mi vida profesional, impulsándome al éxito con sus consejos y brindándome apoyo incondicional en mi vida.

Resumen

La presente investigación tuvo como objetivo general, establecer la apropiación de datos por medios electrónicos en el ordenamiento jurídico ecuatoriano, para evitar la vulneración de los derechos económicos de la víctima, para ello se analizaron los elementos teóricos que forman parte de la apropiación de datos por medios electrónicos, se demostraron las consecuencias positivas evidenciadas en Colombia al incluir la apropiación de datos por medios electrónicos como un delito en el Código Penal y por último se propuso la inclusión de la apropiación de datos por medios electrónicos como un delito dentro del Código Orgánico Integral Penal. Desde el punto de vista metodológico, el enfoque de la investigación fue de carácter cualitativo, por cuanto la investigación presento primordialmente una minuciosa investigación bibliográfica, pertinentes para el análisis de la apropiación de datos por medios electrónicos, para evitar la vulneración de los derechos económicos de la víctima así como también se efectuaron entrevistas en profundidad. Los resultados de la investigación, demostraron que en relación al delito de apropiación fraudulenta por medios electrónicos en Ecuador tiene múltiples falencias y se hace necesario que el legislador ecuatoriano, efectúe una revisión a los fines de evitar la comisión de delitos electrónicos mediante la apropiación de datos. De igual forma los resultados demostraron que en el Estado ecuatoriano hace falta instituciones que velen por la ciudadanía a los efectos de tutelar su derecho a la protección de datos, y que terminen siendo víctimas de su patrimonio a consecuencia de terceras personas.

Palabras Clave: Apropiación, datos, medios, electrónicos, patrimonio

Abstract

The present investigation had as a general objective, to establish the appropriation of data by electronic means in the Ecuadorian legal system, to avoid the violation of the economic rights of the victim, for this the theoretical elements that are part of the appropriation of data by electronic means, the positive consequences evidenced in Colombia by including the appropriation of data by electronic means as a crime in the Penal Code were demonstrated and finally the inclusion of the appropriation of data by electronic means as a crime within the Integral Organic Code was proposed. Penal. From the methodological point of view, the research approach was of a qualitative nature, since the research primarily presented a detailed bibliographical investigation, relevant for the analysis of the appropriation of data by electronic means, to avoid the violation of the economic rights of the victim as well as in-depth interviews were conducted. The results of the investigation showed that in relation to the crime of fraudulent appropriation by electronic means in Ecuador it has multiple shortcomings and it is necessary for the Ecuadorian legislator to carry out a review in order to avoid the commission of electronic crimes through the appropriation of data. . In the same way, the results showed that in the Ecuadorian State there is a need for institutions that watch over citizens in order to protect their right to data protection, and that they end up being victims of their heritage as a result of third parties.

Keywords: Appropriation, data, media, electronic, heritage

Índice

Resumen _____	IV
Abstract _____	V
Introducción _____	1
Pregunta problémica _____	1
Objetivos _____	2
Objetivo general _____	2
Objetivos específicos _____	2
Justificación _____	2
Alcance _____	2
Capítulo I: Marco teórico _____	4
Antecedentes _____	4
Marco doctrinario _____	7
La protección de datos _____	7
La protección de datos por medios electrónicos. _____	8
Vulneración de la identidad por medios electrónicos _____	11
Apropiación de datos por medios electrónicos en Colombia _____	14
La banca virtual _____	16
Necesidad de la banca virtual _____	17
Necesidad de información a usuarios de banca on line _____	20
Derechos de las personas víctimas de apropiación de datos por medios electrónicos _____	23
Capítulo II: Marco metodológico _____	24
Tipo de investigación _____	24
Enfoque de investigación _____	24
Diseño de investigación _____	25
Métodos _____	26
	VI

Inductivo _____	26
Analítico _____	26
Sintético _____	27
Técnicas e instrumentos para la recolección de datos _____	27
Entrevista _____	27
Operacionalización de las variables _____	27
Variable Independiente _____	27
Variable dependiente _____	27
Entrevistas _____	28
Entrevista N° 1 _____	28
Entrevista N° 2 _____	31
Entrevista N° 3 _____	34
Entrevista N° 4 _____	37
Capítulo III: Análisis de los resultados _____	40
Capítulo IV: Propuesta _____	47
Exposición de motivos _____	47
Justificación _____	47
Objetivos _____	48
Alcance y Beneficios _____	48
Desarrollo _____	49
Conclusiones _____	51
Recomendaciones _____	53
Bibliografía _____	54

Introducción

En la ciudad de Guayaquil, Ecuador año 2023 existe la necesidad de contemplar una disposición normativa que proteja la identidad por medios electrónicos, ya que el Código Orgánico Integral Penal vigente no lo contempla, situación que trae como consecuencia que este tipo de delitos o actuaciones ilícitas, queden impunes, vulnerando de esta manera el derecho de la víctima a la protección de su patrimonio. En consecuencia, se requiere que la Asamblea Nacional en futuras modificaciones al Código Orgánico Integral Penal, establezca un artículo en el cual se proteja a las víctimas de la usurpación de identidad así como también sancione a los sujetos activos que causen este tipo de daño.

Cuando se analiza la legislación internacional, es importante señalar que en Colombia está contemplado protección de la identidad en fraudes financieros, ello para tutelar el patrimonio de las personas que últimamente estaban siendo engañadas a través de delitos como el Phishing online, el cual es efectuado por delincuentes cibernéticos ya que logran obtener mediante correo electrónico enviados a la víctimas, la información financiera que se encuentra en los dispositivos tecnológicos, en el cual se lograba abrir un correo electrónico.

En Colombia el Código Penal contempla en su artículo 296, el delito de falsedad personal y ocurre cuando una persona con el fin de obtener un provecho para sí o para otro, sustituye su identidad y se atribuye ciertas cualidades que son inherentes a otra, como su nombre edad y número de identificación, es importante señalar que en este país, se encuentran contemplados el delito de hurto por medios informáticos y semejantes así como también la violación de datos personales, situación que configura la protección de la identidad de una persona a los fines de evitar la vulneración de sus derechos y que de esta forma se puede efectuar el retiro total o parcial de dinero de las cuentas de un titular (Tocora, 2022).

Pregunta problémica

¿Cómo proteger la identidad de las personas por medios electrónicos?

Objetivos

Objetivo general

Establecer la apropiación de datos por medios electrónicos en el ordenamiento jurídico ecuatoriano, para evitar la vulneración de los derechos económicos de la víctima.

Objetivos específicos

Analizar los elementos teóricos que forman parte de la apropiación de datos por medios electrónicos.

Demostrar las consecuencias positivas evidenciadas en Colombia al incluir la apropiación de datos por medios electrónicos como un delito en el Código Penal.

Proponer la inclusión de la apropiación de datos por medios electrónicos como un delito dentro del Código Orgánico Integral Penal.

Justificación

La presente investigación se justifica, porque en el ordenamiento jurídico ecuatoriano no se encuentra contemplada en el Código Orgánico Integral Penal la protección de la identidad por medios electrónicos, en consecuencia, se hace necesaria la presente investigación a los fines de poder determinar la manera como debe incluirse una normativa que contemple dicha situación en la ley penal, ya que producto de ello de la ausencia de este tipo de disposiciones normativas no existe una sanción para aquellas personas que vulnera la identidad por medios electrónicos, trayendo como consecuencia, lesiones patrimoniales de las víctimas afectadas.

Alcance

El presente estudio investigativo posee un alcance de carácter exploratorio por cuanto hace referencia a la vulneración de la identidad por

medios electrónicos, que no se encuentra contemplada en el Código Orgánico Integral Penal a los efectos de proteger la vulneración de la identidad de las víctimas, ya que el tema ha sido muy poco estudiado, es más no se encuentra contemplado dentro de la legislación ecuatoriana y el fin de la presente investigación es justificar las razones por las cuales la Asamblea Nacional en futuras modificaciones del Código Orgánico Integral Penal debe incluir esta figura jurídica.

Capítulo I: Marco teórico

Antecedentes

Dentro de las investigaciones previas que poseen una relación directa con el con el tema desarrollado en el presente estudio, es importante hacer referencia a la efectuada por Rodas (2018) que lleva por título, “El delito de apropiación fraudulenta por medios electrónicos en la ciudad de Guayaquil” en la cual la autora hace referencia que en los actuales momentos los delitos informáticos han venido calando y aumentando sus cifras de una manera bastante ascendente, trayendo como consecuencia la lesión del patrimonio de muchas personas, a tal punto que se ha convertido en un delito bastante común, el cual se materializa por el robo de clave contraseñas causando un daño patrimonial a las personas que son afectadas a consecuencia de este delito.

Los resultados de la investigación, permitieron determinar qué este tipo de delito es bastante común, producto que las personas tiene un conocimiento muy escaso vinculado a la seguridad en cada una de las transacciones que se realizan a través de internet o mediante dispositivos tecnológicos, situación que permite que los delincuentes tomen ventajas y pueden obtener sus usuarios y contraseñas con el fin de realizar operaciones bancarias vulnerando los derechos de la víctima.

La investigación concluye señalando que se hace necesario que se contemple dentro del Código Orgánico Integral Penal la inclusión de la protección de datos por medios electrónicos, como un delito a los efectos de sancionar este tipo de conducta, ya que por ser atípica no existe una sanción que se puede aplicar a las personas que causan este tipo de daños. Concluye de igual manera la investigación, señalando que se hace necesario que las autoridades competentes en materia de investigación penal, deben dictar un conjunto de charlas informativas a la población que en su gran mayoría desconoce este tipo de delitos y por tal motivo es presa fácil de los delincuentes que quieran apropiarse de su dinero.

Otra de las investigaciones que posee una pertinencia directa con la presente es la realizada por López (2022) titulada “Delito de apropiación fraudulenta por medios electrónicos bajo la modalidad del piching dentro del

marco jurídico ecuatoriano”, en dicha investigación el autor realiza un análisis profundo de la manera cómo se afectan los recursos económicos de muchas personas que por desconocimiento no toma las medidas necesarias para ser objeto de estafas o cualquier tipo de delito informático, que al final termina causando un gravamen en el patrimonio de la víctima.

Los resultados de la investigación, tanto desde el punto de vista cualitativo como cuantitativo permitieron determinar que existen múltiples falencias dentro del Código Orgánico Integral Penal y que se hace necesaria una revisión profunda, a los fines de evitar la comisión de delito electrónicos mediante la apropiación de datos, ya que en muchas oportunidades se evidencian falencias dentro de dicho cuerpo normativo, que permiten que personas inescrupulosas que causan un daño económico a otra, no sean sancionados por cuanto su actividad no se ajusta a lo contemplado en la norma legal vigente.

En conclusión el autor plantea, que se hace necesario una revisión íntegra del Código Orgánico Integral Penal a los efectos de evitar los delitos de apropiación de datos por medios electrónicos y recomienda efectuar una comparación con otros ordenamientos jurídicos, como el caso de Colombia en el cual se contemplan de una manera más rígida los delitos que se cometen mediante el ejercicio de la apropiación de datos personales.

Continuando con las investigaciones que se encuentra vinculada en el presente tema de estudio, es importante hacer referencia a la realizada por Chiluisa (2021) titulada “Los delitos informáticos y los vacíos legales que afectan a los ciudadanos” en ella se realiza un análisis efectuado por el autor, en el cual parte del criterio que el sistema jurídico contemplado dentro del Estado ecuatoriano contempla un conjunto importante de normas, la cual se encuentran recogidas en el Código Orgánico Integral Penal vinculada a la sanción de delitos que se cometen por lo por vía electrónica, pero lamentablemente señala el autor hace falta que se haga referencia de manera directa a la apropiación de datos, por cuanto el mismo desarrollo tecnológico en la medida que ha ido surgiendo, ha traído como consecuencia que surjan nuevos tipos delictuales que se hace necesario que el legislador lo contemple porque causan un gravamen a la ciudadanía en general.

Los resultados de esta investigación, permitieron determinar que se han constituido dentro del territorio ecuatoriano diversas actividades delictivas que se efectúan mediante las estructuras electrónicas y tecnológicas, que tienen como fin efectuar una manipulación de la banca virtual, a los efectos de tener acceso a datos personales de un individuo y de esta manera poder efectuar determinadas transacciones económicas en perjuicio de la víctima, por lo cual se hace necesario que la legislación del Ecuador debe adaptarse a nuevos tipos penales que se encuentra contemplado en otros países, y que en la actualidad han existido ciertas actividades similares por lo cual se hace necesario que el legislador adecue la normativa penal interna y toma en consideración experiencias de otros países.

