SEGURIDAD JURÍDICA DEL COMPRADOR A TRAVÉS DE LA RED SOCIAL FACEBOOK EN COLOMBIA.

CARLOS MAURICIO GELVES OMAÑA
MANUEL RICARDO MANCERA GARCIA
SERGIO ANDRÉS PEREZ PEREZ
JOSE MANUEL RIVERA RAMIREZ

UNIVERSIDAD SIMÓN BOLÍVAR SEDE CÚCUTA
FACULTAD DE DERECHO
PROGRAMA ACADÉMICO DE DERECHO
SAN JOSÉ DE CÚCUTA
2018

SEGURIDAD JURÍDICA DEL COMPRADOR A TRAVÉS DE LA RED SOCIAL FACEBOOK EN COLOMBIA

CARLOS GELVES

MANUEL RICARDO MANCERA GARCIA

SERGIO PEREZ PEREZ

JOSE MANUEL RIVERA RAMIREZ

Proyecto de Trabajo de investigación presentado como prerrequisito para optar título de Abogado

Tutor:
ANDREA AGUILAR BARRETO
Doctora

UNIVERSIDAD SIMÓN BOLÍVAR SEDE CÚCUTA

FACULTAD DE DERECHO

PROGRAMA ACADÉMICO DE DERECHO

SAN JOSÉ DE CÚCUTA

2018

CONTENIDO

Pág.

Lista de anexos

Pag

TITULO

SEGURIDAD JURÍDICA DEL COMPRADOR A TRAVÉS DE LA RED SOCIAL FACEBOOK EN COLOMBIA.

INTRODUCCIÓN

El internet se convirtió en una herramienta necesaria en la vida de los seres humano, es decir, con la evolución y avances de la tecnología y su influencia en todos los ámbitos sociales, se puede afirmar, que este gran avance se ha convertido en una necesidad básica para el hombre; Uno de estos avances que cuenta con una gran importancia en el mundo actual es la compra-venta por perfiles que cualquier persona puede crear con tan solo llenar unos requisitos en los que hay libertad sin ninguna supervisión de veracidad por parte de las redes sociales, especialmente el Facebook, la cual en esta era globalizada ha generado nuevas formas de interrelación entre las personas, relaciones que son relevantes para el mundo jurídico.

Dentro de este universo de relaciones, el Comercio Electrónico a través de Internet se caracteriza por comunicar directamente a las empresas y a los consumidores, por medio de sitios Web de acceso global. Es a través de este medio que se suelen desarrollar contratos de compraventa masificados, es decir, dirigidos a un universo indeterminado de potenciales contratantes, los cuales deciden obligarse sobre la base de ciertos términos y condiciones contractuales preestablecidas por la empresa oferente. (Santander, Carbajal, Silva & Villanueva, 2004).

Con las redes sociales se ha implementado nuevas formas de comercio con el ofrecimiento de bienes y servicios, aunque pareciera que todo son beneficios, lo cierto es que también este nuevo avance "Social Commerce" trae una sociedad de problemas, problemas que juegan con la confianza del usuario por medio de engaño ofrecen en venta productos de supuesto fácil acceso para obtenerlos y un precio cómodo los cuales otros usuarios consumidores proceden a comprar dichos productos, pero al momento de la entrega del producto ya anterior mente pagado se ven en la situación de que ya han sido estafados y no tienen a quien reclamar su garantía o devolución del dinero pues estos perfiles ya fueron eliminados de la red social Facebook.

Rodríguez (2011) afirma: "Los desarrollos de las tecnologías de información y comunicación como las redes sociales generan infinidad de cambios y repercusiones en el comportamiento humano, (…). Como se está adecuando la normatividad en Colombia a este

crecimiento constante de las tecnologías" (p.1). la protección al consumidor es un tema de suma importancia, en la medida que es la base necesaria para toda relación comercial, siendo el instrumento practico mediante el cual se pretende salvaguardar los intereses de las personas, estudiar la reglamentación de protección al consumidor existente para ser manejado con mayor seriedad y preocupación.

Se puede en cierto sentido incentivar la aplicación del comercio en la red social Facebook, una mayor seguridad al igual que generar conciencia de lo que implica la ausencia jurídica entorno a los fenómenos de estafa y mostrar las ventajas que tendrían tanto los consumidores como para los comerciantes la utilización de este medio que cada día esta tan fijado en las personas ya que cuentan con esta aplicación en sus celulares haciendo de este un medio practico para realizar sus actividades comerciales creando una relación con el fin de crear índole segura. Se puede encontrar un gran tema de investigación, dado que tiene un buen tema de impacto mundial y nacional, igualmente tiene un gran campo de acción y no se encuentra completamente desarrollado, de ahí nace la idea de este proyecto de investigación que pretende describir la evolución y el comportamiento de la ley para enfrentar este delito de estafa por medio de la red social Facebook a través de perfiles falsos.

Para concluir que las nuevas prácticas delictivas en Colombia están a la mano de la aplicación de los avances tecnológicos, pero a pesar de esto en Colombia existen las bases legales a partir de las cuales se puede empezar a combatir las diferentes modalidades de delitos informáticos, analizando e interpretando la norma existente para identificar su alcance, obteniendo así elementos de juicio para desarrollar políticas y estrategias en este tema. (Rodríguez, 2011). Esta investigación busco analizar cuál es la condición de indefensión y afectación que lleva la inseguridad jurídica del comprador a través de la red social Facebook en Colombia. Dentro de la metodología se aplicará un paradigma investigativo interpretativo con enfoque cualitativo con un diseño hermenéutico que permitirá dar respuesta a la formulación del problema planteado para este trabajo investigativo, usando la matriz de sobre la norma y jurisprudencia e igualmente un trabajo comparado varias legislaciones y la entrevista a funcionarios de la policía y fiscalía.

1 PROBLEMA

1.1 Planteamiento del Problema

Teniendo en cuenta las posibles falencias que se están presentando en la red social Facebook en el nuevo comercio conocido como "Social Commerce" que está evolucionando en actividades de adquirir productos de manera "sencilla" y rápida, nace la problemática dado a la ausencia jurídica, al no tener un control de la comercialización que garantice la veracidad de los perfiles creados que actúan de manera dolosa afectando de esta manera el patrimonio económico de las personas.

Delitos de todo tipo, desde la suplantación de identidad, hasta situaciones que atentan contra la vida como es la trata de personas y la pornografía infantil, pasando por el narcotráfico y la estafa son realizados con la ayuda de las redes sociales, sin que los usuarios puedan a ciencia cierta, conocer cómo protegerse de este tipo de delitos y en peor de los casos acceder a la justicia para que sea esta la que sancione a quienes comenten estos hechos (Serrano, 2016). La tecnología y sus avances han sido algo muy positivo para mejora la calidad de vida de cientos de individuos, pero igualmente han avanzado los delitos y los malos comportamientos de cientos de estafadores.

"las nuevas formas de comunicación en el mundo no deben estar separadas de las correspondientes reformas y creaciones legales, (…). para que las personas puedan tener opciones y medios dónde acudir para denunciar y protegerse frente a cualquier delito" (Rodríguez, 2011, p.22). Es decir, estos avances han obligado a los legisladores a crear reformas y creaciones legales, nuevas normas que abarquen y contemplen las posibles vulneraciones a los derechos constitucionales y así los usuarios de las redes sociales como el Facebook puedan realizar de forma confiable compra-ventas sin miedo a ser estafados o a caer en manos de perfiles fasos manejadas por ciberdelincuentes.

Hoy en día este tema está en la mira de muchas legislaciones en el mundo y Colombia no ha sido la excepción, Al llegar la tecnología y consigo muchas herramientas prácticas para el hombre, se les han abierto la puerta a muchas conductas antisociales, que afecta a miles

de colombianos que a diarios son víctimas y pareciera que las autoridades competentes no hacen nada para combatir a estos delincuentes.

Se debe entender que en el contexto de la tecnología y las comunicaciones existen unas condiciones de vulnerabilidad para todos los ciber usuarios y la tendencia al riesgo ha generado una reacción a nivel mundial de las autoridades para combatir con estos actos antisociales que atenta contra muchos derechos fundamentales y constitucionales de los Colombianos, por eso se entrara a revisar el trabajo del legislador y las autoridades (CONGRESO, POLICÍA NACIONAL Y FISCALIZA) para generar un trabajo contundente desde sus instituciones logrando impartir justicia ante la eventual violación y la creciente oleada de delitos informáticos en este país. Teniendo en cuenta las posibles falencias que se están presentando lo que se busca es mejorar.

Se debe dar confiabilidad a los usuarios que requieren hacer esta clase de comercio por las redes sociales, de debe estudiar el trabajo de las autoridades y el control que ejercen, indagar si la ley cumple con su objetivo de prevención y además mejorar el nivel de seguridad para crear perfiles en el Facebook, en fin la hipótesis de este grupo de trabajo es puntual en observar la vulneración que viven cientos de usuarios de estas redes sociales que a diario desconfían y son víctimas de los ciberdelincuentes.

1.2 Formulación del Problema

¿Cómo es la eficacia del legislador y las autoridades del Estado colombiano para brindada seguridad jurídica a los usuarios Facebook y así contra restar la estafa que se llevar a cabo a través de la compraventa?

1.3. Objetivos

1.3.1 Objetivo General

Analizar la seguridad jurídica del comprador a través de la red social Facebook en el Estado colombiano.

1.3.1 Objetivos Específicos

* Identificar las garantías del reglamento y de las políticas establecidas por la red social Facebook respecto a la seguridad jurídica para el comprador a través de este medio.

* Comparar el tratamiento de los delitos informáticos en Latinoamérica, en especial el delito de la estafa a través de internet y las redes sociales.

* Indagar la efectividad de las autoridades competentes para contra restar el accionar de los estafadores por medio de la red social Facebook en Colombia.

1.4 Justificación

El objetivo de este trabajo cambiar la visión y brindar un aporte positivo a la seguridad del consumidor y así mejorar el mercado virtual en la red socia Facebook, para que de esta manera no se afecte la economía del consumidor y frenar las estafas que se hacen por medio de engaños a los usuarios de esta red social en Colombia a través de perfiles falsos.

Aun cuando es un tema complejo, se hace interesante investigar sobre la inseguridad jurídica que hoy representa la compra-venta a través de la red social Facebook para cientos de usuarios en Colombia, y es un honor para este grupo de investigación como estudiantes de derecho, profundizar en esta problemática que hace parte de los delitos informáticos. Al entender el delito se debe recordar que el gran Jorge Eliécer Gaitán y el inmolado profesor Alfonso Reyes Echandía, discípulos de la Escuela Positiva del Derecho Penal que lo definieron como el comportamiento humano, atípico, antijurídico y culpable, conminado con

una sanción penal (Téllez, 2007). A si las cosas se deben realizar un trabajo contundente que lleve a la confiabilidad de los consumidores a través de la sanción penal.