Por último la investigación concluyó hoy que el legislador ecuatoriano debe efectuar una evaluación actual de los delitos informáticos, a los efectos de evidenciar las lagunas legales o algún tipo de elementos que no han sido incluidos y que están causando un daño a la colectividad, ya que producto del paso del tiempo, surgen nuevas actividades delictivas que deben ser incorporadas dentro del cuerpo legal, a los efectos de poder defender los derechos de la colectividad quien en la actualidad queda en indefensión en aquellas situaciones en las que existe apropiación de datos y producto de ello sufre las consecuencias económicas de una disminución patrimonial producto de una actividad delictual realizada por terceros.

Por último en destacable la investigación realizada por Chitalogro (2022) denominada “Análisis dogmático penal de los delitos de apropiación fraudulenta y estafa cuando son realizados por medios electrónicos en el Código Orgánico Integral Penal” esta investigación hace de una manera profunda un análisis del delito estafa y apropiación fraudulenta, que son unos de los más comunes que se realizan por la vía de los medios electrónicos, destacando que son producto de las nuevas tecnologías que han venido surgiendo con el devenir del tiempo, pero qué importante también destacar que se hace necesaria la incorporación de nuevos delitos, como por ejemplo la apropiación de datos, ya que la mayoría de las personas se centra en delitos como la estafa y apropiación fraudulenta dejando de lado que en muchas oportunidades este tipo de delitos son producto de la apropiación de datos, que sería un delito principal y por ejemplo los delitos

señalados anteriormente como la estafa u otros serían ya de naturaleza accesoria.

Los resultados de la investigación permitieron demostrar que se hace necesario que dentro del Código Orgánico Integral Penal debe contemplarse la figura de la apropiación de datos, ya que hay muchos delitos informáticos que se encuentran contemplados en dicha normativa, en principio cuando existe la apropiación de datos con el fin de cometer un delito electrónico mediante los usuarios de banca virtual, en consecuencia, se requiere por una parte que se incluya esta actividad como delictuosa así como también normalísimo competentes deben tomar la iniciativa de efectuar campañas de concientización, con el fin que las personas de una manera general tengan conocimiento de este tipo de delitos cómo se cometen para evitar ser presa fácil de los estafadores.

Por último, la investigación concluye señalando que en la actualidad producto de la evolución del tiempo el Código Orgánico Integral Penal debe ser realizado en materia de delitos electrónico por cuanto existen muchas falencias que terminan lesionando los derechos de la ciudadanía por cuanto existen vacíos legales que deben ser llenados por el legislador haciéndose para ello de la experiencia que existe en países en las cuales se han cometido ese tipo de actividades delictivas.

Marco doctrinario

La protección de datos

En principio es importante señalar, que los datos personales están formados por un conjunto de información que son inherentes a una persona natural y que una decisión muy individual de un ciudadano, determinar si los comparte o no con terceros y es por ello que ha sido considerado desde el punto de vista doctrinal cómo de derecho privado, ya que forma parte de la esfera personal de un individuo así como también que son informaciones que la mayoría de las personas y el legislador por su naturaleza le han dado un carácter especial (Pérez, 2022).

Los datos personales, son concebidos como un conjunto de documentos informaciones que son inherentes a una persona, y qué esta ha decidido excluir

por decisión propia del conocimiento público, ya que existen información como la vinculada a una cuenta bancaria a ciertos documentos a tramitaciones o a negocio que incumben solamente a una persona y no al resto de la sociedad. (Carazo, 2021)

De la definición anterior, se evidencia que los datos personales son inherentes a una persona y se encuentran dentro de la esfera privada de la misma, salvo que su titular decida compartirlo con terceras personas o con el público en general, pero el criterio es que los datos personales forman parte de la esfera privada de una persona.

Los datos personales están formados por un conjunto de información que está vinculada directamente con una persona así como también sus intereses, que pueden ser familiares económicos patrimoniales o de cualquier índole y que por decisión propia pasan a formar parte de la esfera privada y de la intimidad de una persona, en consecuencia si un tercero accede a ello o efectúa una publicación de los mismos, o los utiliza para fines propios o de terceros ,está vulnerando el derecho a la privacidad de los datos de una persona (Conde, 2019).

Al efectuar un análisis de la definición anterior, se demuestra que los datos personales forman parte de la esfera privada de un ciudadano y que de acuerdo a lo que establece la doctrina dominante, si un tercero por cualquier vía, sea física o electrónica, accede a ellos sin consentimiento está vulnerando el derecho a la intimidad de una persona así como también si al obtener esa información la divulga de manera pública o a terceras personas estaría cometiendo e igual forma un delito.

La protección de datos por medios electrónicos.

La protección de datos por formar parte del aspecto íntimo de una persona siempre ha sido una preocupación para el legislador, con el fin de evitar la sustracción de los mismos, y que se creen mecanismos que permitan la obtención de los datos de manera fraudulenta con el fin de causar un daño al titular de los mismos.

En la actualidad, gracias a las nuevas tecnologías y el desarrollo del internet y de nuevo dispositivos desde el punto de vista delictual, se han

generado programas software y estrategias con el fin de obtener datos esenciales de las personas, principalmente de carácter bancario, a los fines de lograr un perjuicio económico en la víctima en beneficio de la persona que comete este hecho punible (Pacheco, 2022).

Es muy común en la actualidad el fraude a través de medios electrónicos, mediante el cual se clonan tarjetas y se envían programas a través de correos electrónicos con el fin de obtener la información básica, que tiene una persona en su computadora, para de esta manera obtener claves bancarias con el fin de lesionar económicamente una persona. En este sentido, se hace necesario que el legislador contemple las medidas necesarias para sancionar este tipo de conductas así como también periódicamente se deben evaluar las nuevas tecnologías así como también las nuevas actividades que causan perjuicio de la ciudadanía, a los efectos que el derecho siempre esté a la par de cualquier tipo de actividades que lesionen al ciudadano, porque muchas veces el derecho se ha quedado muy por detrás de las nuevas tecnologías, situación que trae como consecuencia que se causen daños a persona y que no existan sanciones.

Un delito bastante común que se comete en la actualidad en la sustracción de datos personales por medio electrónicos, en este aspecto hay que señalar que el continente latinoamericano en general desde el punto de vista legal se ha quedado por detrás de las nuevas tecnologías, si se le compara con la Unión Europea y países como España los cuales existe un desarrollo normativo y organizacional a los fines de tutelar los derechos económicos de la población, haciendo frente con tecnologías para detener este tipo de delitos (Davara, 2018).

La cita anterior demuestra que en materia de medios electrónicos se hace necesario que el sistema de justicia contemple medidas tecnológicas en el ámbito judicial y de investigación, con el fin de poder detener este tipo de delitos que son bastante complejos, por lo cual se requiere de auxiliares judiciales que posea un conocimiento tecnológico a los fines de poder investigar y posteriormente sancionar este tipo de actos que por lo general no dejan huellas y se efectúan desde la clandestinidad.

Ahora bien es importante señalar que el Estado como máximo representante de la ciudadanía, como el ente encargado de tutelar los derechos de la población, dentro de su estructura organizativa producto de la evolución de

las nuevas tecnologías, debe tener instituciones que velen por la protección de los datos personales de la población en general, como por ejemplo la dirección nacional de registro de datos públicos o un ministerio de telecomunicaciones e información, que dicte periódicamente políticas públicas para evitar la comisión de este tipo de delitos así como también genere campañas de difusión masiva para que el ciudadano común que es víctima de ese tipo de situaciones conozca cómo proteger sus datos personales, especialmente aquellos que están vinculados con su banca virtual para que no sean presa de criminales y estafadores que utilizan esta vía para causarle un perjuicio económico (Pérez, 2022).

En la actualidad la gran mayoría de los fraudes que se cometen por medios electrónicos se realizan con el fin de causar un daño patrimonial a la víctima de obtener datos esenciales de su banca virtual como claves contraseñas números de cuentas y de esta manera poder acceder a sus cuentas personales y de esta manera efectuar transferencia u operaciones con el fin de sustraer recursos económicos de la víctima.

En la actualidad uno de los delitos más comunes es el phishing el cual consiste en el envío de virus a través de correo electrónicos dirigidos a la víctima, los cuales en la mayoría de los casos señalan que el destinatario es una entidad bancaria la cual se ofrecen crédito o promociones a los fines que la víctima opte por entrar en una aplicación o en un enlace que al efectuarlo sí generan virus que sustraen la información de dicho computador para ubicar principalmente clave y contraseñas bancarias (Determan, 2017).

Lo anterior evidencia una de las formas más comunes de delitos electrónicos, ya que de esta manera se pueden obtener los datos personales claves contraseñas que se requieren a los fines de poder entrar a la banca virtual de una persona y de esta manera poder efectuar transferencia, de igual forma al obtener datos esenciales de las transacciones bancarias que se encuentren en el computador de la persona, poder obtener números de tarjeta claves y códigos de seguridad que van a permitir efectuar operaciones de manera virtual y obtener recursos económicos de la víctima.

La nueva tecnologías han permitido que por existir múltiples plataformas hoy los estafadores informáticos estén en cada una de ellas, en el párrafo

anterior se habló del phishing que se comete en correos electrónicos pero es que también esta forma de fraude se observa también a través de cualquier tipo de plataforma como puede ser Facebook, Instagram, en el cual se pueda recibir un mensaje que al abrirlo pueda robar la información que tiene una persona en su computadora o dispositivo móvil (Rosales, 2022).

Ahora bien, en la actualidad se hace necesario tomar medidas preventivas pero para ello se necesita del conocimiento de la colectividad, por lo cual tienen que existir recomendaciones de los bancos así como también de los cuerpos de seguridad del Estado que permitan a la colectividad tomar las medidas preventivas necesarios para evitar ser víctima de delitos electrónicos que sustraen sus recursos económicos.

Se hace necesario cuando se opera por medios electrónicos específicamente en banca online ciertas recomendaciones dentro de las cuales destacan tener instalado un software de seguridad así como también sistemas operativos actuales, evitar guardar información vinculada a números de cuenta en plataformas digitales o en archivos especiales de internet, ya que de existir un software que recupere la información de la PC o el dispositivo móvil fácilmente y un tercero puede tener acceso a ello y de esta manera ingresar a la banca virtual (Ferreira, 2019).

De acuerdo a lo señalado en la cita anterior, se evidencia que se hace necesario que la víctima debe poseer una investigación una información específica a los fines de evitar la vulneración de sus derechos, en consecuencia, debe tomar las medidas necesarias dentro de las cuales se recomienda un software especializado así como también evitar abrir correo electrónico de destinatarios desconocidos y desconfiar de aquellas ofertas que pareciera muy atractivas por parte de instituciones bancarias y verificar la autenticidad de dichas páginas a los efectos de evitar ser víctima de delincuentes que tienen como fin causar un perjuicio económico a la víctima.

Vulneración de la identidad por medios electrónicos

Una de las formas por las cuales puede ocurrir la vulneración de la identidad por medio electrónicos, ocurre en aquellas situaciones en las que existe un robo de identidad personal, el cual se manifiesta mediante el acceso

ilegítimo a sistemas informáticos, propios de la víctima, en consecuencia, es importante señalar que para que ello ocurra, por una parte tiene que existir el acceso ilegítimo y por la otra la sustracción de datos personales que permitan efectuar operaciones bancarias mediante la banca online, dentro de las cuales se pueden observar nombres de usuario, contraseñas claves y ciertos elementos que permitan a cualquier tercero, suplantar vía electrónica la identidad de una persona mediante un conjunto de datos que son privados (Orellana, 2020).

De acuerdo a lo anterior se puede señalar que la vulneración ocurre desde el momento en que se obtienen los datos por vía electrónica, con el fin de crear un falso perfil para suplantar ante la banca virtual la personalidad de la persona que es titular de la cuenta, y efectuando operaciones como si se tratase de ella, esto es un delito que es eminentemente intencional, porque existe el dolo de causar un perjuicio económico a la víctima. Este es un delito que se ha hecho bastante común en la actualidad, producto de las nuevas tecnologías y de la utilización de software que permiten obtener datos bancarios de los dispositivos móviles o de los computadores de la víctima.

Cuándo se efectúa un robo de identidad con un fin patrimonial, se causa por una parte una lesión al derecho a la intimidad que ocurre desde el momento en que se obtienen datos privados de la persona, así como también existe una vulneración al patrimonio, ya que posteriormente se utilizan los datos obtenidos para efectuar compras en nombre de la persona o transferir cantidades de dinero a otras cuentas, en consecuencia, se evidencia que es un delito bastante complejo, por cuanto presenta variadas aristas y puede lesionar varios bienes jurídicos (López J. , 2019).

En la actualidad en delito de robo de identidad es bastante común, sobre todo cuando se efectúa mediante algún sistema informático o algún software que permite obtener información confidencial, como clave y contraseñas, con el fin de causar un daño patrimonial a la víctima, este tipo de actuaciones han sido descritas por la mayoría de la doctrina penal como acto de delincuencia informática. Este tipo de delitos son bastante complejos, por cuánto los criminales operan bajo la clandestinidad y generalmente cambian de domicilios para no ser ubicados, en la mayoría de los casos la víctima no tiene ningún nexo

común con el delincuente caso distinto que se presenta la mayoría de los delitos comunes en los cuales en la mayoría de ellos existe una vinculación (Rebolledo, 2020).

La cita anterior, evidencia lo complejo de este tipo de actividades delictuales, ya que el autor parte del criterio que son muy diferentes a los delitos comunes, por cuanto lo único que queda es un rastro informático y en oportunidades es imposible recuperar el dinero perdido, ya que la persona tiene conocimiento mucho tiempo después y por ello que es esencial que el Estado a través de cada uno de sus órganos, capacite a la colectividad de manera general, efectúe campañas publicitarias a través de redes sociales, de medios de comunicación, que permitan a la ciudadanía estar alerta ante este tipo de situaciones que puedan detectar cuándo un correo electrónico enviado no es fidedigno, cuáles son los elementos esenciales para determinar la veracidad de un sitio en internet, ya que ello permitiría la disminución de este tipo de delito y de los efectos del mismo.

En este aspecto es importante señalar que a nivel internacional existen normativas que hacen referencia a este tipo de delito dentro de las cuales es importante mencionar el artículo 3 del Convenio Sobre la Ciberdelincuencia (2001) que contempla la interceptación ilícita, En la cual se hace referencia que los estados tienen la obligación de establecer las políticas públicas desde el punto de vista legislativo que sean necesarias para contemplar este tipo de delito dentro de su jurisdicción interna incluidas cualquier tipo de misiones electromagnéticas incluidas las emisiones electromagnéticas provenientes de un sistema informático que transporte dichos datos informáticos, las partes podrán exigir que el delito se cometa con intención delictiva o en relación a un sistema informático conectado a otro sistema informático.

Al efectuar un análisis del artículo anterior se evidencia cómo desde el punto de vista internacional existe la obligación para los estados de establecer desde el punto de vista legislativo, un conjunto de normas que impidan la vulneración del derecho a la identidad, y los datos de una persona por medio informático, destacando de esta manera que es una obligación del Estado establecer las condiciones necesarias para la comisión de este hecho punible, bien desde el punto de vista legislativo, creando disposiciones legales para ello

pero también desde el punto de vista organizativo y funcional, a través cada uno de los organismos que forman parte de la administración pública que posea la competencia en la materia.

Apropiación de datos por medios electrónicos en Colombia

En Colombia es importante hacer referencia a la ley 1273 del año 2009, ya que a través de ella se modificó el Código Penal, partiendo del criterio que producto de las nuevas tecnologías, existe un nuevo bien jurídico tutelado que es la protección de la información y de los datos a los fines de poder preservar de una manera completa cada uno de los sistemas que utilicen tecnologías de información y comunicación.

Esta disposición normativa en Colombia ha sido bastante positiva, porque ha permitido la sanción de un conjunto de actuaciones que estaban causando un daño a muchos particulares, dentro de ella es importante hacer referencia al uso de software malicioso que se materializa en aquel caso que se produzca trafique o adquiera cualquier tipo de software que tengan como fin crear un efecto dañino en cualquier medio informático.

Se encuentra también la violación de datos personales, que incurre en este tipo delictual cualquier persona que no tenga la potestad y con provecho propio o de un tercero sustraiga por medio de la utilización de medios informáticos, datos inherentes a una persona mediante la utilización de datos personales contenidos en archivo o en ficheros, ya que de esta manera en primera instancia se estaría vulnerando el derecho a la intimidad, de la persona así como también este tipo de datos personales pudieran estar siendo utilizado para causar un daño patrimonial a la víctima (Ayjon, 2019).

También dentro de esta disposición normativa, se contempla la transferencia no consentida de activos que ocurre en el tipo de situaciones en la cual una persona con ánimo de lucro y valiéndose de algún tipo de manipulación informática, pueda ingresar a la banca virtual de una persona, utilice su usuario y contraseña para efectuar una transferencia económica para sí o para un tercero será sancionado con una pena de prisión de 48 a 120 meses así como también una multa de 200 a 1500 salarios mínimos a los fines de sancionar este tipo de conductas y evitar que otras personas intenten cometer este tipo de delitos.

Ahora bien es importante destacar que de acuerdo a las cifras establecidas por la Fiscalía General de Colombia, al efectuar una comparación de las cifras de delitos electrónicos, apropiación de datos por medios electrónicos antes de la entrada en vigencia de esta normativa y comparando la cifra con el año 2021, se pudo reducir en un 63% la cantidad de delitos que eran cometidos por esta vía, tomando en consideración que en la actualidad cuatro de cada cinco colombianos ya forman parte de la era digital, poseen un dispositivo móvil, una computadora, manejan su banca virtual así como también existen políticas públicas iniciadas por parte del Estado colombiano a los fines de realizar la mayor cantidad de operaciones a través de la banca virtual (Campos, 2022).

Las estadísticas han demostrado, en este país que de forma progresiva cada año disminuyen las personas que no tienen acceso a internet, que no poseen una banca virtual, correos electrónicos o algún dispositivo que permite una conexión a internet como puede ser una tableta, una computadora o una laptop o un teléfono inteligente. En este país, los usuarios manejan múltiples plataformas desde mensajería instantánea, correos electrónicos y aplicaciones bancarias, situación que ha hecho que el legislador colombiano haya tomado un interés importante en el establecimiento de medidas para evitar la apropiación de datos por medios electrónicos.

La promulgación de esta ley ha sido bastante beneficiosa, tomando en consideración el tráfico comercial que existe por medios electrónicos, ya que de acuerdo a las estadísticas de la Fiscalía General de Colombia, para el año 2021 en comparación con el año 2015, la compra por medios electrónicos había aumentado un 32%, así como también en ese mismo periodo de tiempo las aplicaciones por cuenta de ahorro se habían incrementado de 21 a un 39% es decir, en este país existe un comercio electrónico importante así como también una gran cantidad de personas que poseen aplicaciones bancarias, situación que obligó al Estado colombiano a tomar las medidas pertinentes y dictar una normativa legal para la protección del patrimonio del colombianos.

Ahora bien importante también señalar que el 24 de julio del año 2008 fue aprobada la ley número 1928 mediante la cual se ratificó el convenio sobre el cibercrimen en Budapest, actividad que se realiza con mucho tiempo después de

haber sido aprobado este convenio a nivel mundial pero que igualmente es beneficioso a los fines de la protección de los datos por medios electrónicos que posee una persona, en este sentido es importante hacer referencia a la exposición de motivos de la ley 1928 (2018) que señalo a grandes rasgos la necesidad de contemplar política penales que tengan como fin tutelar los derechos de la sociedad en relación a la ciberdelincuencia, mediante un conjunto de medidas que permitan la cooperación internacional, tomando en consideración que la nueva era de la digitalización ha hecho que se creen los delitos informáticos, en consecuencia, el ejercicio del derecho debe estar a la par y debe evolucionar para solventar esto problemas a la sociedad.

La banca virtual

Las nuevas tecnologías han traído como consecuencia, la facilidad de la vida del ser humano en todos sus aspectos. dentro de la cual es importante hacer referencia a las transacciones bancarias. las cuales son una necesidad bastante común en toda persona ya que a través de ello, se pueden comprar alimentos pagar los servicios e internet. En este sentido, es importante señalar que la creación de este tipo de sistema bancario, ha hecho más sencillas las transacciones electrónicas comunes, en la actualidad no es necesario que una persona deba acudir a la sede de un banco para efectuar un depósito, para retirar un dinero, perfectamente puede hacer una transferencia a través de su computador, o a través de una aplicación que posee en su dispositivo móvil (Cianciardo, 2021).

En la actualidad ha sido muy ventajoso la utilización de la banca a distancia, porque ha permitido que situaciones que anteriormente eran bastante complejas, se puedan simplificar, por ejemplo el comercio internacional se ha beneficiado bastante de este tipo de bancas, las que era bastante complejo los trámites. En este sentido, hasta el punto que se necesitaba a veces hasta una semana o dos semanas para que se materializara un pago de un continente a otro en la actualidad es cuestión de segundo para procesar una transacción de esta naturaleza (López J. , 2019).

Dentro de las ventajas que poseen la banca virtual es importante señalar que ella posee varios tipos de tecnologías, entre las cuales se encuentra la banca telefónica, que permite realizar operaciones por esta vía se encuentran de igual manera las transferencias electrónicas así como también la banca online, que es aquella que presta servicio exclusivamente a través del internet. Una de las debilidades que se observa en la banca virtual es que ha existido poca difusión por parte de los órganos bancarios en establecer medidas preventivas para las personas, si bien es cierto cuando la persona firma un contrato se hacen algunas recomendaciones, la misma no se realizan con la suficiente profundidad en consecuencia, no existe una toma de conciencia real en relación a la parte preventiva que debe tenerse al efectuar transacciones vía online, lo cual puede permitir que se efectúen cualquier tipo de delitos tomando en consideración el desconocimiento de las medidas preventivas que debe tomar la víctima.

Necesidad de la banca virtual

La banca virtual, ha surgido como una necesidad producto del desarrollo de las actividades económicas que se efectúan entre empresas y entre particulares o entre particulares y las empresas, inclusive el Estado se ha visto beneficiado de las nuevas tecnologías específicamente mediante el sistema financiero virtual. Este tipo de sistema bancario, es bastante positivo porque trae como consecuencia, que se ahorre tiempo para las personas que realizan este tipo de operaciones, en consecuencia, las transacciones bancarias se realizan como una mayor facilidad a tal punto que si existe una institución financiera que no presenta este tipo de tecnología, puede presentar una merma en sus clientes ya que ellos consideran que es una entidad bancaria de poca calidad (Conde, 2019).

En consecuencia, la banca virtual se ha constituido como un canal comercial alternativo al sistema como venía tratándose la banca anteriormente, a tal punto que en la actualidad existen más personas que utilizan la banca virtual que la banca tradicional, es más existen instituciones financieras que a los fines de economizar en la contratación de personal y tener grandes sedes apuestan por tener sedes físicas mucho más reducidas e impulsan políticas bancarias a los efectos que las personas efectúen la mayoría de sus transacciones por vía

virtual, ya hasta las tarjetas de débito o crédito no es necesario acudir a la entidad bancaria a solicitarlas o retirarlas perfectamente se puede hacer utilizando los canales de la banca virtual (Lefebvre, 2022).

En la actualidad la banca virtual es muy bien valorada, por parte de los usuarios quién es en primer lugar ya buscan que se efectúen operaciones mediante las nuevas tecnologías, por cuanto le facilita el tiempo a la mayoría de las personas que ya están adaptadas a este nuevo sistemas tecnológicos, así como también le facilitan la realización de actividades de carácter bancario, lo cual al final trae como consecuencia, que se reducen los costos económicos, En este sentido es importante señalar que otro de los elementos que se encuentra bastante presente es el competitivo, debido a que prácticamente ninguna entidad bancaria no posee banca virtual, en consecuencia, se ha convertido en una institución que es bastante común y está obligatoria desde el punto de vista comercial para cualquier institución bancaria.

La banca virtual de la actualidad se ha convertido en una necesidad, ya que los nuevos tiempos hoy en día son más acelerados y se requieren respuestas más efectivas por parte de los operadores bancarios, situación que he encontrado respuesta en este tipo de sistema bancario, es importante señalar, que el usuario tiene también la responsabilidad conjuntamente con institución bancaria de tomar las medidas necesarias para evitar cualquier tipo de fraude o suplantación de identidad (Bueno, 2022).