Con el desarrollo de las posibilidades de interacción global mediante las tecnologías de información y comunicación, específicamente en el Facebook, las personas y organizaciones han quedado expuestas por la vulnerabilidad de estos sistemas de manejo de información, la falta de medidas de prevención y cuidado al contante progreso y peligro de la delincuencia informática, por eso la importancia de conocer dicho contexto, estar consciente de las consecuencias de los delitos informáticos y la normatividad aplicable en el país, para así encontrar posibles respuestas o formas de prevención y tratamiento.

Colombia frente a estos dos fenómenos actuales, uno positivo como lo es el avance global de la tecnología de información y comunicaciones, y el otro negativo como lo son los delincuentes y delitos informáticos, como algunos gobiernos de países de todo el mundo que han venido tomando conciencia de la creciente amenaza y han comenzado a implementar avances tecnológicos.

2 MARCO REFERENCIAL

2.1 Antecedentes

Los siguientes antecedentes investigativos utilizados como objeto de estudio en este proyecto de investigación, permitirán entender el contexto de la problemática y hacer una descripción de los aportes más relevantes de otros autores sobre los mecanismos alternativos de solución de conflictos, y sobre el impacto social que se reflejan los centros de conciliación de la Universidades en Colombia.

La Impunidad De Los Delitos Informáticos En Ciber-Sociedad Costarricense En El Ámbito Del Derecho Penal. Roberto Lemaitre Picado, 2010

Como primer antecedente en el ámbito Internacional, se resalta la investigación realizada por Roberto Lemaitre Picado, De La Universidad De Costa Rica (2010), titulada: La Impunidad De Los Delitos Informáticos En Ciber-Sociedad Costarricense En El Ámbito Del Derecho Penal. el cual planteo como objetivos: Analizar la deficiencia presente en el ordenamiento jurídico penal costarricense en materia de delitos informáticos.

En este sentido, la investigación se realizó bajo un método cualitativo con el aporte del cuantitativo, cuyos resultados permitieron entender que para comprender el delito informático se debe visualizar correctamente, si no se comprende el ecosistema donde se desarrolla, de esta manera se logra un primer acercamiento a la complejidad de la persecución del delito.

La anterior investigación realiza aportes a nivel teórico donde se plantea según el doctor en derecho Héctor Ramón Peñaranda Quintero, dice que para hablar propiamente de la autonomía de una rama del derecho se necesita ciertas características: La existencia de campos normativos, docentes, institucional y científicos (Peñaranda, 2000). Esta investigación es importante para el presente trabajo de investigación por que resalta que hay un atraso agigantado del derecho frente a los delitos informáticos. El panorama es difícil al no existir un organismo internacional de seguridad, a pesar de existir la interpol y otras

instituciones, estas no parecen estar muy especializadas en acciones policiales contra la ciberdelincuencia. Por tal motivo es difícil llegar a pensar que a nivel nacional el Estado Colombiano este haciendo trabajo o pensando en desarrollar trabajos para contra restar esta problemática que afecta a toda la sociedad.

Este antecedente es importante para esta investigación, por que logra entrar en un contexto internacional de la realidad que viven los ciber usuarios frente a la ciberdelincuencia, existe además de una inseguridad jurídica, un gran olvido y vacío por parte de las autoridades internacionales para logra contra restar estos delitos.

Observando diversos productos que la red Facebook que ofrece por medio de perfiles supuestamente empresariales que a simple vista brindan un amplio mercadeo y confiabilidad. Jurado, 2016

Como segundo antecedente esta Jurado (2016), cuando se encontraba navegando por internet y observando diversos productos que la red Facebook que ofrece por medio de perfiles supuestamente empresariales que a simple vista brindan un amplio mercadeo y confiabilidad, cosa que llamo la atención del joven Alejandro, al ojear un poco el perfil que tenía como nombre Importaciones S.A. Se puede observar comentarios de usuarios satisfechos con los productos que este perfil vendía algo que llamo mucho la atención.

El perfil promocionaba como producto primordial y el más vendido un celular de alta gama un Samsung S6 a un muy buen precio con un descuento que de inmediato lo deslumbro, no lo pensó dos veces y quiso comprar el producto, hizo lo que el usuario vendedor le exigía como requisitos entre esos enviar el dinero junto con su dirección de domicilio para hacerle él envió, días después como lo acordado a su domicilio llego un paquete con el celular que Alejandro pago y si a simple vista era un celular con las mismas especificaciones que el compro, el mismo nombre la misma forma con los accesorio que acompañaban el celular entre ellos audífonos manos libres cargador y un estuche protector.

Lo que el joven poco tiempo después se percato fue de la gran estafa en la que se vio afectado puesto que dicho celular era una réplica que el valor económico era muy bajo del que el cancelo y no brindaba las mismas funciones que el original que el creyó a ver

comprado, cuando quiso enviar un mensaje al perfil no recibió respuesta alguna a los reclamos que por medio de mensajes les envió y al indagar un poco más sobre la página pudo notar perfiles falsos calificando positivamente esta página y dando testimonio de supuestas compras y satisfacción de este perfil lo cual fue un poco indignante pues no encontró como resolver el problema solo informar a los usuarios advirtiendo de la estafa que este perfil viene realizando.

Estafa Por Método Phishing. Netflix, 2017

Netflix (2017), otra vez estafada por el método Phishing en el cual los usuarios reciben un email en el que les pide una actualización de sus datos, pero todo es una estafa para que los delincuentes cibernéticos puedan hacer su estafa y obtener información confidencial de forma fraudulenta como puede ser contraseñas o información detallada sobre las tarjetas de crédito u otra información de la víctima.

El estafador, conocido como phisher, se vale de técnicas de ingeniería social, haciéndose pasar por una persona o empresa de confianza en una aparente comunicación oficial electrónica más común en la red social Facebook Faraldo (2010). Profesora titular de derecho penal universidad de a Coruña en la que en su trabajo de investigación hace un análisis sobre el fenómeno delictivo de la suplantación de identidad y uso de nombre supuesto tanto en el comercio tradicional como en el electrónico que da lugar a soluciones dispares en la doctrina y jurisprudencia, se presenta las posibilidades que ofrecen los delitos de usurpación del estado civil, como objetivo principal pretende hacer un llamativo ya que no existe una regulación específica de la suplantación de identidad y uso de nombre supuesto en el comercio tradicional y electrónico en el Código penal, se pretende en este trabajo aludir al comportamiento delictivo. Esta ausencia provoca una serie de consecuencias indeseable.

Bicarregui (2008), El objeto del presente estudio lo constituye la exposición de las principales modalidades de fraude omisibles utilizando Internet como herramienta. A dicha exposición se acompaña una primera parte en la que se analiza la relevancia de estos fenómenos, debida en gran parte a su vertiginoso incremento en los últimos años. Por último

y como abogado en ejercicio, se acompaña también una relación esquemática de consejos y recomendaciones para evitar terminar siendo víctima de un fraude On-Line.

El presente trabajo se realiza, por tanto, con una vocación eminentemente útil y práctica, tratando de acercar al lector no familiarizado con estos fenómenos de terminología tan técnica, en unos casos, como "exótica", en otros, el conocimiento de los recursos utilizados por los defraudadores, así como sus prácticas más habituales. No se busca, por tanto, el agotamiento de todas las posibles modalidades delictivo-fraudulentas, ni con ello, por ende, el del propio lector.

ciberespacio y el crimen organizado. Los nuevos desafíos del siglo XXI. Sánchez, 2013

Sánchez, (2013) "*ciberespacio y el crimen organizado. Los nuevos desafíos del siglo XXI"* como objetivo del siguiente articulo pretende disminuir el ciberterrorismo que afecta la economía también prevenir por medio de la concientización de los riegos del uso inadecuado de las redes sociales para concluir Internet se ha convertido en el espacio ideal para la ciberdelincuencia y el ciberterrorismo, ya que ofrece fácil acceso, poco o ningún control gubernamental, anonimato, rápido flujo de información, altísimo impacto, escaso riesgo, barato e indetectable. Además, hay que tener en cuenta que por mucho que se empeñen las agencias o secretarías de seguridad de los Estados, es imposible garantizar la seguridad plena de los sistemas informáticos.

La única solución realmente efectiva y eficaz es apagar Internet o suprimirlo, pero esta alternativa no es, lógicamente, razonable en un mundo como el actual, pese a las excepciones particulares como son las de los Emiratos Árabes, Corea del Norte o China. Aunque también existe otra posibilidad: identificar las vulnerabilidades e individualizar los peligros existentes y potenciales que dichas debilidades permiten, y esperar a ver cuál es el resultado final. Las otras soluciones aquí planteadas, como los sistemas de control de comunicación, la creación de agencias y de cibersoldados, de momento no están resultando totalmente efectivas. Es cierto, que están contribuyendo a detectar a ciberdelincuentes y ciberterroristas, pero todavía no son capaces de controlar ni impedir su actividad en la red.

Riesgos del consumidor electrónico en las prácticas publicitaria, Rodríguez, 2015

Rodríguez (2015), “Riesgos del consumidor electrónico en las prácticas publicitaria” una profunda investigación que nos permite ver un método muy utilizado en las redes social Facebook en el cual por medio de publicidad pretenden incentivar un falso comercio masivo. Este trabajo considera que en Internet es tan difícil separar la falsa publicidad del resto de las áreas de marketing, ya que simultáneamente se anuncia, se ejecuta la transacción comercial, se informa técnicamente, se ofrece regalos y se prosigue el servicio postventa en la que los usuarios son engañados puesto que nunca se cumple con lo publicado.

Oxman (2013), “Estafas informáticas a través de Internet: acerca de la imputación penal del “phishing” y el “pharming” con esta investigación se pretende más que al usuario de internet a los estados para que tomen medidas ante estos fenómenos de estafa que se están presentando en todo el mundo y que cada día toma más fuerza y un libre desarrollo, para abordar la imputación penal de los fraudes informáticos de apoderamiento patrimonial más comunes en Chile. Teniendo en cuenta las posibilidades que ofrece el derecho comparado, Después de haber transitado por las múltiples respuestas que ofrece nuestro Derecho para la sanción de las conductas que comentamos, las que en ningún caso se limitan a la mera discusión sobre la concurrencia de la estafa, estamos en condiciones de sostener que el estado actual de la legislación chilena en esta materia requiere de una adecuación necesaria y urgente que permita hacer frente a la necesidad de punición que reclaman los fraudes bancarios cometidos a través de la banca “online”, en todas sus dimensiones.