En consecuencia, se puede señalar que las nuevas tecnologías fueron presionando para que las instituciones bancarias utilizarán estas estos nuevos sistemas bancarios, ya en la actualidad toda persona posee o un ordenador o un móvil inteligente, situación que le facilita la realización de transacciones bancarias. Ahora bien, como señalaba la cita anterior existe una corresponsabilidad entre la institución bancaria y el cliente en tomar las medidas necesarias para evitar el fraude realizado por terceras personas.

En este mismo sentido, es importante señalar que siempre ha existido una valoración bastante positiva por parte de los usuarios de la banca virtual, porque a diferencia de la banca tradicional esta puede operarse las 24 horas del día, así como también todos los días del año, situación que marca una diferencia bastante vertical con la tradicional banca, que tiene unos horarios diurnos así

como también funciona determinados días de la semana, situación que trae como consecuencia, limitantes para efectuar determinadas transacciones que mediante la banca virtual se efectúan de una manera más rápida e inmediata (Lefebyre, 2022).

En este mismo sentido, es importante señalar que dentro de las ventajas de la banca virtual, ha traído como consecuencia, que existan nuevas posibilidades de expansión, lo cual permite a las personas naturales o jurídicas expandirse hacia otros mercados así como también ampliar un negocio o inversión, al ver que existen plataformas que efectúan pagos y la materialización de transacciones financieras de una manera más rápida.

Ahora bien, desde el punto de vista institucional, han constituido que los bancos hayan podido redistribuir las sucursales bancarias y colocado de una manera más estratégica solamente sedes físicas, que se requieren para aquellas funciones del banco, para lo cual se hace necesario de manera obligatoria la presencia de una persona delegando en la banca virtual aquellas que no se requiere su presencia física (Cianciardo, 2021).

Dentro de los contras, de la banca virtual se encuentran los denominados riesgos operativos, que suene aquella serie de situaciones que puede traer como consecuencia que exista un mal funcionamiento de la tecnología y causar un daño económico, alguno de los usuarios del banco o que terceras personas realicen actos delictivo de suplantación de información u obtengan por medio fraudulento, claves de banca virtual y pueda ocurrir que existan ciertos delitos con el fin de dañar el patrimonio de la de la víctima.

Ahora bien, los riesgos señalados en el párrafo anterior de la banca virtual no solo son exclusivo en esta materia, sino para cualquier tipo de tecnología que se maneje a través de internet, para ello es esencial que existan medidas preventivas como la utilización de software especializado, como el hecho de que los usuarios de la banca virtual tengan conocimientos específicos para poder detectar cuando existe un software malicioso, cuando existe un correo electrónico que no debe ser abierto, como identificar datos que demuestran que se está ante una web segura, ya que de esa manera se va a permitir que exista mayor control y una mayor seguridad al momento de la utilización de la banca virtual

Necesidad de información a usuarios de banca on line

El lado frágil de la banca virtual ,se ha demostrado a través de dos elementos esenciales que hacen que pueda disminuir la eficacia de este tipo de tecnología, así como también crean desconfianza en los usuarios por una parte no existe una preparación o capacitación del cliente sobre cómo iniciar la banca virtual, en la mayoría de los casos la persona acude al banco y apertura una cuenta bancaria que puede ser de ahorro o corriente y automáticamente tiene acceso a la banca virtual, pero no existe una preparación previa una capacitación que le informe a la persona cómo debe utilizar la banca, salvo cierto tutoriales que poseen información muy reducida, de cómo poder efectuar operaciones a través de la banca virtual, pero en ningún momento existe formación para el usuario para determinar tanto la utilización como la prevención de fraudes electrónicos (Cianciardo, 2021).

Continuando es importante señalar que desde otro punto de vista es la mayoría de los casos los clientes no poseen el conocimiento de las consecuencias que puede traer la mala utilización de la banca virtual, situación que por no prestar la debida precaución puede terminar causando un perjuicio económico para la víctima, en definitiva se requiere que cada una de las entidades financieras deben promover procesos de aprendizaje a los fines de que el usuario pueda sacar el máximo provecho de la banca virtual y al mismo tiempo tener la seguridad de que no será víctima de un fraude electrónico, ya que podrá detectar todas aquellas situaciones en las cuales pueda ser víctima de un hecho punible en contra de su patrimonio personal.

En este sentido es importante la opinión de Defferary (2019) quien ha señalado lo siguiente

La banca virtual hoy es esencial para el progreso económico mundial, así como también para el normal desenvolvimiento de todas aquellas actividades económicas que tienen una vinculación por medios electrónicos, es un fenómeno que es totalmente irreversible. Ahora bien se hace necesario que las instituciones bancarias garanticen la seguridad de cada una de las operaciones de banca virtual, mediante la elaboración de manuales de funcionamiento de la página web, cursillos para los usuarios, explicaciones antes de la contratación y que

todo ello se pueda hacer de manera periódica, de tal manera de influir positivamente en la forma como el usuario debe utilizar la banca virtual para evitar de esta manera un perjuicio en su contra (Defferary, 2019).

Al efectuar un análisis de la cita anterior, se evidencia la importancia en la actualidad de la banca virtual y que es un tipo de tecnología que ya es totalmente irreversible a nivel mundial, forma parte de uno de los elementos o herramientas del sistema bancario, que permite que las operaciones se efectúen con una mayor rapidez, sencillez, en consecuencia, es responsabilidad de los agentes bancarios proporcionar a la ciudadanía a todas las personas que contratan con estas instituciones y que poseen acceso a una banca virtual, generar un conjunto de conocimientos, para evitar de esta manera un perjuicio económico en su contra.

En relación a lo anterior es importante porque de esta manera si se puede mostrar que el perjuicio económico que ha sufrido la víctima, ha sido producto que la institución bancaria no ha establecido las medidas de seguridad necesarias y pertinentes para tutelar el dinero que tiene resguardado en institución un particular va a existir una responsabilidad económica del banco hacia los usuarios situación que pudiera colocar en riesgo también la situación económica de la institución bancaria.

La banca virtual es una innovación muy importante en la actualidad, pero puede ser considerada también un arma de doble filo, en aquellas situaciones en que los usuarios no posean el conocimiento, es necesario ya que de esta manera pueden colocar en riesgo su situación económica y patrimonial. En este sentido, existe una correspondencia de usabilidad entre la institución bancaria y la ciudadanía, los primeros tienen que generar las condiciones de seguridad necesarias para evitar que terceros utilicen la red bancaria para generar un perjuicio al usuario y en relación a estos últimos deben tomar medidas necesarias para evitar que terceras personas de manera fraudulenta puedan acceder a sus datos bancarios y de esta manera utilizar la banca virtual como si fuese el titular y poder efectuar transferencia o compras que lesionen la economía de la persona (López J. , 2019).

Al efectuar un análisis de la cita anterior, es importante señalar que los dos contratantes, tanto la institución bancaria, como el usuario, tienen un

conjunto de obligaciones para poder determinar y evitar que se cause un perjuicio por vía de la banca virtual el banco por una parte tiene y está obligado a velar por tener una red de seguridad que esté encriptada a los efectos de tutelar los derechos económicos de las personas que han contratado con él, institución financiera y de esta manera evitar que por ataques cibernéticos hoy se pueda causar un daño alguna de las personas que utilizan la banca virtual.

Ahora bien importante señalar que los usuarios tienen también una responsabilidad en el hecho de tomar las medidas preventivas para evitar que datos como nombre de usuario y contraseña puedan ser obtenidos fácilmente, por parte de terceros, en este tipo de situaciones múltiples decisiones de la banca cuando se demuestra que se causa un perjuicio a un tercero pero el producto pero las investigaciones demuestran qué ha sido por negligencia del titular de la cuenta, de aquí las operaciones bancarias fueron realizadas bajo el usuario y la contraseña creada por el mismo titular allí en este tipo de situaciones no existe una responsabilidad por parte del banco en consecuencia le corresponde al titular de la cuenta actuar de manera directa en contra de las personas que han utilizado cualquier tipo de mecanismo para obtener sus datos de la cuenta virtual.

En definitiva se puede señalar, que la aplicación de la banca virtual en la actualidad es un elemento bastante común e inclusive necesario producto de la evolución de los tiempos y que se evidencia que es un tipo de tecnología que ha llegado para quedarse porque llenó muchos vacíos que se encontraban en la banca tradicional, pero hay que señalar que los riesgos son elevados porque principalmente se está jugando en muchas oportunidades los ahorros, una persona cantidades de dinero, que se tienen destinadas para un proyecto en específico, por lo cual se hace necesario que exista por parte de las instituciones financieras un conjunto de medidas que permitan hacer del conocimiento del usuario de este tipo de banca de los riesgos que ella conlleva y de esta manera pueda tomar las medidas previsibles necesarias para cuidar su actividad económica.

Derechos de las personas víctimas de apropiación de datos por medios electrónicos

En relación a los derechos de las víctimas de este tipo de delito es importante señalar por una parte que puede acceder al Estado a los efectos de obtener una protección en relación al daño sufrido, con el fin de exigir de los órganos competentes las sanciones por una parte a las personas responsables de este tipo de hechos así como también exigir la reparación del daño causado y obtener una reparación integral.

En este sentido importante la opinión de Bueno (2022) quien manifestó lo siguiente

Toda persona que ya ha sido víctima de un delito de apropiación de datos, por medios electrónicos cuyo fin sea vulnerar la banca virtual para obtener un provecho económico, en primer lugar tiene el derecho de denunciar a los fines de obtener una respuesta por parte del Estado para encontrar a las personas que han cometido el daño económico, en consecuencia, tiene el derecho de recibir un trato respetuoso, profesional, individualizado que de manera oportuna, permita el restablecimiento de su derechos vulnerados. (p. 33)

Al efectuar un análisis de la cita anterior, se evidencia que el legislador ha contemplado un conjunto de derechos para las víctimas de este tipo de delitos, ya que existe una afectación directa al patrimonio, y va ligado a otros derechos como el trabajo, la salud, ya que se priva la capacidad de disponer ciertos recursos o el aprovechamiento de terceros, lo que trae consecuencias negativas para la víctima en su aspecto patrimonial.

Otro de los derechos esenciales de la víctima, es que es el requerimiento que el proceso sea rápido y sin dilaciones indebidas, ya que ha existido una afectación directa a su patrimonio, que al mismo tiempo genera consecuencias indirectas como la disminución de la capacidad económica de la persona que ha sido limitada o vulnerada, le genera incomodidades ya que en base a sus recursos ella se organiza desde el punto de vista económico para el desarrollo de sus actividades y el pago de sus necesidades.

Capítulo II: Marco metodológico

Tipo de investigación

La presente investigación, posee un carácter documental, que se aplica esencialmente en todas aquellas investigaciones de naturaleza cualitativa, en la cual se tiene como fin recuperar una cantidad importante de información como obras literarias, libros, revistas, análisis de doctrinarios especialistas en el tema de estudio, con la finalidad de brindar un conocimiento profundo sobre un tema específico.

Las investigaciones documentales se efectúan principalmente cuando se pretende efectuar un análisis o una comparativa sobre un tema de estudio y lograr conclusiones específicas, ello que se vale en su mayoría de investigaciones previas y en base a ello se efectúan los análisis pertinentes, los cuales se pueden contrastar con otras investigaciones así como también con la opinión de especialistas en la materia.

Las investigaciones documentales son aquellas que se efectúan mediante el análisis, comparación, revisión de la literatura, periódicos, anuarios, normas jurídicas, siempre con el fin de efectuar, un análisis entre investigaciones que poseen temas similares, también se le denomina investigación secundaria ya que tiene su base en investigaciones realizadas por otras personas (Balestrini, 2019).

Del análisis anterior, se evidencia perfectamente que el presente tema investigativo posee un carácter documental, el cual se evidencia en el estudio de la protección de identidad por medio electrónicos, efectuando un análisis inclusive cómo se va a abordar esta problemática en el derecho comparado, en países como en Colombia, que posee una legislación más avanzada que la ecuatoriana.

Enfoque de investigación

El enfoque de la investigación es cualitativo, el proyecto presenta primordialmente una minuciosa investigación bibliográfica, pertinentes para el análisis de la apropiación de datos por medios electrónicos, para evitar la vulneración de los derechos económicos de la víctima, en este mismo sentido también se pretende, en este mismo sentido analizaron los elementos teóricos

que forman parte de la apropiación de datos por medios electrónicos y se demostraron las consecuencias positivas evidenciadas en Colombia, al incluir la apropiación de datos por medios electrónicos como un delito en el Código Penal.