Tanatología Digital Y Delito Informático. Diana Marcela Ardila Carrillo & Oscar Fabián Lombana Jiménez, 2015

Como sexto antecedentes en el ámbito nacional se resalta la investigación realizada por Diana Marcela Ardila Carrillo & Oscar Fabián Lombana Jiménez, de la Universidad Libre de Bogotá (2015), titulada: “Tanatología Digital Y Delito Informático”, el cual planteo como objetivos general: Construir el referente normativo de especificación y consulta, que permita a la comunidad académica del programa de ingeniería de sistemas UniLibre, el interpretar y dimensionar el espacio o contexto donde se genera el delito informático por aplicación procedimental del conjunto de técnicas cobijadas por la tanatología digital.

En este sentido, la investigación se realizó bajo La estructura de definición a nivel investigativo que soporta el desarrollo de este trabajo por sus principios de referenciación cualitativa, permiten visualizar la relación que el delito informático mantiene con las técnicas y procedimientos de la informática forense que considera la jurisprudencia colombiana, hecho que demanda la observación en primera instancia de la correspondiente ley (1273).

La anterior investigación realiza aportes a nivel teórico donde se plantea, La red de comunicaciones, se define normalmente como la entidad computacional validada telemáticamente, que permite interconectar nodos con independencia geográfica para transmitir o recibir valores informáticos que fluyen en una transacción" (Tomasin, 2004). De la misma forma en Colombia los delitos informáticos incluyen el manejo de claves programáticas espías, la estafa en línea, la divulgación no permitida de contenidos, la violación de derechos de autor, la piratería y la pornografía infantil sobre estas tipificaciones el tanatólogo debe tener capacidad de respuesta." (Tomasin, 2004)

Esta investigación es importante para el presente trabajo de investigación por que resalta El índice es directamente asociado con el número de delitos informáticos, cuyo crecimiento preocupa a las autoridades colombianas, por ejemplo, resulta fácil establecer que, para julio del 2014, el número de intrusos de fraude se fijó en la más alta de la historia. Hecho que ha obligado la incorporación de un conjunto de acciones orientadas a consolidar la plataforma de seguridad, según lo estipulo el TCB (Trusted Computing Base), se deben fijar las autoridades en este fenómeno que se acrecienta todos los días, si no se le coloca mano fuerte a los ciberdelincuentes, esto nunca va cambiar. Acciones de seguridad. Todo plano de seguridad orientado a contrarrestar el delito informático, debe estructurar el conjunto de acciones listados, que persiguen la computación operacional de los llamados agentes validadores (Stallings,2010); debe aclararse que si bien estas acciones no eliminan de tajo el delito informático si contribuyen a su reducción.

El Delito De Hurto Por Medios Informáticos Que Tipifica El Articulo 269i De La Ley 1273 De 2009 Y Su Aplicabilidad En El Distrito Judicial De Cúcuta En El Período 2012 – 2014. Ricardo Granados Ramírez & Astrid Carolina Parra Rojas, 2016

Como séptimo antecedente en el ámbito local, se resalta la investigación realizada por Ricardo Granados Ramírez & Astrid Carolina Parra Rojas, de la Universidad Libre De Colombia Seccional Cúcuta (2016), Titulada: El Delito De Hurto Por Medios Informáticos Que Tipifica El Articulo 269i De La Ley 1273 De 2009 Y Su Aplicabilidad En El Distrito Judicial De Cúcuta En El Período 2012 - 2014.

En este sentido, la investigación se realizó bajo un método tipo descriptivo-propositivo, ya que con él mismo se analizará la aplicabilidad que ha tenido el artículo 269I de la Ley 1273 de 2009 que tipifica el delito de hurto por medios informáticos. La anterior investigación realiza aportes a nivel teórico donde se indica que: El uso de las tecnologías de la información y las comunicaciones trae consigo cambios y retos permanentes y se constituye como uno de los pilares del mundo globalizado.

De manera simultánea el avance de estas tecnologías ha incrementado el uso de medios tecnológicos con fines delictivos alrededor del mundo. La continua evolución, crecimiento y sofisticación de los ataques cibernéticos, al igual que la convergencia tecnológica, ponen de manifiesto la necesidad de adoptar las medidas y controles que permitan proteger al Estado ante estas nuevas amenazas. El aumento de la capacidad delincuencial en el ciberespacio, así como la utilización de nuevas tecnologías para generar amenazas informáticas, constituyen una preocupación común a todos los países, dado que impactan de manera significativa la seguridad de la información, en los ámbitos tanto público como privado e incluyendo a la sociedad civil. (Departamento Nacional de Planeación, Conpes 3701 de 2011).

Esta investigación es importante para el presente trabajo de investigación por que resalta que hay un atraso agigantado del derecho frente a los delitos informáticos. El panorama es difícil al no existir un organismo internacional de seguridad, a pesar de existir la interpol y otras instituciones, estas no parecen estar muy especializadas en acciones policiales contra la ciberdelincuencia. Por tal motivo es difícil llegar a pensar que a nivel nacional el Estado Colombiano este haciendo trabajo o pensando en desarrollar trabajos para contra restar esta problemática que afecta a toda la sociedad.

Con resultados importantes: La revolución informática surgida desde mediados del siglo XX hasta la actualidad, ha traído consigo un sinnúmero de beneficios, especialmente

relacionados con la facilidad para el intercambio de información y comunicación a nivel mundial; sin embargo, así como esta ha evolucionado y tiene importantes ventajas, también ésta tiene sus desventajas, y es que a la par con ella han surgido los delincuentes informáticos, quienes han venido perfeccionando sus modus operandi en los delitos informáticos, siendo uno de los más frecuentes el delito de hurto por medios informáticos, consagrado en la Ley 1273 de 2009 (Artículo 269I).

Este antecedente es importante para esta investigación, por que logra entrar en un contexto de la importancia y beneficios que trae el internet, pero a la vez muestra las desventajas y estas vienen por parte del surgimiento de los ciberdelincuentes quienes han venido perfeccionando sus modus operandi en los delitos informáticos.

2.2 Marco Teórico

A continuación, se presentan las bases teóricas que sustentan la investigación, es de vital importancia hacer alusión a como las relaciones humanas conllevan a que se ejecuten conductas. Ángel Arias en su libro Estafas Digitales plantea una serie de soluciones y métodos partiendo de bases históricas y cómo evoluciona cada día la estafa digital, en el cual menciona datos importantes.

2.2.1 Delitos Informáticos:

Un delito informático que tiene lugar mediante el empleo de las Tecnologías de la información y la comunicación TIC. Es importante hacer un correcto análisis y profundizar en nuestra investigación, consideramos imprescindible comprender qué es un delito informático y tener claras sus características ya que el tema que nos ocupa, la estafa por compra venta en Internet, y en especial en la red social Facebook, no son más que un delito informático que tiene lugar mediante el empleo de esta tecnología.

Muchos autores y organismos han intentado proporcionar una definición de delito informático. Algunos expertos en la materia han llegado a afirmar que delito informático y delito común es lo mismo, que no hay que hacer una diferenciación entre estos dos conceptos, ya que el resultado final de los delitos informáticos y de los delitos tradicionales viene a ser el mismo, diferenciándose entre sí solo por el medio empleado para llevar a cabo el acto ilícito (Ramírez & Aguilera, 2015).

Una definición válida podría ser la siguiente: los delitos informáticos son aquellas conductas que, tanto por el medio utilizado como por el objeto sobre el que recaen, son realizadas a través de procesos electrónicos, teniendo como característica común un ámbito de riesgo centrado en la expansión de la tecnología informática (Garrido, Stangeland & Redondo, 2006).

Otra definición es la que se establece en el Convenio de la Ciberdelincuencia Europeo. Establece que los delitos informáticos son "los actos dirigidos contra la confidencialidad, la integridad y la disponibilidad de los sistemas informáticos, redes y datos informáticos, así como el abuso de dichos sistemas, redes y datos" (Consejo de Europa, 2001).

Hay una serie de características que comparten todos los delitos informáticos. Destaca tanto la dificultad probatoria, ya que es mucho más difícil seguir un delincuente informático porque estos pueden cometer sus infracciones de una forma muy rápida y sin importar el área geográfica en la que se encuentran, como su perseverante evolución y proliferación, cosa que dificulta mucho su persecución. Además, estos delitos también se caracterizan porque 11 no cualquier persona los puede llevar a cabo, ya que para su comisión es necesario tener ciertos conocimientos informáticos (Gallego, 2012).

Respecto al fraude online, hay que decir que este está recogido en el artículo 8 del Convenio de Budapest del Consejo de Europa sobre Ciberdelincuencia, definiendo el mismo como "(…) los actos deliberados e ilegítimos que causen un perjuicio patrimonial mediante una amplia gama de procedimientos (…) con la intención fraudulenta o delictiva de obtener ilegítimamente un beneficio económico para uno mismo o para otra persona" (Consejo de Europa, 2001, p. 31).

Según INTECO, los elementos que concurren en el fraude a través de Internet son los siguientes: voluntad, carácter lucrativo, perjuicio patrimonial de un tercero y empleo de medios electrónicos o informáticos para la comisión del delito. En cuanto a los tipos de fraudes cometidos a través de medios electrónicos, generalmente la legislación es poco explícita. Es muy frecuente recoger tipos genéricos, en los que se puedan encajar los diferentes supuestos de estafa o fraude en Internet que puedan cometerse (INTECO, 2007).

2.2.2 Redes Sociales

Para (Requena Santos, 2011, pág. 2) una red social son la serie de vínculos que existe entre varios actores sociales que tienen como capacidad principal la interpretación de la conducta de los miembros que la componen.

Por otra parte (Cacales, García, & Benedicto, 2011) manifiestan que las redes sociales en internet son conformadas por un grupo de amigos que, al ingresar a un portal de redes sociales, tienen la oportunidad de hacer partícipe de la misma a sus propios contactos que a su vez son puestos a consideración a los demás miembros de la red de tal manera que el acceso a este grupo se va ampliando exponencialmente se vayan integrando personas a la red

Este fenómeno se sustenta en las teorías de los seis grados de Frigyes Karinthy quien en 1929 publico la historia denominada “Chains” en esta aseguraba que siguiendo la secuencia “un amigo de un amigo mío” por seis niveles de personas, es decir “el amigo, de un amigo, de un amigo, de un amigo, de un 12 amigo, de un amigo” y que cada una de estas personas le repitiera el mensaje al menos a 100 de sus amigos, se podría transmitir el mensaje a un billón de personas. (Cacales, García, & Benedicto, 2011)

Otra cualidad importante de las redes sociales en internet y que la diferencia de los demás espacios disponibles en la red es que para que una red sea funcional debe mantener vigente dos principios según el (Observatorio Nacional de las Telecomunicaciones España, 2011)

Contenidos libres del derecho de autor: pese a que existen normas para proteger el derecho de autor, los participantes de la red social deben de aceptar que, con la exposición de sus contenidos, estos pueden ser usadas por los miembros de la red sin su consentimiento.

Construcción de contenidos colaborativos: la finalidad de exponer la información a los miembros de la red es que estos a su vez realicen la misma actividad de tal manera que se desarrolla una interacción que forme nuevo contenido y que a su vez estimule el ingreso de nuevos contactos en la red.

De esta manera, se resume que una red social se da por la composición de un sitio virtual en donde un grupo de personas con intereses comunes comparten su información la cual a su vez está disponible para los que accedan a este sitio y que también se vinculan con las redes que estos comparten.

2.3 Marco Contextual

Este trabajo se relocalizo, con el fin de recolectar datos a través de instrumentos de investigación que permitió obtener información y respuestas para analizar y realizar una mirada profunda en cuanto lo que ha sucedido en el tiempo con un fenómeno tan presente y tan latente en la red social Facebook afectando en la sociedad factores económicos y permitiendo el libre desarrollo de actos dolosos ilícitos sin ningún control alguno, Mediante investigación, obtener respuestas que nos permitan identificar cuáles son los avances que se han obtenido, y la especificación en cuanto a la disminución de seguridad en la red social Facebook y derechos que se están vulnerando.

El proyecto se llevará a cabo en su aplicación práctica en la ciudad de Cúcuta Norte de Satandera y en la red social Facebook en grupos específicos creados para enlazar un comercio de diferentes clases sociales y edades en la ciudad de Cúcuta departamento de norte de Santander, siendo también un factor por el cual es común para analizar el comportamiento de la sociedad en la red Facebook.

2.4 Marco Legal

El marco Legal de esta investigación parte desde la carta magna de 1991, don se le dan garantías al ciudadano frente a sus derechos y por lo tanto se garantiza la seguridad en todos sus ámbitos, por lo tanto, en este trabajo se arrancará desde la constitución política de Colombia.

Nuestra constitución política establece normalmente normas que tocan directamente con la información y por ende se convierten en el sustento de firmeza superior para fundar los llamados delitos informaticos.es así como encontramos en el artículo 15 de la Carta, en lo concerniente a la intimidad de las personas y el artículo 20 relativo al derecho de información. Artículo 15. Todas las personas tienen derecho a su intimidad personal y familiar y a su buen nombre, y el Estado debe respetarlos y hacerlos respetar.

De igual modo, tienen derecho a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en bancos de datos y en archivos de entidades públicas y privadas. En la recolección, tratamiento y circulación de datos se respetarán la libertad y demás garantías consagradas en la Constitución. La correspondencia y demás formas de comunicación privada son inviolables. Sólo pueden ser interceptadas o registradas mediante orden judicial, en los casos y con las formalidades que establezca la ley.

Para efectos tributarios o judiciales y para los casos de inspección, vigilancia e intervención del Estado podrá exigirse la presentación de libros de contabilidad y demás documentos privados, en los términos que señale la ley. Constitución política. Artículo 20. Se garantiza a toda persona la libertad de expresar y difundir su pensamiento y opiniones, la de informar y recibir información veraz e imparcial, y la de fundar medios masivos de comunicación.

Estos son libres y tienen responsabilidad social. Se garantiza el derecho a la rectificación en condiciones de equidad. No habrá censura. Es entonces claro que la constitución política de Colombia si otorga a través de su principia listica y de normas que consagran derechos fundamentales, tales como los articulo 15 y 20, un respaldo suficiente como para que el

legislador consagre normas tendientes a desarrollar lo que se conoce mundialmente como delitos informáticos.

En estos artículos se plasma una idea inicial a partir de la cual se puede formular de acuerdo al avance de la tecnología y las comunicaciones una nueva reglamentación que proporcione seguridad jurídica en el uso de las redes sociales frente a los delitos informáticos. Por otro lado, también está el artículo 2 de la constitución Política que ofrece un amplio margen legal, suficiente como para sustentar una labor legislativa tendiente a la expedición de normas que contemplen también los llamados delitos informáticos. Artículo 2. Son fines esenciales del Estado: servir a la comunidad, promover la prosperidad general y garantizar la efectividad de los principios, derechos y deberes consagrados en la Constitución; facilitar la participación de todos en las decisiones que los afectan y en la vida económica, política, administrativa y cultural de la Nación; defender la independencia nacional, mantener la integridad territorial y asegurar la convivencia pacífica y la vigencia de un orden justo.

Las autoridades de la República están instituidas para proteger a todas las personas residentes en Colombia, en su vida, honra, bienes, creencias, y demás derechos y libertades, y para asegurar el cumplimiento de los deberes sociales del Estado y de los particulares.

Aspectos jurisprudenciales Las altas corporaciones que tiene dentro de sus funciones la de administrar justicia y velar porque el ordenamiento jurídico no atente contra la carta constitucional, no han tenido una actividad jurisprudencial notoria frente al tema de los llamados delitos informáticos pues no han producidos pautas o líneas jurisprudenciales contundentes y esto se da por la ausencia de normas que estén en esa sintonía tecnológica.

El código penal colombiano en su capítulo VII del libro segundo del título III: delitos contra la libertad individual y otras garantías, trata sobre la violación a la intimidad, reserva e interceptación de comunicaciones: Articulo 192. Violación ilícita de comunicaciones. Artículo 193. Ofrecimiento, venta o compra de instrumento apto para interceptar la comunicación privada entre personas. Artículo 194. Divulgación y empleo de documentos reservados. Artículo 195. Acceso abusivo a un sistema informático. Artículo 196. Violación

ilícita de comunicaciones o correspondencia de carácter oficial. Artículo 197. Utilización ilícita de redes de comunicaciones.

Estos artículos son concordantes con el artículo 357: “daño en obras en los servicios de comunicaciones, energías y combustibles. Otra norma que habla sobre los delitos informáticos en Colombia fue la ley 679 de 2001, que estableció el estatuto para prevenir y contrarrestar la explotación, la pornografía y el turismo sexual con niños menores de edad. De igual manera, consagra prohibiciones para los proveedores o servidores, administradores o usuarios de redes globales de información, respecto a alojar imágenes, textos, documentos o archivos audiovisuales que exploten a los menores en aptitudes sexuales o pornográficas. Sin embargo, la norma no contiene sanciones legales, si no administrativas, pues siendo simple prohibición, deja un vacío que quita eficacia a la ley, cuando se trata de verdaderos delitos informáticos.

También está la ley 1336 por medio de la cual se sanciona y se fortalece la ley 679 de 2001, de lucha contra la explotación, la pornografía y el turismo sexual, con niños, niñas y adolescentes. De forma específica, en su capítulo VI, sanciona los tipos penales de turismo sexual y almacenamiento e intercambio de pornografía infantil, con penas de prisión de 10 a 20 años y multas de 150 a 1550 salarios mínimos legales mensuales vigentes.

La ley 1273 de 2009 complementa el código penal y crea un nuevo bien jurídico tutelado a partir del concepto de la protección de la información y los datos, con el cual se preserva integralmente a los sistemas que utilicen las tecnologías de la información y las comunicaciones. El primer capítulo de los dos en que está dividida la ley, trata de los atentados contra la confidencialidad, la integridad y la disponibilidad de los datos y de los sistemas informáticos.

El segundo capítulo se refiere a los atentados informáticos y otras infracciones. “A partir de la ley 1273 de 2009 se tipificaron los delitos informáticos en Colombia en los siguientes términos: Acceso abusivo a un sistema informático (modificado de código penal); obstaculización ilegitima del sistema informático o red de telecomunicación; interceptación de datos informáticos; daño informático; uso de software malicioso; hurto por medios

informáticos y semejantes; violación de datos personales; suplantación de sitios web para capturar datos personales y transferencia no consentida de activos.

Esta ley y marco jurídico se ha convertido en una importante contribución y en un instrumento muy efectivo para que las entidades públicas y privadas puedan enfrentar los delitos informáticos, con definiciones de procedimientos y políticas de seguridad de la información; y, en consecuencia, con las acciones penales que pueden adelantar contra las personas que incurren contra las acciones tipificadas en la norma.

Con ella, Colombia se ubica en el mismo nivel de los países miembros de la comunidad económica europea, los cuales ampliaron el nivel internacional de los acuerdos jurídicos relacionados con la protección de la información y los recursos informáticos de los países, mediante el convenio "cibercriminalidad", suscrito en Budapest Hungría en 2001 y vigente desde julio de 2004. Con los desarrollos jurídicos hasta ahora los grados acerca "la protección de la información y de los datos y la preservación integral de los sistemas que utilicen las tecnologías de información y comunicación", las organizaciones puede amparar parte de sus sistemas integrados de información: datos, procesos, políticas, personal, entradas, salidas, estrategias, cultura corporativa, recursos de las tic y el entorno externo, de manera que, además de contribuir y asegurar las características de la calidad de información, incorpora la administración y el control del concepto de protección integral.

Gracias a esta tipificación del delito se pueden aplicar a la norma para después exigirse una sanción y así tener un marco jurídico aplicable a las diferentes conductas que se están presentando en las redes sociales que vulneran y afectan los derechos de los diferentes usuarios."

La ley 1273 de 2009 trae importantes figuras tipificadas en las cuales se identifican actuaciones que llegan a convertirse en delitos informáticos presentes en las redes sociales y que tipificación del delito se pueden aplicar a la norma para después exigirse una sanción y así tener un marco jurídico aplicable a las diferentes conductas que se están presentando en las redes sociales que vulneran y afectan los derechos de los diferentes usuarios.

Algunas de esas figuras de la ley 1273 de 2009 que se incorporaron al código penal son: Artículo 1 de la ley 1273 de 2009, incorporar al código penal el artículo 269A y complementa

el tema relacionado con “el acceso abusivo a un sistema informático”, que se manifiesta cuando el pirata informático o hacker aprovecha la vulnerabilidad en el acceso a los sistemas de información, o las deficiencias en los procedimientos de seguridad informática establecidos por las organizaciones, para extraer beneficios económicos o para indagar o demostrar la capacidad y recursos que ofrece la tecnología de información. Cuando se presenta este abuso, en muchos casos se observa que proviene de los mismos usuarios del sistema y de los empleados.