La investigación cualitativa es aquella que tienen su razón de ser, en investigaciones documentales que pretenden efectuar comparaciones entre la opinión de varios autores así como también realizar un análisis de la forma cómo está concebido el problema, cómo ha evolucionado y cómo se encuentra en la actualidad, en la mayoría de los casos se hace ayuda de otros como el analítico, inductivo y sintético (Baquero de la Calle, 2018).

Al efectuar un análisis de la cita señalada en el párrafo anterior, se evidencia que la naturaleza de la presente investigación demuestra que es de carácter cualitativo, ya que el centro de la investigación parte del estudio bibliográfico de la apropiación de datos por medios electrónicos, así como también su vinculación con la banca virtual, también es importante destacar que se efectuarán entrevistas a profundidad a personas especialistas en esta área, todo lo que evidencia que se está en presencia de una investigación de carácter netamente cualitativo.

Diseño de investigación

La presente investigación posee un diseño no experimental, que es aquel que se efectúa en aquellas situaciones en las cuales no existe una alteración en la medición de las variables de estudio, en consecuencia, el investigador se limita solamente a analizar las principales variables del tema planteado.

Los diseños no experimentales son todos aquellos estudios en el cual el investigador tiene como fin analizar e investigar o desarrollar las variables de estudio que ha planteado desde el momento en que toma la decisión de iniciar la investigación y tiene definido el tema de estudio en consecuencia puede comparar las variables así como también analizarla pero no efectuará una alteración de las mismas en el desarrollo de la investigación. (Bernal, 2018)

Métodos

Inductivo

El método inductivo es propio de las investigaciones cualitativas, por cuanto él tiene como fin partir del estudio de situaciones concretas es un método muy importante del cual se vale el investigador en aquellas situaciones en las cuales se busca estudiar un tema específico con el fin de llegar a conclusiones generales para el logro de este método se requiere una investigación concreta o también la aplicación y análisis de entrevistas realizadas en profundidad (Hernandez, Fernandez, & Baptista, 2014).

Este método fue aplicado dentro de la presente investigación, en el momento que se efectuaron los análisis de las investigaciones vinculadas a la protección de identidad por medios electrónicos, así como también en el momento en el cual se realizaron las entrevistas en profundidad, lo cual permitió llegar a conclusiones generales del problema de estudio.

Analítico

El método analítico, se aplica en aquellas investigaciones en las cuales se pretenden conocer a profundidad ciertos aspectos del problema de estudio, pero sectorizando los mismos con el fin de obtener un estudio detallado de cada una de las partes que conforman el todo, y en base a ello tener un conocimiento más profundo del problema de estudio. Es un método propio de investigaciones documentales y cualitativas, en el cual se efectúa un estudio profundo de obras literarias, leyes opiniones o entrevistas realizadas a profundidad, a los efectos de tener un conocimiento profundo y que permita obtener conclusiones bien de carácter general o particular sobre el tema de estudio investigado (Ruiz, 2019)

Del análisis de la cita anterior se evidencia la importancia de este método, ya que va a permitir dar un enfoque más profundo del tema investigado, ya que se apreciará un estudio más completo sobre los distintos ángulos de la realidad analizada.

Sintético

Este método se aplica en todas aquellas investigaciones de carácter documental, que presentan un amplio contenido bibliográfico y se hace necesario efectuar una reducción de cuáles son los autores más importantes que tienen una vinculación específica con el tema de estudio. Es aquel método que pretende efectuar una reducción de la bibliografía contemplada para una investigación determinada, pretende seleccionar las obras bibliográficas y decantarse por aquellas que poseen una mayor pertinencia sobre el tema de estudio, este método se utiliza principalmente en aquellas investigaciones que poseen mucha información pertinente sobre el tema investigado. (Romero, 2018)

Técnicas e instrumentos para la recolección de datos

Entrevista

En la presente investigación como técnica esencial se aplicó la entrevista, la cual permitió obtener la opinión de especialistas en el área de estudio, para en virtud de esa información recabada en la entrevista efectuada a profundidad, poder obtener conclusiones generales al final del presente estudio. En la presente investigación, se entrevistaron a dos peritos informáticos así como también a dos jueces de garantías penales, con el fin de hoy analizar la protección de la identidad por medios electrónicos.

Operacionalización de las variables

Variable Independiente

Apropiación de datos a través de medios electrónicos

Variable dependiente

A usuarios de banca virtual.

Entrevistas

Entrevista N° 1

Dr. Carlos Churta Rodríguez, Juez de Garantías Penales del Guayas

¿A su criterio la apropiación de datos electrónicos puede vulnerar los derechos económicos de la víctima?

Dentro del ordenamiento jurídico ecuatoriano, es una de las causas más comunes por medio de los cuales se sustraen cantidades importantes de dinero a los usuarios de la banca electrónica, en este sentido, se hace necesario que existe una mayor capacitación al usuario, quien es la mayoría de los casos es víctima de ese tipo de delitos por desconocer inclusive cómo mantener el secreto sus datos personales, que están vinculados a su cuenta bancaria.

¿Considera usted que las nuevas tecnologías facilitan la sustracción de datos personales y la comisión de delitos electrónicos?

Sí, en este aspecto estoy totalmente de acuerdo, pero con esto no estoy señalando que las nuevas tecnologías sean perjudiciales, lamentablemente ha existido en mi opinión una migración de esos delitos comunes que tradicionalmente se cometían como las estafas hacia el campo electrónico, en este sentido en mi opinión soy del criterio que se requiere que el Estado conjuntamente con las instituciones privadas y públicas como la banca, capaciten un poco más al usuario a los efectos de evitar ser víctima de este tipo de actos delictuosos.

¿Considera usted que en el derecho comparado se encuentra mejor desarrollado legalmente la apropiación de datos por medios electrónicos que en Ecuador?

Sí es importante, en este sentido que el legislador ecuatoriano efectuó un análisis de la forma cómo se encuentra desarrollada la Protección de Datos en otros países, un ejemplo de ello lo observamos acá en el vecino país de Colombia, donde se establecieron importante reforma legislativa en esta materia que han generado sí cifras y positivos ya que se han disminuido los delitos cometidos por

medios electrónicos. En este sentido, producto que las cifras de este tipo de delito en el ordenamiento jurídico ecuatoriano aumentan año a año, se hace necesario valernos de experiencias de países con el caso de Colombia para poder disminuir estos índices delictivos.

¿Considera usted que la banca virtual está blindada contra ataques electrónicos?

Honestamente considero que la banca virtual de acuerdo a la experiencia en el Ecuador, ha sido construida de una manera bastante sólida y aquí son casi nulos los ataques que ha podido recibir y que han resultado exitosos, el problema se presenta generalmente y cuando el usuario no tiene una seguridad vinculada a sus datos, no tiene el resguardo necesario y mediante actividades como el phishing, mediante software que ha insertado a través de correos electrónicos se obtienen los datos para acceder a la banca virtual allí, está el detalle de este tipo de situaciones.

¿Considera usted que el usuario recibe una capacitación suficiente por parte de las entidades bancarias?

No y allí precisamente creo que está uno de los principales problemas que sucede, porque el usuario acude a aperturar una cuenta bancaria y recibe generalmente una breve charla vinculada sobre lo que es la banca online, se le dan algunos detalles pero no existe una capacitación profunda y no se evidencia por parte del Banco ser lo suficientemente asertivo para que las personas entiendan los riesgos de no tener guardados con seguridad lo que son las claves y contraseñas para acceder a la banca online así como también el hecho de no dejar grabadas claves y contraseña en los ordenadores así como también en cada uno de los exploradores mediante los cuales se puede acceder a la banca virtual.

¿Considera usted que la banca virtual es una necesidad en la actualidad?

Sí totalmente y debe seguirse utilizando, en este sentido lo que sí considero y que se deben dictar políticas públicas para capacitar al usuario en la utilización de la banca virtual y evitar de esta manera ser víctima de algún tipo de hecho punible que lesionen su actividad patrimonial.

¿Considera usted que en la actualidad la apropiación de datos por medios electrónicos queda impune en el ordenamiento jurídico ecuatoriano?

En la mayoría de los casos ocurre porque no existen investigaciones suficientes así como tampoco existe desde el punto de vista de investigación, los organismos que posean las herramientas necesarias para determinar la traza del dinero que ha sido sustraído por parte de una persona, lamentablemente es bastante complejo la persecución de este tipo de delito ya que se realizan desde la clandestinidad.

¿Existen instituciones del Estado que velen por la protección de los datos personales de la ciudadanía?

En mi opinión no, porque no se observa de parte del Estado políticas públicas que efectúen por ejemplo campaña asertiva para capacitar al usuario de la banca virtual y evitar de esta manera que se produzcan este tipo de situaciones que al final lo terminan perjudicando y que la mayoría de los casos el usuario pierde su dinero, ya que se determina que hubo un acceso normal a su banca virtual, ya que se utilizaron sus usuario y contraseña y al final la víctima de este delito termina teniendo la culpa por no tomar las medidas de seguridad necesarias para evitarlo.

¿A su criterio la gran mayoría de los fraudes que se cometen por medios electrónicos se realizan con el fin de causar un daño patrimonial a la víctima?

En este tipo de situaciones, puedo señalar que la mayoría de los casos el fraude se comete con el fin de causar un daño patrimonial, de efectuar una transacción en nombre de la persona, o una transferencia con el fin de obtener cantidades económicas de la víctima.

¿Considera usted pertinente la inclusión de la apropiación de datos por medios electrónicos como un delito dentro del Código Orgánico Integral Penal?

Totalmente, porque en muchas oportunidades existen ciertas situaciones que quedan impunes, a consecuencia de que no se encuentra tipificada textualmente la apropiación de datos por medios electrónicos como un delito dentro de la legislación penal ecuatoriana.

¿Se tutelan los derechos de las víctimas de una manera adecuada en este tipo de delito? Responda si o no.

No

Entrevista N° 2

Dr. José Jiménez Velema, Juez de Garantías Penales del Guayas

¿A su criterio la apropiación de datos electrónicos puede vulnerar los derechos económicos de la víctima?

Sí, este sentido puedo señalar desde mi experiencia, que en la mayoría de los casos la apropiación de datos electrónicos se realice con el fin de causar un daño patrimonial, en otras oportunidades a los fines de obtener datos y dañar la reputación de una persona, ocurre frecuentemente pero cuando efectúas cara a cara una comparación te pudiera decir que más del 80% de los casos lo que busca es causar un perjuicio económico en favor de quien cometa el delito, o en favor de un tercero que está vinculado a la persona que comete el hecho delictual.

¿Considera usted que las nuevas tecnologías facilitan la sustracción de datos personales y la comisión de delitos electrónicos?

En este sentido, puedo señalarte que desde un ángulo pudiéramos analizar que las nuevas tecnologías, facilitan que existan delitos electrónicos, pero el problema no está ligado a las nuevas tecnologías, está ligada que no se ha dado respuesta desde el punto de vista legislativo para sancionar este tipo de situaciones, porque las nuevas tecnologías en mi opinión, han sido positivas en todos los aspectos inclusive en el ámbito bancario. Ahora bien, considero que el derecho y así como también los órganos de investigación deben estar a la par de estas nuevas tecnologías con el fin de que no sucedan hechos punibles que vulneren los derechos de la ciudadanía y dentro de ellos los de los derechos económicos.

¿Considera usted que en el derecho comparado se encuentra mejor desarrollado legalmente la apropiación de datos por medios electrónicos que en Ecuador?

Sí totalmente, de acuerdo existen países como España países inclusive vecinos como en el caso de Colombia, en el cual ha existido un mayor desarrollo legislativo y un estudio profundo acerca lo que es la apropiación de datos, por medios electrónicos, situación que en el Ecuador vemos que estamos como bastante rezagados y se hace necesario que desde el punto de vista legislativo, se tomen las medidas necesarias para sancionar ese tipo de delitos.

¿Considera usted que la banca virtual está blindada contra ataques electrónicos?

La banca virtual ecuatoriana, no ha presentado mayores fallas al respecto considero que más ha sido el descuido de los usuarios, lo que ha permitido que ciertos hackers mediante software especializado, correos electrónicos enviados se aprovechan de las claves usuario que se encuentran establecidas en cada uno de los ordenadores de las víctimas, pero hasta los momentos no te pudiera decir que existido un ataque cibernético, en contra de la banca virtual que haya evidenciado su vulnerabilidad en los de en el ambiente ecuatoriano.

¿Considera usted que el usuario recibe una capacitación suficiente por parte de las entidades bancarias?