El articulo 269B contempla como delito la obstaculización ilegitima del sistema informático o redes de telecomunicación y se originan cuando el hacker informático bloquea en forma ilegal un sistema o impide el sistema por un tiempo, hasta cuando tiene un beneficio por lo general económico. Aquí también se enmarca el acceso a cuentas de correo electrónico sin el debido consentimiento de los respectivos usuarios y el manejo o bloqueo de las claves obtenidas de distinta forma. El articulo 269C plantea la infracción relacionada con la “interpretación ilícita de datos informáticos”, también considerada en el artículo 3 del título 1 de la convención de Budapest de 2001. Se presenta cuando una persona valiéndose de los recursos tecnológicos, obstruye datos sin autorización legal, en su sitio de origen, en el destino o en el interior de un sistema informático, o de emisiones electromagnéticas de un sistema electromagnético que los trasporte.

El delito relacionado con los “daños informáticos” está contemplado en el artículo 269D y se comete cuando una persona que sin estar autorizada, modifica, altera, daña, borra, destruye o suprime datos del programa o de documentos electrónicos, en los recursos de las TIC. El articulo 269 E contempla el delito vinculado con el “uso de software malicioso” técnicamente denominado malware, ya generalizado en internet. Se presenta cuando se produce, adquieren, venden, distribuyen, envían, introducen o extraen del país software o programas de computador que producen daños en los recursos de las TIC.

El delito sobre la “violación de datos personales” (hacking) lo trata el articulo 269F y está orientado a proteger los derechos fundamentales tales de la persona (como dignidad humana y libertad ideológica”. Se da cuando un individuo sin estar facultado, sustrae, vende, envía, compra, divulga o emplea datos personales almacenados en ficheros, archivos, bases de

datos o medios similares con el fin de lograr utilidad personal o para otros. El articulo 269G trata de la “suplantación de sitios web para capturar datos personales”.

Este sucede cuando el suplantador (phiser) o delincuente informático crea una página y un dominio similar al de la entidad a la cual desea abordar, lo ubica en un hosting (espacio en un servidor) desde donde envía correos spam o engañosos, como por ejemplo busca de empleos. Al no diferenciar la página original de la falsa, las personas inocentemente suministran información personal y claves bancarias q el suplantador almacena en una base de datos y luego ordena la transferencia del dinero de la víctima q cunetas de terceros quienes prestan sus cuentas o sirven de testaferros, que luego reclama o distribuye.

La ley 1273 de 2009 también trae unas circunstancias de agravación punitiva q aumenta la pena del delito entre las cuales la más relacionada con los delitos informáticos en las redes, son las circunstancias de agravación en las que la pena se aumenta de la mitad a las tres cuartas partes cuando el delito se cometiera revelando o dando a conocer el contenido de la información en perjuicio de otro, este sería el caso por ejemplo de las personas que utilizan las redes sociales para difundir información de toda clase; fotos, videos, datos, escritos, entre otros, que muchas veces son hurtados de cuentas personales u obtenidos de forma fraudulenta para difundirlos con la finalidad de causarle perjuicio a otra persona.

En estos casos se nota claramente como se está violando el derecho a la privacidad e intimidad, además de vulneraciones claras de la integridad moral y derechos fundamentales, y además se denota como con esta ley existen ya en Colombia más posibilidades para encuadrar legalmente actividades y conductas que día a día aparecen con el uso de las nuevas tecnologías de información y comunicación como las redes sociales. Aunque esta nueva ley todavía sigue siendo muy general y requiera de una amplia interpretación por parte de los jueces y abogados para aplicarla frente los nuevos delitos, es una ley que por lo menos ayuda a avanzar en la lucha contra estos delitos informáticos pues como es sabido el constante y permanente avance día a día de la internet y los diferentes usos que esta ofrece.

a partir del Documento Conpes 3701 del 2011, el país definió una estrategia de ciberdefensa y ciberseguridad y se introdujo la necesidad de contar con un programa articulador de esfuerzos en materia de investigación de delitos cibernéticos. Así mismo,

desde el 2000, con ocasión de la reforma a los códigos Penal y de Procedimiento Penal, se iniciaron labores para dotar a la Rama Judicial de nuevos mecanismos tanto a nivel probatorio como a nivel de investigación criminal. Fue así que en el año 2005, Colombia adoptó un nuevo sistema de prosecución criminal llamado sistema acusatorio. Este nuevo sistema introdujo una labor más especializada de los organismos técnicos (cuerpo de Policía Judicial), un sistema basado en la oralidad y la intervención de los jueces con función de control de garantías.

Para complementar la labor que cumplen las autoridades en materia de investigación criminal, así como en labores de inteligencia, recientemente se expidió una nueva ley de inteligencia nacional: la Ley Estatutaria 1621 de abril del 2013, cuyo antecedente más próximo, la Ley 1288 del 2009, había sido declarada inexequible por la Corte Constitucional por vicios en su formación. La Corte, en ese momento, hizo un análisis de fondo de la violación de derechos como el de la intimidad en ciertos mecanismos concedidos a las autoridades.

También es importante señalar que Colombia ha adoptado normas que obligan a los prestadores de servicios de comunicaciones, por orden de los fiscales, a permitir el procesamiento (analizar, capturar y retener) de información en redes de comunicaciones por parte de los organismos. En especial, el Decreto 1704 del 2012 hace obligatorio para los operadores y prestadores de servicios de comunicaciones colaborar con las autoridades para obtener acceso a la captura del tráfico de las comunicaciones que cursen por sus redes.

3 METODOLOGÍA

3.1 Paradigma de la Investigación

El paradigma de investigación usado en este trabajo de investigación es el Interpretativo. Kuhn (1971) señala: "son realizaciones científicas universalmente reconocidas, que, durante cierto tiempo, proporcionan modelos de problemas y soluciones a una comunidad científica. Este paradigma se basa en el proceso de conocimientos, en el cual se da una interacción entre sujeto y objeto, no pretende hacer generalizaciones a partir de los resultados obtenidos. Su finalidad es profundizar el conocimiento del grupo de investigadores y los estudiantes de derecho y comprender la realidad de la inseguridad jurídica del comprador a través de la red social Facebook en el Estado colombiano.

Este paradigma se basa en analizar y comprender el conocimiento, la postura y la percepción por parte del objeto de estudio que en esta investigación son las autoridades competentes (Congreso, Fiscalía Y Policía) y el análisis Comparativo de la legislación contra el delito de la estafa a través de las redes sociales entre Colombia, Ecuador y España.

La finalidad es profundizar el conocimiento y comprender si en realidad existe eficacia por parte del legislador y las autoridades competentes del Estado colombiano para brindada seguridad jurídica a los usuarios Facebook y así contra restar la estafa que se llevar a cabo a través de la compraventa en redes sociales, lo cual se logra cuando se interpreta los resultados obtenidos en los instrumentos debidamente validados.

3.2 Enfoque de la Investigación

La presente investigación sobre la seguridad jurídica del comprador a través de la red social Facebook en el Estado colombiano, se realizó bajo un enfoque cualitativo por su gran impacto de cualidades sobre la temática, este enfoque permitirá describir las cualidades de un fenómeno, en la búsqueda de un concepto que pueda abarcar una parte de la realidad. Lo

más importante es no trata de probar o de medir en qué grado una cierta cualidad se encuentra en un cierto acontecimiento dado, sino de descubrir tantas cualidades como sea posible o tantas anomalías que pasan por alto como lo es la estafa a través de perfiles falsos por medio de la red social Facebook.

Sampieri (2010) señala: “utiliza recolección de datos sin medición numérica para descubrir o afinar preguntas de investigación y puede o no probar hipótesis en su proceso de interpretación. Sampieri también hace referencia a “la recolección y el análisis de los datos, los estudios cualitativos pueden desarrollar preguntas e hipótesis antes, durante o después para descubrir cuáles son las preguntas de investigación más importantes; y, después para refinarlas y responderlas con el fin de probar hipótesis.

Igualmente, con la matriz de análisis sobre la legislación que trata la problemática en países como Colombia, Ecuador y España se lograr comprender que tantas cualidades como anomalías presenta la inseguridad jurídica del comprador a través de la red social Facebook en estos Estados. Así mismo con el análisis normativo de Colombia y el reglamento de esta red social observar los vacíos que enfrenta este delito cibernético.

3.3 Diseño de la Investigación

El diseño que abordo en este proyecto de investigación, es el hermenéutico teniendo en cuenta que, en el siglo XX, la hermenéutica se convierte en la base de un enfoque filosófico para el análisis y la compresión de la conducta humana. Es una filosofía, un enfoque y un método, pues enfatiza la vuelta a la reflexión y a la intuición para describir y clarificar la experiencia tal como ella es vivida pero con una marcada diferencia, ya que el método hermenéutico trata de introducirse en el contenido y la dinámica de la persona estudiada y en sus implicaciones, buscando estructurar una interpretación coherente del todo, mientras que el fenomenológico se centra en el estudio de esas realidades vivenciales, determinantes para la comprensión de su vida psíquica.

En un amplio sentido este método se utiliza en las investigaciones psicológicas, sociológicas y educacionales entre otras. Por lo tanto, es un diseño positivo a seguir. Baeza (2002) señala: La hermenéutica sugiere un posicionamiento distinto a la realidad, adoptar una actitud distinta de empatía profunda con el texto o lo expresado a través del lenguaje, por lo tanto, no se trata de inhibir su propia subjetividad, sino de asumirla.

Se procura investigar el fenómeno de la inseguridad jurídica del comprador a través de la red social Facebook en Colombia, profundizando desde la matriz de análisis tanto en el derecho comparado entre Colombia, Ecuador y España, e igualmente la entrevista hecha a las autoridades competentes del Estado Colombiano, y así comprender la realidad que viven los usuarios del Facebook frente a la estafa a través de perfiles falsos.

3.4 Fuentes de la información

Entrevistas

En el presente trabajo de investigación estuvieron como informantes claves el intendente Leonardo Ardila Quijano encargado del tema de delitos informáticos y anti atracos de la Sijin (Policía metropolitana de San José de Cúcuta) y un miembro de la fiscalía General de la Nación perteneciente al área de investigación regional Norte de Santander.

Matriz de Análisis:

La Primera Matriz de análisis desde el reglamento y políticas de la red social Facebook, es importante revisar las Garantías de seguridad en este medio de comunicación de ultima vanguardia, se requiere en esta investigación Entrar en el contexto de la realidad que viven los usuarios respecto al reglamento y políticas de la red social Facebook.

La segunda Matriz de análisis derecho comparado sobre los delitos informáticos en Latinoamérica, se requiere revisar el Tratamiento de los delitos informáticos en otros estados Latinoamericanos, y así comprender los vacíos jurídicos más relevantes de la legislación en Latinoamérica especialmente la colombiana.

3.5 Técnicas e instrumentos de recolección de datos

Teniendo en cuenta el enfoque cualitativo de tipo hermenéutico que se basa esta investigación, este grupo de investigación, realizará un análisis documental, realizando una matriz de derecho comparado de la legislación de Colombia, y el resto de Estados Latinoamericanos con el fin de entender el tratamiento y los vacíos para contra restar este delitos y brindar una mejor seguridad jurídica a los usuarios de la redes sociales ; e igualmente se realizó un análisis de la norma nacional y reglamento de Facebook.

Los métodos de recuperación, entre los que se cuenta el análisis documental, responden a tres necesidades informativas de los usuarios, en primer lugar, conocer lo que otros pares científicos han hecho o están realizando en un campo específico; en segundo lugar, conocer segmentos específicos de información de algún documento en particular; y por último, conocer la totalidad de información relevante que exista sobre un tema específico. (Vickery, 1970). Al realizar estas matrices de análisis, se busca primeramente conocer el las bases jurídicas y la falla del reglamento interno de esta red social Facebook, igualmente conocer el tratamiento que tiene el tema del delito informático especialmente la estafa a través de las redes sociales y la efectividad de la aplicación normativa y evolución en la legislación colombiana, ecuatoriana y española.

“Igualmente se aplicó la entrevista semiestructurada: que nos permita obtener información precisa por parte de funcionarios de las autoridades competentes del Estado colombiano, la entrevista es una técnica de gran utilidad en la investigación cualitativa para obtener datos; se define como una conversación que se propone un fin determinado distinto al simple hecho de conversar”. (Diccionario de Ciencias de la Educación, Vol. 1. México: Santillana; 1983. p. 208). Con el fin de precisar la realidad sobre la inseguridad jurídica del comprador a través de la red social Facebook en Colombia, esta técnica de entrevista semiestructurada para recolectar la información necesaria y así analizar esta problemática de una forma eficaz. Son técnicas que ayudaran a comprender la realidad que viven los usuarios de las redes sociales como el Facebook.

3.6 Criterios para el análisis de la información

Las entrevistas Semi-Estructuradas: permite obtener información precisa por parte de las autoridades competentes que enfrentan este delito de la estafa a través de las redes sociales, con el fin de precisar si el Estado cumple con brindar una seguridad jurídica a los usuarios y consumidores que utilizan este comercio social, igualmente indagar si las instituciones competentes realizan un trabajo articulado para conseguir el cumplimiento de la norma. Igualmente se ha realizado un trabajo satisfactorio desde la observación y comprensión con estos funcionarios pertenecientes a las autoridades competentes.

La entrevista se define como "una conversación que se propone con un fin determinado distinto al simple hecho de conversar". Es un instrumento técnico de gran utilidad en la investigación cualitativa, para recabar datos. El presente artículo tiene como propósito definir la entrevista, revisar su clasificación haciendo énfasis en la semiestructurada por ser flexible, dinámica y no directiva. Asimismo, se puntualiza la manera de elaborar preguntas, se esboza la manera de interpretarla y sus ventajas. Finalmente, por su importancia en la práctica médicas y en la educación médica, se mencionan ejemplos de su uso (Días, García, Hernández, 2013).

Al estudiar el reglamento interno de la red social de Facebook, se comprenderá que tan seguro están sus usuarios frente a los ciberdelincuentes, igualmente se puedo evidenciar las estrategias implementadas por es medio para que no existan ninguna clase de ilícitos, es importante esta matriz de análisis sobre las políticas y reglamento.

Igualmente se realizó un trabajo comparativo entre la legislación aplicada para este delito en el Estado Colombiano, y los demás Estados restantes antiamericanos. para empoderar a las victimas colombianas de los derechos establecidos y su cumplimiento en los en estas redes sociales, especialmente el Facebook.

3.7 Análisis y procesamiento de la información:

Pregunta 1 ¿Desde la experiencia en su cargo, ¿cuáles son las estrategias aplicadas por las autoridades competentes para contra restar la estafa a través de las redes sociales?	**Categorización**

Categoría: Efectividad de las autoridades contra este delito Estafa de compra venta en Facebook.	**Dimensión:** Estrategias para contrarrestar el delito de estafa de compra venta en Facebook.	**Categoría Abiertas**	**Categorías Axial**
RESPUESTA	**COMENTARIOS**		
INFORMANTE 1: ehh respecto a la primera pregunta ehh las estrategias aplicadas ehh por parte de la policía nacional ehh primero que todo pues esta ehh puede ser eehhhh por medio de la denuncia de la persona que es víctima de los delitos informativos ehh ehh eso es un mecanismo si para que para poder que ehh individualizar la persona que comete este delito llamado ehh se le puede decir hacker si ehh igualmente de una forma abusiva esta la información para sacar un beneficio económico para el sí igualmente individualizando a esta persona se puede judicializar se puede dejar ehh a disposición de la autoridad competente.	Las autoridades competentes de una u otra manera han creado estrategias para contra restar este delito, entre estas estrategias encontramos la página web de la policía nacional, por medio de esta página se capacita a los usuarios de la internet para que no sean víctimas de los ciberdelincuentes,	Existencia de estrategias por parte de las autoridades	Estrategias aplicadas
INFORMANTE 2 bueno desde la experiencia las estrategias aplicadas serian el de la página de la policía que ha implementado una capacitación para una prevenir y una página para denunciar la cibercriminalidad de igual forma pues ehh el cual el cual resalta todos los delitos informáticos y protege al usuario entonces ahí hay algunos sería bueno sería importante que revisaran también esa página de la policía ehh la página de la policía que ha puesto a disposición de la comunidad para proteger ehh que no se comentan delitos informáticos o que la gente los ciudadanos no sean víctimas de todos que de todos los delitos que puedan cometer los medios informáticos.	igualmente se pueden instaurar denuncia en tiempo real. sería importante que revisaran también esa página de la policía. Se debe recordar que en Colombia como en muchos países la tecnología y la ciberdelincuencia avanza más rápido que la legislación.	Avances de las autoridades.	Compromiso de avanzar.

Pregunta 2 ¿Desde su conocimiento, cual es el aporte de la normatividad en brindar garantías jurídicas a los compradores del Facebook?		**Categorización**	
Categoría: Efectividad de las autoridades contra este delito Estafa de compra venta en Facebook.	**Dimensión:** Estrategias para contrarrestar el delito de estafa de compra venta en Facebook.	**Categoría Abiertas**	**Categorías Axial**
RESPUESTA	**COMENTARIOS**		
INFORMANTE 1: ehhh pregunta numero dos desde mi experiencia ehh puedo hablar que el aporte que le puedo hacer a la normatividad ehhh para castigar a aquellas personas que cometen ehhh los delitos informáticos pienso que ehh me parece que esta como un poco ehhh no actualizada si y de pronto se podría decir así que no es como la que el castigo no se hace de una formar ejemplar ni es como de una forma justa si aquellas personas que cometen ese delito porque pienso ehh que de pronto que la que los tiempos van cambiando y la normatividad ehhh de pronto está quedando si ehhh como desactualizada entonces creo que la lo ideal sería buscar ehhh reformar aquella normatividad que se aplique de una forma más eficaz si y que de mejores resultados a aquellas personas que sufren delitos informáticos.	La ley 1273 de 2009 ha sido el aporte más importante para combatir este delito, esta ley castiga a las personas que cometan un delito informático. De esta manera se está protegiendo a los usuarios de la internet, pero la gran pregunta es si esta ley es suficiente ante los avances a paso agigantado de la tecnología y de las formas de delinquir de estos ciberdelincuentes.	Aportes para combatir el delito	Efectividad de la ley
INFORMANTE 2: bueno respecto a las garantías o a la normatividad existente para brindar garantías ehhh está la ley 1273 de 2009 sí que es lo que ha aportado la el estado digamos para proteger para proteger o castigar a la persona que cometa un delito informático o para proteger a la víctima que sea engañada o estafada por un cibercriminal.	La ley trata de proteger o castigar a la persona que cometa un delito informático o para proteger a la víctima que sea engañada o estafada por un cibercriminal.	Avances de la legislación	Normatividad ineficiente

Pregunta 3 ¿Para usted como funcionario disciplinar, la normatividad existente es suficiente para garantizar seguridad jurídica ante la constate evolución de la tecnología?		**Categorización**	
Categoría: Efectividad de las autoridades contra este delito Estafa de compra venta en Facebook.	**Dimensión:** Estrategias para contrarrestar el delito de estafa de compra venta en Facebook.	**Categoría Abiertas**	**Categorías Axial**
RESPUESTA	**COMENTARIOS**		
INFORMANTE 1: desde mi experiencia puedo hablar que la normatividad existente en el país colombiano no es suficiente pues ehhh al momento de poder judicializar si de una manera jurídica ehhh una persona ehh víctima de estos delitos informáticos pues creo que ehhh no es esto eficaz y ni rápida, mucho menos ehh tampoco creo que las personas que cometen estos delitos ehhh reciben el castigo qué se merecen si entonces creo que esta leyes tiene muchos vacíos la normatividad y ley al momento de poderse efectuar de una forma pienso que sería de una forma correcta entonces creo que lo que puedo sugerir es que hubiera como una modificación donde esas personas recibieran el castigo que se merecen.	se puede interpretar que la normatividad existente en el ordenamiento jurídico colombiano no es sufrientemente eficaz para garantizar la seguridad jurídica a los compradores por redes sociales, por lo tanto, es evidente los vacíos que tiene la norma la cual necesita con urgencia una modificación que vaya a la vanguardia con la tecnología.	Garantías para los usuarios del Facebook	Efectividad de la ley
INFORMANTE 2: bueno para mi concepto yo digo que hay un vacío muy grande no porque cada día la tecnología evoluciona y no son suficientes las garantías que brinda el estado para un delito de patrimonio económico más que todo si lo vemos por el lado de hurto por medios informáticos si lo vemos a diario victimas de 100 200 300 millones etc. o así sea como decimos acá en la práctica así sean 100 mil pesos que le roben a uno de la cuenta es plata entonces pues a veces se ven vacíos que si hacen falta reforzar y si es suficiente no, no es suficiente hace falta más tecnología.	No son suficientes las garantías que brinda el estado para un delito de patrimonio económico más que todo si lo vemos por el lado de hurto por medios informáticos si lo vemos a diario victimas que ven afectados	Falta de garantías que brinden seguridad jurídica	Legislación sin efectividad