En mi opinión, te puedo decir que no inclusive desde el punto de vista personal cuando se apertura una cuenta bancaria sea de ahorro o sea corriente, se le dan algunas nociones muy básicas, de lo que es la banca virtual y cómo utilizarlas, pero no se te da como una capacitación profunda, que indique los riesgos principalmente lo que se le dice al consumidor es que debe tener un cuidado especial con lo que es el usuario y la contraseña, que no sea observado por tercero pero que se le den medidas preventivas al punto de vista de cómo manejar la banca online como proteger de qué archivos abrir de que los archivos no abrir eso honestamente no existe por parte de la banca.

¿Considera usted que la banca virtual es una necesidad en la actualidad?

Totalmente, inclusive sería irracional pensar en estos momentos eliminar la banca virtual con toda la cantidad de beneficios que ellas otorgan a los consumidores, que se puede hacer una transferencia sencillamente desde el celular hoy es algo que es bastante innovador y ha beneficiado a la colectividad.

¿Considera usted que en la actualidad la apropiación de datos por medios electrónicos queda impune en el ordenamiento jurídico ecuatoriano?

En muchas oportunidades ocurre ya que el problema es que no se sanciona hoy el delito de apropiación de datos, por fines electrónicos, entonces eso trae como consecuencia, que se cause un daño patrimonial a las víctimas y en oportunidades el procedimiento para determinar quién es el autor del hecho punible es bastante complejo, ya que son delitos que se cometen desde la clandestinidad

¿Existen instituciones del estado que velen por la protección de los datos personales de la ciudadanía?

En mi opinión, te puedo decir que pareciera que al Estado no le preocupan este tipo de situaciones que afectan a la ciudadanía ya que no existen políticas públicas que evidencien la intención del Estado en la protección de los datos personales de la ciudadanía.

¿A su criterio la gran mayoría de los fraudes que se cometen por medios electrónicos se realizan con el fin de causar un daño patrimonial a la víctima?

Totalmente y la mayoría de ellos se efectúan con el fin de vaciar las cuentas de una persona sin su consentimiento.

¿Considera usted pertinente la inclusión de la apropiación de datos por medios electrónicos como un delito dentro del Código Orgánico Integral Penal?

Totalmente considero que sería un acierto bastante positivo del legislador ecuatoriano el establecer la Protección de Datos por medios electrónicos como un delito dentro del Código Orgánico Integral Penal.

¿Se tutelan los derechos de las víctimas de una manera adecuada en este tipo de delito? Responda si o no.

No

Entrevista N° 3

Ing. Carlos Samuel Alcívar. Perito informático

¿A su criterio la apropiación de datos electrónicos puede vulnerar los derechos económicos de la víctima?

Sí, de hecho es el medio que en la actualidad se utiliza para lesionar la economía de una persona, en mi experiencia como perito informático puedo señalar que el objetivo esencial de la apropiación de datos electrónicos es con el fin de entrar a la banca virtual de la persona y efectuar transferencia o transacciones en perjuicio del titular de la cuenta.

¿Considera usted que las nuevas tecnologías facilitan la sustracción de datos personales y la comisión de delitos electrónicos?

Sí, ya que puedo señalar que ha existido una migración de esa delincuencia tradicional que operaba de una manera directa persona a persona, y gracias a estas nuevas tecnologías, a la interacción a las nuevas aplicaciones muchos de todos delincuentes se han perfeccionado y han migrado hacia la parte electrónica

e informática, creando de esta manera ciertas conductas delictuales. Ahora bien es importante señalar que las nuevas tecnologías no son malas, ni son creadas con ese fin, lastimosamente hay personas que le dan una utilidad distinta para la cual fueron creadas y ello debe ser sancionado perfectamente por el legislador.

¿Considera usted que en el derecho comparado se encuentra mejor desarrollado legalmente la apropiación de datos por medios electrónicos que en Ecuador?

Sí, porque ya hay mayor experiencia, lamentablemente en Ecuador el legislador no le ha dado la importancia o la connotación que requieren este tipo de delitos en consecuencia, se producen de una manera más fácil, ya que no existen sanciones fuertes para los responsables de este tipo de actos.

¿Considera usted que la banca virtual está blindada contra ataques electrónicos?

Honestamente desde mi experiencia, puedo decir que la banca virtual ecuatoriana posee niveles de seguridad importantes, ya que en la actualidad no existen hechos que demuestren que si han realizado ataques cibernéticos y han sido exitosos, el problema se presenta es con el descuido de los titulares de la banca en exponer sus claves o contraseñas, y dejarlas guardadas en su explorador y en este caso si se envía un correo con un gusano perfectamente puede robar esta información.

¿Considera usted que el usuario recibe una capacitación suficiente por parte de las entidades bancarias?

No, y esto es uno de los principales errores, porque hay que señalar también que la mayoría de los usuarios, inclusive la mayoría de los que son víctimas de delitos informáticos, son personas que no poseen una capacitación, son personas de

mediana edad los jóvenes ya cuentan inclusive con antivirus y saben manejar más las plataformas digitales.

¿Considera usted que la banca virtual es una necesidad en la actualidad?

Sí totalmente inclusive las ventajas son enormes sería un error retroceder lo que sigue que se hace necesario que existan existe una mayor protección desde el punto de vista tecnológico así como también un marco legal que respalde cualquier tipo de delitos en contra de la banca virtual.

¿Considera usted que en la actualidad la apropiación de datos por medios electrónicos queda impune en el ordenamiento jurídico ecuatoriano?

En oportunidades, sucede que no se realizan las denuncias en la vía penal generalmente queda en el trámite que se efectúa ante el banco que en oportunidades se le da respuesta a la persona y en otras oportunidades sigue si la víctima no acude a alguna instancia judicial y queda impune.

¿Existen instituciones del estado que velen por la protección de los datos personales de la ciudadanía?

En mi experiencia, te puedo decir que no hay un órgano administrativo que tutele la Protección de Datos personales de la ciudadanía de una manera efectiva salvo las instituciones judiciales creo que aparte de ello no existe.

¿A su criterio la gran mayoría de los fraudes que se cometen por medios electrónicos se realizan con el fin de causar un daño patrimonial a la víctima?

Totalmente y creo que hice referencia a ello dentro de la primera pregunta, el delito electrónico tiene como fin en la gran mayoría de los casos obtener un beneficio patrimonial de la víctima.

¿Considera usted pertinente la inclusión de la apropiación de datos por medios electrónicos como un delito dentro del Código Orgánico Integral Penal?

Sí porque se hace necesario que sí que exista un blindaje desde el punto de vista legislativo como lo existe en Colombia, a los fines de sancionar este tipo de actuaciones que lesionan al patrimonio de una persona.

¿Se tutelan los derechos de las víctimas de una manera adecuada en este tipo de delito? Responda si o no.

No

Entrevista N° 4

Ing. Mauro Ernesto Segura Morales. Perito informático

¿A su criterio la apropiación de datos electrónicos puede vulnerar los derechos económicos de la víctima?

Sí y en este punto estoy totalmente de acuerdo, porque al efectuar un análisis de la mayoría de las situaciones en las cuales se obtienen datos electrónicos de terceras personas, el fin es causar una lesión patrimonial en la mayoría de las de los casos, cuando se inserta un virus en la PC de una persona se hace con el fin de causar un daño, pero principalmente patrimonial, no totalmente ya que en oportunidades se quiere también obtener información para otros fines pero el principal es el patrimonial.

¿Considera usted que las nuevas tecnologías facilitan la sustracción de datos personales y la comisión de delitos electrónicos?

Sí porque es que precisamente la sustracción de datos es un delito electrónico y se materializa a través de las nuevas tecnologías, es imposible por ejemplo que se cometa un delito electrónico mediante una estafa tradicional, pero es importante señalar en este aspecto no denigrar de las nuevas tecnologías porque ya han sido más beneficiosas lamentablemente hay personas que la utilizan para un fin distinto para el cual está diseñado.

¿Considera usted que en el derecho comparado se encuentra mejor desarrollado legalmente la apropiación de datos por medios electrónicos que en Ecuador?

Sí existen países como el caso de Colombia que desde el punto de vista legislativo, han tenido un mayor desarrollo de la profesión de datos por medios electrónicos, que el Estado ecuatoriano que se ha quedado un poco rezagado en este sentido.

¿Considera usted que la banca virtual está blindada contra ataques electrónicos?

A grandes rasgos no tengo un conocimiento de la forma como puede estar encriptado la banca virtual en el Ecuador, pero puedo señalar que no ha existido escándalo que demuestren que se ha vulnerado la banca virtual por ataque cibernético.

¿Considera usted que el usuario recibe una capacitación suficiente por parte de las entidades bancarias?

No y precisamente allí está el error, porque por falta de capacitación, por no tener conocimiento necesario en materia de seguridad bancaria, ocurren este tipo de situaciones que termina lesionando el patrimonio de una persona.

¿Considera usted que la banca virtual es una necesidad en la actualidad?

Sí es que la banca virtual de la actualidad se ha convertido en una forma muy práctica de efectuar operaciones bancarias, ahora lo que sí es importante es que las instituciones bancarias deben capacitar al cliente e inclusive el Estado los fines de vista como responsable de la tutela de los derechos del ciudadano, debe establecer capacitaciones políticas públicas y a través de los medios masivos de las redes sociales, establecer un conjunto de indicaciones para evitar este tipo de delito electrónico.

¿Considera usted que en la actualidad la apropiación de datos por medios electrónicos queda impune en el ordenamiento jurídico ecuatoriano?

En la mayoría de los casos sí, porque no existen las denuncias en oportunidades se efectúa la denuncia y no existe el trámite necesario salvo cuando son de una

cuantía bastante alta, pero cuando es una cuantía media o ínfima, a criterio muchas veces de la víctima gasta más en un proceso judicial que lo que perdió.

¿Existen instituciones del Estado que velen por la protección de los datos personales de la ciudadanía?

Salvo los entes judiciales no hay entes administrativos que de verdad efectúen un seguimiento a lo que es la Protección de Datos personales.

¿A su criterio la gran mayoría de los fraudes que se cometen por medios electrónicos se realizan con el fin de causar un daño patrimonial a la víctima?

Sí o sea en la gran mayoría de casos es para cometer un daño patrimonial en beneficio propio o de un tercero.

¿Considera usted pertinente la inclusión de la apropiación de datos por medios electrónicos como un delito dentro del Código Orgánico Integral Penal?

Sí es importante que el legislador ecuatoriano tenga una mayor contundencia e incluya la legislación penal la Protección de Datos por medios electrónicos para de esta manera brindar una mayor seguridad a la ciudadanía

¿Se tutelan los derechos de las víctimas de una manera adecuada en este tipo de delito? Responda si o no.

No

Capítulo III: Análisis de los resultados

Los resultados de la presente investigación que ha tenido como fin el estudio de la apropiación de datos a través de los medios electrónicos a usuarios de la banca virtual, en primer lugar desde el punto de vista doctrinal, es importante destacar que en el Ecuador y especialmente la ciudad de Guayaquil se ha evidenciado la necesidad de contemplar medidas para tutelar la identidad por medios electrónicos, ya que no existe una normativa que de manera expresa proteja este derecho y sancione a aquellas personas que cometan delitos que por vía electrónica sustraigan la identidad o datos personales de una persona, con el fin de utilizar su banca virtual.

De acuerdo a lo anterior es importante señalar que ha existido múltiples investigaciones, en las cuales se ha efectuado el estudio del delito de apropiación fraudulenta por medio electrónico, situación que demuestra que de manera progresiva este tipo de delitos ha venido aumentando en el Ecuador y especialmente en la ciudad de Guayaquil, causando de esta manera una lesión patrimonial a las víctimas de este delito, las investigaciones analizadas dentro del presente estudio coincidieron en el hecho que este tipo de delito es bastante común, y ello se debe principalmente a que las personas no tienen un conocimiento de los riesgos que implica la banca virtual, la mayoría de las personas se centran en las ventajas que tiene este tipo de banca, que son muchísimas pero no toman las medidas preventivas en relación a los riesgos que se corren, y la lesión patrimonial que puedes sufrir, sí sus datos personales como claves y contraseñas para utilizar en este tipo de bancas son obtenidas por terceros.

Otro de los elementos en los cuales coincidieron las investigaciones previas, que se han dedicado al estudio del delito de apropiación fraudulenta por medios electrónicos, es que el Código Orgánico Integral Penal tiene múltiples falencias y se hace necesario que el legislador ecuatoriano, efectúe una revisión a los fines de evitar la comisión de delitos electrónicos mediante la apropiación de datos, ya que en muchas oportunidades delitos que son cometidos por esta vía son de difícil sanción, porque no se adecuan a ciertos parámetros de la norma, situación que se ocurre en el derecho comparado, en consecuencia, en

futuras modificaciones o adecuaciones de estos delitos, en el Código Orgánico Integral Penal, se hace necesario revisar el derecho comparado.

Ahora bien, desde el punto de vista doctrinal se puede señalar que muchos autores sostienen que la protección de datos es un mecanismo necesario para evitar que una información que pertenece a la esfera privada de una persona por seguridad, pueda caer en manos de terceros que pretendan lesionar de manera intencional su patrimonio, ya que se ha demostrado que la mayoría de los casos la apropiación de datos busca ese fin, hay un porcentaje muy bajo que busca obtener información de la vida privada de la persona, para exponerse la al público, pero ya este tipo de situaciones constituye una minoría.

En relación a la primera pregunta de la entrevista, vinculada al hecho si la apropiación de datos electrónicos puede vulnerar los derechos económicos de la víctima, se desprende del análisis de las respuestas de los entrevistados, que los datos personales por la naturaleza que ellos poseen, forman parte de la esfera privada de una persona, ya que ellos obtienen información que el individuo ha decidido reservar para sí, porque solo son de su incumbencia y allí entran todos aquellos que tienen una relación con la banca virtual, y que por ser sus ahorros su dinero, y formar parte de su patrimonio, la información que está relacionada con ello es de naturaleza privada.

En relación a la segunda pregunta, vinculada al hecho que si las nuevas tecnologías facilitan la sustracción de datos personales y la comisión de delitos electrónicos, al efectuar un análisis de las respuestas de los entrevistados se puede analizar que en la actualidad es bastante común el fraude que se produce a través de medios electrónicos con el fin de sustraer dinero de las cuentas de una persona, los más comunes son la clonación de tarjetas de crédito y débito así como también el phishing, que consiste en enviar correos electrónicos a una persona, que al abrirlos se liberan ciertos gusanos que roba la información que tiene la persona en su computadora, en consecuencia, dentro de toda esa información general que se obtiene en se encuentran claves y contraseñas que van a permitir la utilización de la banca virtual por parte de un tercero, con el fin de causar un perjuicio económico al titular de la cuenta.

En relación a la tercera pregunta, vinculada a verificar si en el derecho comparado se encuentra mejor desarrollado legalmente la apropiación de datos por medios electrónicos que en Ecuador, de análisis de las respuestas de los entrevistados se demuestra que desde el punto de vista internacional, han existido normativas que tienen como fin la tutela de la víctima ante la comisión de delitos informáticos, dentro de las cuales se puede señalar el convenio sobre la delincuencia del año 2001 efectuado en Budapest, donde insta a los países europeos al hecho de adoptar medidas de carácter legislativa que tengan como fin sancionar la interceptación ilegítima de datos informáticos, ya que la mayoría de los casos, cuando sucede este tipo de acciones, existe la mala fe del sujeto activo de esta acción, que pretende crear un daño a la víctima, en oportunidades puede ser de carácter moral, porque pretende exponer ciertas informaciones privadas de la persona ante la colectividad, pero también ocurre que se realiza con el fin de obtener información vinculada a las cuentas de una persona, con el fin de poder utilizar su banca virtual.

En el ámbito del derecho comparado es importante mencionar que se pudo efectuar un análisis de la ley 1273 del año de 2009 en Colombia, ya que ella trajo como consecuencia que esté país efectuar una modificación del Código Penal, ajustándolo a las nuevas tecnologías y a los delitos informáticos creando de esta manera un nuevo bien jurídico tutelado, el cual es la protección de la información, los datos permitieron determinar que el Estado colombiano, gracias a esta disposición legislativa, pudo reducir el volumen de delitos por vía electrónica, ya que antes de crear esta esta disposiciones legislativas estos delitos año a año iban aumentando, y desde el momento en que fue aprobada, al año posterior se evidencio un descenso gradual en la comisión de este tipo de delitos.

En el caso colombiano se pudo demostrar que se posee una banca virtual bastante segura, y que de forma progresiva la mayoría de las personas utilizan este canal en relación a la banca tradicional, salvo personas de edad avanzada las cuales ya por la costumbre de toda una vida realizan operaciones bancarias de forma presencial, y debido al desconocimiento de las nuevas tecnologías

siguen utilizando ese tipo de banca, que inclusive de punto de vista económico, la banca virtual ha sido beneficiosa para el sector bancario, porque ha permitido la reducción de las sedes bancarias a nivel nacional.

Ahora bien la investigación permitió evidenciar, que por ejemplo en Colombia ya desde el año 2008 se había ratificado el convenio de ciber delito en Budapest a través de la ley 928 partiendo del criterio que era de carácter prioritario contemplar políticas penales que tuvieron como fin proteger a la sociedad frente a los delitos cibernéticos, así como también se requería el fomento la de la cooperación internacional en materia de delitos electrónicos.

En relación a la cuarta pregunta, relacionada con el hecho que si la banca virtual está blindada contra ataques electrónicos los entrevistados manifestaron que no se han observado ataques con éxito a la banca virtual ecuatoriana, lo que demuestran que posee niveles de seguridad importantes, ya que se ha demostrado que en la mayoría de los casos en los cuales las personas han sufrido algún tipo de vulneración de sus cuentas, ha sido por descuido del titular por entregar claves y contraseña a terceras personas.

En relación a la quinta pregunta, vinculada al hecho que si el usuario recibe una capacitación suficiente por parte de las entidades bancarias, los entrevistados estuvieron de acuerdo en el hecho que la mayoría de las personas que son víctimas de cualquier tipo de delitos informáticos, es una consecuencia de no tener la capacitación necesaria, ya que la mayoría de los casos son personas de mediana edad y avanzada edad, que no conocen el funcionamiento de la banca virtual, el porcentaje es mucho menor en jóvenes que tienen ya una experiencia o se encuentran familiarizados con cualquier tipo de plataformas digitales.

En relación a la sexta pregunta, vinculada al hecho que si la banca virtual es una necesidad de la actualidad, del análisis de las respuestas de los entrevistados, todos concluyeron que a pesar de que la banca virtual implique algunos riesgos para los titulares de las cuentas, las ventajas son muy superiores y sería un error volver al pasado, después de los grandes avances que se han hecho en materia tecnológica, lo que sí debe existir es una mayor protección desde el punto de vista tecnológico, de cada una de las instituciones bancarias

así como también un marco jurídico que sancione a aquellas personas que cometan algún tipo de delito en contra de la banca virtual.

En relación a la séptima pregunta, vinculada al hecho si en la actualidad la apropiación de datos por medios electrónicos queda impune, en el ordenamiento jurídico ecuatoriano, al efectuar un análisis de las respuesta a los entrevistados, manifestaron que existen oportunidades en las cuales no se realizan las denuncias en la vía penal, por cuánto solamente se limitan a efectuar una reclamación en sede bancaria y dependiendo de la respuesta la víctima tiene la potestad de acudir a la instancia judicial, ello depende mucho del monto de la cuantía ya que si es ínfima la víctima prefiere dejar que se pierda ese dinero en lugar de reclamar.

En relación a la octava pregunta, vinculada al hecho que si existen instituciones del Estado que velen por la protección de los datos personales de la ciudadanía, los entrevistados fueron del criterio, que no existe un órgano que posea la competencia administrativa que tutele de manera efectiva la protección de datos personales, solamente le queda el ciudadano común cuando acude la institución bancaria y recibe una respuesta negativa acudir a la instancia judicial caso contrario el delito queda impune.

En relación a la novena pregunta, vinculada al hecho que si la gran mayoría de los fraudes se cometen por medios electrónicos tienen como fin causar un daño patrimonial a la víctima, la mayoría de los encuestados fue el criterio que el fin esencial que posee un delito electrónico, es obtener un beneficio patrimonial en beneficio de un tercero o del autor del hecho punible puede tener también otras razones pero ya en un menor porcentaje.

Por último, una de las preguntas que posee una mayor relación con el contenido íntegro de la presente investigación, es la vinculada al hecho se considera pertinente la inclusión de la apropiación de datos por medios electrónicos como un delito dentro del Código Orgánico Integral Penal, en este caso los entrevistados de forma conjunta manifestaron que sí es una necesidad en la actualidad que se le den una mayor fortaleza a la seguridad de la de sancionar ese tipo de delito como lo es por ejemplo en Colombia a los fines de tutelar los derechos económicos de la sociedad.

La investigación permitió determinar desde el punto de vista doctrinal, que la banca virtual en la actualidad ha sido bastante ventajosa, producto que ha hecho que las transacciones bancarias se puedan realizar de una manera más sencilla, al comparar la forma como se efectuaban hace 20 ó 30 años, era casi imposible efectuar una transferencia de grandes cantidades de dinero, que pudieran hacerse efectivas en un momento, inclusive se está tan avanzado que se pueden realizar transferencia de un país a otro, gracias a las innovaciones de la banca virtual, mejorando de esta manera el comercio entre particulares, y en la actualidad se ha convertido en una necesidad producto de la evolución de los sistemas financieros así como también de las nuevas generaciones, que han adoptado ya la banca virtual, como una manera práctica de efectuar transacciones que se pueden realizar desde su propio celular.

En relación a las entrevistas realizadas se puedo demostrar, que la apropiación de datos electrónicos vulnera de una manera directa los derechos económicos de la víctima, así como también que las nuevas tecnologías han servido para que delincuentes comunes hayan migrado a este sector, destacando muchos de los entrevistados fueron del criterio que las nuevas tecnologías por esta causa, no pueden ser consideradas como negativas, porque efectuando un balance han sido positivas, pero lastimosamente personas han desnaturalizado su función.

En este mismo sentido las entrevistas de forma general mantuvieron una concordancia con el desarrollo doctrinal, en el cual se evidenció que existe un avance en la legislación colombiana vinculada a la protección de datos, ya que los entrevistados fueron del criterio que el vecino país, ha mostrado un desarrollo legislativo bastante avanzado en esta materia, que e inclusive desde el 2008 ya se había adoptado en la legislación interna, con el fin de lograr la protección de los datos de las personas, reduciéndose de esta manera, el índice delictivo desde el punto de vista informático.

De igual forma se pudo señalar que en el Ecuador, el sistema bancario no ha presentado ataques que hayan demostrado su vulnerabilidad, ya que la mayoría de casos, que existe una sustracción de fondos a los particulares, no ocurre por factores inherentes a la banca, si no al hecho que los particulares son

víctima directa de correos electrónicos y proceden a efectuar transferencia de los fondos de la víctima a terceros.

Se pudo demostrar, también que los usuarios al efectuar una contratación con el banco no reciben una capacitación suficiente por parte de estas entidades, situación que trae como consecuencia, que desconocen muchas veces los riesgos de no tomar las medidas de seguridad necesarias, ya que se ha demostrado que en la actualidad la banca virtual es una necesidad. En este sentido, se requiere que exista una mayor capacitación de las entidades bancarias a los particulares así como también por parte del Estado, a los fines de poder capacitar y divulgar por ejemplo cuando un correo electrónico no es legítimo, y no proviene de una institución bancaria, ya que de esta manera se evitaría que muchas personas fueran víctimas de este tipo de delitos.

En este mismo sentido, es importante señalar que de una manera amplia que los entrevistados señalaron, que en el Estado ecuatoriano hace falta instituciones que velen por la ciudadanía a los efectos de tutelar su derecho a la protección de datos, y que terminen siendo víctimas de su patrimonio a consecuencia de terceras personas, concluyendo la mayoría de los entrevistados, que se hace necesario la inclusión de la apropiación de datos por medios electrónicos, como un delito dentro del Código Orgánico Integral Penal a los efectos que en el Ecuador, puedan disminuir los niveles de este tipo de delitos, que se evidencian que con el paso del tiempo van en ascenso, de esta manera pueda ocurrir como sucedió en Colombia, que a partir de aprobada la normativa que sancionaba este tipo de delitos de una manera bastante firme existió paulatinamente una disminución de ellos.

Capítulo IV: Propuesta

Exposición de motivos

Las nuevas tecnologías se han convertido en el aliado perfecto del hombre moderno, porque le han facilitado muchas tareas así como también tienen múltiples ventajas en todos los ámbitos de la vida, en la salud en las comunicaciones y sobre todo en el elemento económico, porque ha permitido qué aspectos como el comercial se efectúen de una manera más rápida, en consecuencia, se puede señalar que los medios electrónicos han sido bastante positivos en el desarrollo de la humanidad.