Pregunta 4 ¿Cuál cree usted como funcionario disciplinar, que es la mayor debilidad de las autoridades competentes para contra restar este accionar delictivo?		**Categorización**	
Categoría: Efectividad de las autoridades contra este delito Estafa de compra venta en Facebook.	**Dimensión:** Estrategias para contrarrestar el delito de estafa de compra venta en Facebook.	**Categoría Abiertas**	**Categorías Axial**
RESPUESTA	**COMENTARIOS**		
INFORMANTE 1: bueno mi aporte ehhh que puedo hacer desde mi experiencia la mayor debilidad que tienen las autoridades competentes ehhh que castigan a estas personas ehhh que cometen los delitos informáticos si y que tienen como herramienta para contrarrestar la estafa de compraventa por ehhh la red social ehhh Facebook ehhh yo creo que es la misma ley si porque esa es la se puede decir que es la la el mecanismo si para ellos poder hacer ehhh la implementación de la ley pero vemos ehh que tiene muchas falencias y tiene muchos vacíos sí que al momento de implementarla ehh no es esto pues lo de la mejor forma que se quisiera hacer no y de la manera ejemplar para que las personas ehhh que son ehhh que comenten esos delitos si reciban ehh de una manera justa sí.	La mayor debilidad vienen primeramente de la ley que tiene muchas falencias y vacíos, en segunda medida de los usuarios que no toman la precaución al momento de hacer la compraventa, es muy difícil para las autoridades o el Estado colocar un investigador o policía para cada compraventa que se realice en redes sociales	La debilidad es de la ley no de las autoridades	Mejor legislación
INFORMANTE 2: debilidad la cuarta debilidad como tal de las autoridades pues no porque pues tampoco el estado como dicen por ahí nos va a poner un investigador o un policía ahí en red para que lo proteja a usted si pueda comprar o no pueda comprar o si es confiable o no más que todo depende del ciudadano o de la persona que va a realizar la compra en internet para tener las precauciones debidas no así como usted va al banco hace sus retiros y pues depende de usted si sale con los rollos a rollos de billetes en la mano a exhibirlos pues la ocasión hace al ladrón en internet pues hay varias formas de establecer cuando una página es segura o no y pues ya depende de la destreza del usuario al hacer las compras y lo que les decía en las primeras preguntas hay algunas precauciones hay algunos tipos de seguridad que brinda la página de la policía que se deben seguir.	La mejor conclusión para esta pregunta es que la gran debilidad es de los mismos usuarios confiados que hacen contratos por redes sin verificar si es real la información que le están suministrando por parte de los ciberdelincuentes.	Usuarios más precavidos y menos confiados	Prevención y precaucion

Pregunta 5 ¿Para usted como funcionario disciplinar, la normatividad existente es suficiente para garantizar seguridad jurídica ante la constate evolución de la tecnología?		**Categorización**	
Categoría: Efectividad de las autoridades contra este delito Estafa de compra venta en Facebook.	**Dimensión:** Estrategias para contrarrestar el delito de estafa de compra venta en Facebook.	**Categoría Abiertas**	**Categorías Axial**
RESPUESTA	**COMENTARIOS**		
INFORMANTE 1: ehhh desde mi experiencia las recomendaciones que les puedo hacer a todas aquellas personas que son ehhh usuarios de la red ehh tecnológica de Facebook al momento de hacer algún tipo de negocio por medio de una compraventa para que no sean estafados pues primero que todo ehh que lo hagan con personas ehhh que sean recomendadas que sean ehhh personas que generen confianza y que realmente de pronto ehh tengan un historial ya ehh con un tiempo moderado si ehhh no con cualquier persona desconocida que pueda llegar a cometer ehhh cualquier tipo de estafa si también ehhh brindar ehhh como segunda recomendación brindar los datos necesarios no excederse en datos que no lo están preguntando y tercero siempre ehhh ser una persona precavida si al momento de hacer estos negocios por Facebook ehh pues esto ya que abundan ehh las personas que comenten estos delitos informáticos.	Las mejores recomendaciones para los usuarios que realizan compraventa por las redes sociales son la siguientes: capacitarse en la página de la policía sobre estos delitos y la forma operandi de los ciberdelincuentes, no dejarse llevar por ofertas tentadoras que al final van a salir estafados, verificar bien la información con otros compradores, la precaución es la mejor estrategia para evitar ser estafados.	Recomendaciones para los usuarios del Facebook	Seguir las recomendación
INFORMANTE 2: como tal recomendaciones que se deben seguir los usuarios de Facebook cuando vayan a realizar compras pues las mimas que se han divulgado en redes sociales no mirar que la pagina o el usuario de Facebook que le van a comprar pues sea un usuario confiable queque que tenga buenas recomendaciones de otros compradores mmmm que otra recomendaciones que ya haya realizado otras ventas con otros usuarios en ocasiones se crean perfiles falsos y se ofrecen productos desconfiar de ese tipo de usuarios de Facebook en el cual le solicitan inmediatamente consignarles.	Seguir las recomendaciones de la página de Facebook y de las autoridades competentes	Prevenir y estar atentos	Cuidado y responsabilidad

Primera matriz de análisis:

SEGURIDAD JURÍDICA DEL COMPRADOR A TRAVÉS DE LA RED SOCIAL FACEBOOK EN COLOMBIA.		
Identificar las garantías de seguridad que tiene el comprador a través de la red social Facebook en Colombia.		
SEGURIDAD DEL FACEBOOK	**RESULTADOS**	**OBSERVACIÓN**
¿Se hace Facebook responsable de lo que se vende en un grupo?	No. Los compradores y vendedores son los responsables de lo que se vende en los grupos de compraventa de Facebook.	Para garantizar una experiencia profesional y segura durante la compra y venta de productos enviados en Facebook, ten en cuenta estas normas en primer lugar. Vendedores: Revisa nuestra Política de comercio antes de publicar un artículo para la venta. Nunca envíes un artículo si no recibiste antes el pago completo. Brinda al comprador información clara sobre el plazo de envío, la empresa de transporte (FedEx, etc.), el estado de la entrega y la información de seguimiento. Usa una opción de pago que brinde protección de compra y verifica las condiciones de uso para garantizar que la transacción se encuentre protegida. Compradores: Consulta el perfil del vendedor para conocer mejor a la persona que vende el artículo. A fin de asegurarte que conoces bien la condición del artículo que estás comprando, envía un mensaje al vendedor para realizar preguntas o solicitar información adicional o imágenes. Investiga cuál es el costo de venta del artículo. Si, al parecer, el vendedor ofrece el artículo a un precio demasiado bajo, es muy probable que haya una razón. Habla con el vendedor sobre tus preferencias de pago y sugiere usar un proveedor de pagos que ofrezca protección para quien realiza la compra. Asegúrate de revisar las condiciones de uso para garantizar que la transacción se encuentre protegida.
Compradores:	Las compras realizadas a través de un grupo de compraventa de Facebook son entre el vendedor y tú. Ten en cuenta que no somos propietarios de los artículos que ofrece un vendedor y que los productos no están en nuestro poder. Si tienes alguna pregunta relacionada con algo que vas a comprar en un grupo de compraventa de Facebook, envía un mensaje al vendedor.	
Vendedores:	Describe claramente los artículos que vendes y asegúrate de cumplir nuestra Declaración de derechos y responsabilidades y nuestras Normas comunitarias. Además, en algunos países, como Alemania, Austria y Suiza, a las personas que venden con fines comerciales se les exige por ley que ofrezcan información sobre su identidad, incluido su nombre, dirección postal, correo electrónico, número de registro o número de IVA. Si no estás seguro de si este requisito se aplica a tu caso, puedes consultar a un abogado especializado en la legislación local.	

RESPONSABILIDAD DEL COMERCIANTE	RESULTADOS	OBSERVACIÓN
Contenido del comerciante	La función del botón Comprar incluye principalmente contenido de Comerciantes (y no de Facebook). Usted acepta que Facebook no garantiza y no es responsable ni responsable de (a) el contenido publicado por los comerciantes u otros terceros a través de la función Comprar botón, incluido el Listado de productos (por ejemplo, precios, imágenes o descripciones) o (b) o cualquier otro contenido, sitios web, materiales, productos o servicios de Comerciantes u otros terceros.	**Si reclamo no prospera hay que demandar** Si usted es engañado, antes de demandar al vendedor, productor o proveedor del producto o servicio debe agotar el requisito de procedibilidad previsto en el numeral 5 del artículo 58 de la Ley 1480 de 2011, el cual consiste en reclamar directamente al productor o proveedor, para lo cual estos expedirán una constancia por escrito que se debe anexar a la demanda. Como alternativa al cumplimiento de este requisito, el consumidor puede citar a una audiencia de conciliación al productor o proveedor y en ese caso anexará a la demanda la constancia o el acta de la audiencia. La responsabilidad por publicidad engañosa opera con la sola demostración de que la publicidad no corresponde a la realidad o que por ser insuficiente tiene la capacidad de inducir a error o confusión al consumidor. La Superintendencia de Industria y Comercio es el organismo competente para conocer de este tipo de demandas por violación a los derechos de los consumidores, por la vía administrativa y jurisdiccional.
Cumplimiento de pedidos, entrega y riesgo de pérdida	Los comerciantes cumplen y envían productos (y no Facebook). El riesgo de pérdida para los Productos que compra es únicamente entre usted y el Comerciante (y no Facebook). Lea la Política de entrega, devolución y disputa y los Términos de comerciante para conocer los términos de entrega. Facebook no se hace responsable de la pérdida, destrucción o daño de los Productos, ya sea durante la entrega o de otro modo.	
Producto	El producto es vendido por el comerciante (y no Facebook). Facebook no fabrica ni vende los Productos. Usted acepta que Facebook no garantiza y no es responsable de los Productos (p. Ej., Facebook no garantiza la calidad, seguridad, legalidad, autenticidad, precisión o confiabilidad del Producto). Si bien Facebook puede ayudarlo con las disputas, tal como se describe a continuación, usted acepta consultar únicamente al Comerciante por cualquier problema o reclamo sobre un Producto.	
Los reembolsos	Lea la Política de entregas, devoluciones y disputas y los Términos de los comerciantes para obtener información sobre los reembolsos.	
No aprobación	La referencia a cualquier producto, servicio, proceso u otra información, por nombre comercial, marca comercial, fabricante, proveedor o de otro modo no constituye ni implica respaldo, patrocinio o recomendación de los mismos por parte de Facebook.	