Ahora bien, el problema de las nuevas tecnologías, es que han traído como consecuencia que muchos delincuentes tradicionales, que comúnmente operaban en otros ámbitos hayan migrado a las nuevas tecnologías y han buscado ciertas maneras de cometer hechos ilícitos en contra de terceros, utilizando medios electrónicos a los fines de causar una lesión patrimonial en provecho propio o de un tercero en contra de una víctima.

En consecuencia, se hace necesario que se deben sancionar todas aquellas conductas que tengan como fin la apropiación de datos por medios electrónicos, ya que se ha demostrado que es una vía que se utiliza con el fin de lesionar patrimonialmente a una persona así como también su derecho a la intimidad. Por tal motivo, se hace necesario que el legislador ecuatoriano establezca sanciones a los fines de castigar a las personas que realicen este tipo de conductas, tomando como referentes normas de países que tenían este problema y a partir de la aprobación de normativas que contemplan el delito de apropiación de datos por medios electrónicos, las estadísticas de este tipo de delitos disminuyeron.

Justificación

La presente propuesta se justifica, en el hecho que se ha evidenciado que gracias a las nuevas tecnologías a aumentado la apropiación de datos por medios electrónicos en el Ecuador, en consecuencia, se requiere que el legislador que tiene como norte garantizar los derechos y garantías de la ciudadanía en general, adecue el Código Orgánico Integral Penal y contemple

de una manera directa el delito de apropiación de datos por medios electrónicos, tal como lo efectuó el legislador colombiano en el año 2009, mediante la ley 1273 que efectuaba una modificación al Código Penal de ese país.

Se hace necesario que el Código Orgánico Integral Penal consagre la figura del delito de apropiación de datos por medios electrónicos, ya que existen artículos de dicho código que no denotan de una manera tajante este delito, situación que trae como consecuencia que muchos operadores de justicia, por no estar contemplado de manera expresa, existen situaciones en las cuales se pudiera aplicar otra disposición normativa establecida en el COIP y sancionar este tipo de conductas, pero muchos jueces se abstienen de aplicar ciertas normas en virtud del principio de la tipicidad, que establece que la que el acto o el hecho ilícito realizado por el hombre, debe adecuarse perfectamente al tipo jurídico que contempla la norma, en consecuencia, muchas situaciones en las cuales existe una apropiación de datos por medios electrónicos quedan impune en el ordenamiento jurídico ecuatoriano.

Objetivos

Establecer dentro del Código Orgánico Integral Penal el delito de apropiación de datos por medios electrónicos.

Garantizar a la ciudadanía su derecho a la intimidad así como también a su patrimonio.

Alcance y Beneficios

La presente propuesta, posee un alcance general por cuanto no va dirigida a un sector específico de la población que se beneficiaría de ella, sí no a cualquier persona que sea víctima de la apropiación de sus datos personales por medios electrónicos, en consecuencia, se puede señalar que la ciudadanía de manera amplia tendrá mayor seguridad de sus datos personales por medios electrónicos y si un tercero realiza a dicha actividad sería sancionado de conformidad con lo establecido en el Código Orgánico Integral Penal.

Desarrollo

Tomando en consideración:

Que el artículo 1 de la Constitución de la República de Ecuador hace referencia que se está en un Estado constitucional de derecho y de justicia, social en el cual se tiene como fin la tutela de los derechos y garantías de la población y que los órganos del Estado en su totalidad deben tener como centro al ciudadano.

Que el numeral 20 del artículo 66 de la Constitución de la República de Ecuador reconoce y garantiza el derecho a la intimidad personal y familiar.

Que el numeral 19 del artículo 66 de la Constitución de la República de Ecuador hace referencia al derecho que tienen todos los ciudadanos de la protección a sus datos de carácter personal, partiendo del criterio que es un derecho inherente a la persona humana en consecuencia todo lo vinculado a los datos personales forma parte de la esfera íntima de una persona.

Que el Código Orgánico Integral Penal en su sección sexta contempla los delitos contra el derecho a la intimidad personal y familiar, y específicamente el artículo 178 contempla de manera expresa el delito de violación a la intimidad.

Que el capítulo tercero sección tercera del Código Orgánico Integral Penal hace referencia a los delitos contra la seguridad de los activos de los sistemas de información y comunicación, protegiendo de esta manera la interceptación ilegal de datos.

En uso de las facultades que le confiere el numeral seis del artículo 120 de la Constitución de la República de Ecuador. La Asamblea Nacional:

RESUELVE LA MODIFICACIÓN DEL NUMERAL 1 DEL ARTÍCULO 230 DEL CÓDIGO ORGÁNICO INTEGRAL PENAL EL CUAL QUEDARÁ DE LA SIGUIENTE MANERA:

Art. 230.- Apropiación de datos por medios electrónicos.- Será sancionada con pena privativa de libertad de tres a cinco años:

1. La persona que por vía electrónica se aproveche de los datos personales o información vinculada de manera directa a una persona sin el

consentimiento de esta última. De igual manera será sancionada 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.

Conclusiones

La presente investigación tuvo como objetivo general establecer la apropiación de datos por medios electrónicos en el ordenamiento jurídico ecuatoriano, para evitar la vulneración de los derechos económicos de la víctima, de la cual se desprende las siguientes conclusiones:

El capítulo uno de la presente investigación permitió demostrar la importancia de la protección de datos en el ordenamiento jurídico ecuatoriano demostrando, que se requiere una mayor tutela de este derecho por parte del Estado, analizó cómo se encuentra contemplado este delito en Colombia a los fines de permitir en el mediano o corto plazo se puedan establecer dentro del Código Orgánico Integral Penal modificaciones similares que permitan la efectividad de las sanciones en este tipo de delitos, tutelando de esta manera los derechos de muchas víctimas quienes por no existir criterios de manera específica la legislación penal ecuatoriana, no se reconoce la afectación de sus derechos.

El capítulo número dos, contemplo la parte metodológica formada por el conjunto de métodos y técnicas de estudio necesarios para llevar a cabo esta investigación, efectuando para ello cuatro entrevistas a personas que tienen un conocimiento real de la situación actual de la apropiación de datos a través de medios electrónicos para tutela los derechos de los usuarios de la banca virtual, lo cual permitió tener un conocimiento bastante profundo de la realidad actual del problema investigado, demostrando de esta manera que existe la necesidad de incluir en el Código Orgánico Integral Penal y una forma más específica una normativa que tu tele a las víctimas del delito de apropiación de datos por medio electrónico.

El capítulo número tres hizo referencia a los resultados de la investigación los cuales demostraron que se hace necesario que en la ciudad de Guayaquil y en el Ecuador se contemplen medidas con el fin de proteger la identidad por medios electrónicos Por cuanto no existe una normativa que contemple de manera expresa estos derechos y sancionen a los responsables de este tipo de delitos.

Por último el capítulo cuatro de la investigación contempló una propuesta que fue una consecuencia de los resultados de la investigación desde el punto de vista doctrinario así como también de las entrevistas realizadas, lo cual condujo a la necesidad de efectuar una propuesta sobre la modificación del numeral 1 del artículo 230 del Código Orgánico Integral Penal.

Recomendaciones

La presente investigación tuvo como objetivo general establecer la apropiación de datos por medios electrónicos en el ordenamiento jurídico ecuatoriano, para evitar la vulneración de los derechos económicos de la víctima, de la cual se desprende las siguientes recomendaciones:

Se recomienda a las universidades que dicta la carrera de derecho en materia de pregrado hacer un mayor énfasis en el estudio de la importancia de la protección de datos en el ordenamiento jurídico ecuatoriano así como también analizar cómo se encuentra contemplado este derecho en Colombia a los fines de permitir en el mediano o corto plazo se puedan establecer dentro del Código Orgánico Integral Penal modificaciones similares que permitan la efectividad de las sanciones en este tipo de delitos, tutelando de esta manera los derechos de muchas víctimas quienes por no existir criterios de manera específica la legislación penal ecuatoriana, no se reconoce la afectación de sus derechos.

Se recomienda a las universidades así como también a los alumnos que cursan la carrera de derecho, profundizar en investigaciones que se encuentran vinculadas al presente tema, consultando de manera específica a abogados en ejercicio así como también operadores de justicia que tengan un conocimiento profundo Sobre la apropiación de dato a través de medios electrónicos para tutelar los derechos de los usuarios de la banca virtual.

Se recomienda al estado ecuatoriano así como también a la banca pública y privada establecer campañas de orientación al cliente en las cuales se contemplen medidas con el fin de proteger la identidad por medios electrónicos.

Por último se recomienda a la Asamblea Nacional, efectuar una modificación del numeral 1 del artículo 230 del Código Orgánico Integral Penal a los fines de tutelar los derechos de los usuarios de la banca virtual y sancionar aquellas personas que cometan el delito de profesión de datos por medio electrónicos.

Bibliografía

- Chiluisa, D. (2021). *Los delitos informáticos y los vacíos legales que afectan a los ciudadanos*. Guayaquil: UG.
- Ayjon, M. (2019). *Hoy la Protección de Datos de carácter personal en la justicia penal*. Bogotá: JB.
- Balestrini. (2019). *Metodología de la Investigación*. Colombia: Metodos.
- Baquero de la Calle, J. (2018). *Metodología de la Investigación Jurídica*. Quito: CEP.
- Bernal, C. A. (2018). *Metodología de la Investigación* (Tercera ed.). Bogotá, Colombia: Pearson Educación.
- Bueno, E. (2022). *El reto de la banca en la economía digital un desafío organizativo y evolutivo*. México: UIE.
- Campos, C. (2022). *Aplicación práctica y adaptación de la Protección de Datos en el ámbito local*. Bogotá: Wolters.
- Carazo, M. (2021). *El derecho a la protección de datos*. Quito: Jurua.
- Chitalogro, Y. (2022). *Análisis dogmático penal de los delitos de apropiación fraudulenta y estafa cuando son realizados por medios electrónicos en el coip*. Quito: UCE.
- Cianciardo, J. (2021). *El reto de la banca en la economía digital*. Barcelona: Reus.
- Conde, C. (2019). *La protección de datos personales*. Cádiz: Universidad de Cádiz.
- Congreso de Colombia. (2018). *Ley 1928*. Bogotá: D.O . 50.664, julio 24 de 2018.
- Consejo Europeo. (2001). *Convenio sobre la Ciberdelincuencia*. Budapest: Consejo Europeo.
- Davara, L. (2018). *Protección de datos*. México: La Ley.
- Defferary, E. (2019). *Con la banca tenemos que lidiar todos*. Barcelona: Alienta.
- Determan, L. (2017). *Protección global de datos personales*. Madrid: Astrea.
- Ferreira, J. (2019). *Hacia una efectiva protección de los datos en Iberoamerica*. Quito: Defensoria del Pueblo.
- Hernandez, R., Fernandez, C., & Baptista, P. (2014). *Metodología de la investigación*. Mexico: Mc Graw Hill.
- Lefebvre, F. (2022). *Protección de datos*. Madrid: CEP.

- López, J. (2019). *Banca digital y "Fintech"*. Barcelona: Aferre.
- López, J. (2022). *Delito de apropiación fraudulenta por medios electrónicos bajo la modalidad de phishing dentro del marco jurídico ecuatoriano*. Azuay: UA.
- Orellana, M. (2020). *El derecho a la Protección de Datos personales HD cómo garantía del derecho a la privacidad*. Navarra: Thomson.
- Pacheco, A. (2022). *Protección de Datos*. Barcelona: Jurídica.
- Pérez, J. (2022). *Derecho a la Protección de Datos y seguridad de la información*. Madrid: Rama .
- Rebolledo, L. (2020). *Vida privada y protección de datos en la Unión Europea*. Madrid: Dykinson.
- Rodas, P. (2018). *El delito de apropiación fraudulenta por medios electrónicos en la ciudad de Guayaquil*. Guayaquil: UG.
- Romero, L. (2018). *Metodología de investigación jurídica*. Madrid: Ediciones de la Universidad de Castilla -La Mancha.
- Rosales, M. (2022). *Protección de Datos personales*. México: Aqua-ediciones.
- Ruiz, J. (2019). *Metodología de la Investigación Cualitativa*. Bilbao: Deusto.
- Tocora, L. (2022). *Derecho Penal Especial*. Bogota: Ediciones del Profesional.