ACCIONES QUE PUEDE TOMAR FACEBOOK	RESULTADOS	OBSERVACIÓN
Derecho a limitar o restringir el uso	Facebook se reserva el derecho de limitar su capacidad para usar la función Comprar botón o prohibirle que use la función Comprar botón por completo en cualquier momento y sin previo aviso. Cualquier acción de este tipo no lo eximirá de sus obligaciones de pagar por los Productos que haya comprado.	Para los estafadores, la información personal de los consumidores es tan valiosa como el dinero. Ellos usan los datos para comprar productos o robar la identidad de sus víctimas. Para proteger la información personal se recomienda lo siguiente: Comprar en sitios seguros. Al momento de pagar hay que asegurarse que el domicilio del sitio comience con https (la "s" significa que el sitio es seguro). Esto significa que el sitio codifica la información que transmite para protegerla. Tener cuidado al compartir información. No compartir información personal a cambio de regalos u ofertas en línea ya que podrían ser una trampa para obtener datos personales. Asimismo, hay que evitar, cuando sea posible, compartir el número de Seguro Social y no transmitir datos personales por e-mail ya que no es una manera segura de hacerlo. Tener cuidado con las redes wifi públicas. Las redes públicas más seguras son aquellas que requieren que el usuario ingrese una contraseña. De cualquier forma, en las redes wifi públicas siempre hay que usar sitios seguros (que comiencen con https) al hacer compras en Internet. Monitorear las cuentas. Como medida de precaución, siempre hay que revisar las facturas del banco y tarjetas de crédito para asegurarse que todas las compras fueron autorizadas.
Modificación y descontinuación	Facebook se reserva el derecho de modificar, suspender, descontinuar o imponer límites en la función del botón Comprar (o en cualquier parte) en cualquier momento, con o sin previo aviso.	
Consultas	Al utilizar la función Comprar botón, acepta que podemos realizar cualquier consulta que consideremos necesaria, ya sea directamente o a través de terceros, con respecto a su identidad y solvencia.	
Derecho de cancelar	Podemos cancelar cualquier transacción si creemos que la transacción infringe estos Términos de ventas de Facebook o la SRR, o si creemos que hacerlo puede evitar pérdidas financieras.	
Prevención de la pérdida financiera	Con el fin de evitar pérdidas financieras para usted o para nosotros, podemos retrasar un pago por un período de tiempo, o limitar los métodos de pago de una transacción, o limitar su capacidad de realizar una compra, o desactivar su cuenta. También podemos contactar al emisor del método de pago, la policía o los terceros afectados (incluidos otros usuarios) y compartir los detalles de los pagos y / o transacciones, si creemos que hacerlo puede evitar pérdidas financieras o una violación de la ley.	

DISPUTAS	RESULTADOS	OBSERVACIÓN
Asistencia al cliente	Sujeto a las otras Secciones en estos Términos de venta de Facebook, proporcionamos varias herramientas en la función Comprar botón para ayudarlo a comunicarse con el Comerciante para resolver una disputa derivada de la compra de una función Comprar botón. Como se establece a continuación, también podemos proporcionar una mediación informal para facilitar la resolución de una disputa entre usted y el Comerciante.	Para minimizar el riesgo de estafas hay que comprar en sitios de Internet conocidos o de buena reputación. En Internet la buena reputación se mide, en parte, en las calificaciones y comentarios que dejan las personas que han hecho compras ahí. Estos consejos podrían ser útiles al hacer compras por Internet: Usar tarjetas de crédito ya que ofrecen mayores protecciones que las tarjetas de débito. Por ejemplo, el portador de una tarjeta de crédito típicamente es responsable por sólo $50 de cargos no autorizados, si llega a eso. Las tarjetas de débito no ofrecen este tipo de protección. Conocer el precio total a pagar. Antes de hacer clic en "comprar" hay que asegurarse que el precio final incluya todos los cargos, como los costos de envío, seguro e impuestos. También hay que asegurarse que incluya descuentos o cupones. Leer la política de devoluciones. Las devoluciones son parte de la experiencia de hacer compras en línea. Cada comerciante tiene su propia política de devoluciones o intercambios, algunos cobran por el reabastecimiento de productos o por el envío de retorno y esto podría afectar lo que paga el consumidor. No hacer compras en sitios de otros países para evitar problemas, ya que a veces es difícil localizar o hacer devoluciones o intercambios con vendedores en el extranjero. En Estados Unidos el negocio de compras por Internet se rige por las leyes de protección al consumidor y por ende protegen al comprador.
Sin responsabilidad por la transacción	Si realiza una transacción con el comerciante y tiene una disputa sobre el producto que compró, no tenemos ninguna responsabilidad por el producto o la disputa. Nuestra única responsabilidad es proporcionar una plataforma para facilitar la transacción y cualquier servicio de atención al cliente expresamente establecido en estos Términos de venta de Facebook.	
Obligación de notificar con nosotros	Si cree que una transacción no autorizada o problemática ha tenido lugar en su cuenta, usted acepta notificarnos de inmediato, para que podamos tomar medidas para evitar pérdidas financieras. A menos que nos envíe el reclamo dentro de los 30 días posteriores al cobro, habrá renunciado, en la máxima medida permitida por la ley, a todos los reclamos contra nosotros que surjan o se relacionen con la transacción.	
Disputas de Facebook	Usted acepta que cualquier disputa entre usted y Facebook que surja de la función del botón Comprar se manejará de conformidad con las disposiciones sobre disputas en la SRR, incluidas las disposiciones sobre procedimientos de disputas, leyes vigentes y jurisdicción.	
Disputas mercantiles	Usted acepta que cualquier disputa entre usted y el Comerciante que surja de una compra a través del botón Comprar se manejará de acuerdo con la Política de entrega, devolución y disputa. Facebook puede facilitar la resolución de disputas comerciales al proporcionar mediación informal como se describe en la Política de entrega, devolución y disputa. Nos reservamos el derecho de intervenir en cualquier disputa entre usted y el comerciante.	

AVISOS Y ENMIENDAS	RESULTADOS	OBSERVACIÓN
Aviso para usted	Al utilizar la función Comprar botón, acepta que podamos comunicarnos con usted electrónicamente con respecto a sus compras, pagos o cuentas. También podemos proporcionarle avisos publicándolos en nuestro sitio web, o enviándolos a una dirección de correo electrónico o calle que nos proporcionó anteriormente. El sitio web y los avisos por correo electrónico se considerarán recibidos por usted dentro de las 24 horas posteriores a la publicación o envío; los avisos por correo postal se considerarán recibidos dentro de los tres (3) días hábiles posteriores a la fecha de envío.	Te notificaremos antes de realizar cambios en estas condiciones y te daremos la oportunidad de revisar y comentar las condiciones modificadas antes de seguir usando nuestros Servicios. Si realizamos cambios en las políticas, normas u otras condiciones a las que hace referencia esta Declaración o que están incorporadas en ella, podremos indicarlo en la página "Facebook Site Governance". Tu uso continuado de los Servicios de Facebook después de recibir la notificación sobre los cambios en nuestras condiciones, políticas o normas supone la aceptación de las enmiendas.
Aviso a nosotros	1. Salvo que se indique lo contrario, debe enviarnos avisos relacionados con estos Términos de ventas de Facebook por correo postal a: Facebook, A la atención de: Departamento Legal, 1601 Willow Avenue, Menlo Park, California, 94025.	
Directrices de enmienda	Facebook puede actualizar estos Términos de venta de Facebook en cualquier momento sin previo aviso, según lo consideremos necesario en la medida permitida por la ley. Al igual que entre usted y Facebook, los Términos de ventas de Facebook vigentes en el momento en que use la función Comprar botón regirán esa transacción.	

TÉRMINOS ADICIONALES	RESULTADOS	OBSERVACION
Separabilidad	Si alguna parte de estos Términos de venta de Facebook se consideran inválidos o no exigibles, esa parte se interpretará de manera coherente con la ley aplicable para reflejar, en la medida de lo posible, las intenciones originales de las partes, y las partes restantes permanecerán en plena vigencia y efecto	Si infringes la esencia o el espíritu de esta Declaración, creas riesgos de cualquier tipo para Facebook o nos expones a posibles responsabilidades jurídicas, podemos impedirte el acceso a Facebook de forma total o parcial. Te notificaremos por correo electrónico o la próxima vez que intentes acceder a tu cuenta. También puedes eliminar tu cuenta o desactivar tu aplicación en cualquier momento. En tales casos, esta Declaración cesará,
Renuncia	El hecho de que Facebook no haga cumplir ningún derecho o disposición en estos Términos de venta de Facebook no constituirá una renuncia a tal o ninguna otra disposición.	
Fuerza mayor	Facebook no será responsable por el incumplimiento de cualquier obligación debido a causas fuera de su control.	
Cumplimiento de la ley	Acepta cumplir con todas las leyes, estatutos, ordenanzas y normativas aplicables a su uso de la función Comprar botón. Nada en estos Términos de venta de Facebook impedirá que cumplamos con la ley.	
Reserva de derechos	Nos reservamos todos los derechos no otorgados expresamente a usted.	
Encabezados e Interpretación	Hemos proporcionado algunos encabezados de secciones para su conveniencia, pero debe leer cuidadosamente estos Términos de ventas de Facebook para comprender sus derechos y responsabilidades, así como los nuestros. Tal como se utiliza en estos Términos de ventas de Facebook, las palabras "incluir" o "incluir" no están destinadas a limitar, por ejemplo, "incluir" significa "que incluye, pero no se limita a" o "incluye, entre otros".	

Segunda matriz de análisis:

SEGURIDAD JURÍDICA DEL COMPRADOR A TRAVÉS DE LA RED SOCIAL FACEBOOK EN COLOMBIA.				
Comparar la legislación en Latinoamérica sobre los delitos informáticos en especial el delito de la estafa a través de las redes sociales				
DERECHO COMPARADO EN LATINOAMÉRICA SOBRE DELITOS INFORMÁTICOS				
PAÍS	**LEGISLACIÓN**	**CARACTERÍSTICAS DELITOS INFORMÁTICOS**	**FRAUDE O ESTAFA INFORMÁTICA**	**ESTABLECE**
ARGENTINA	Código Penal, Ley 26.388 (2008), Ley 25.326 (2000)	A partir de junio de 2008, la Ley 26.388 conocida como la "ley de delitos informáticos" ha incorporado y realizado una serie de modificaciones al Código Penal argentino. Es decir, la misma no regula este tipo de delitos en un cuerpo normativo separado del Código Penal (CP) con figuras propias o independientes, sino que dicha ley modifica, sustituye e incorpora figuras típicas a diversos artículos del CP actualmente en vigencia. Se modificó el Epígrafe del Capítulo III cuyo nuevo título es "Violación de Secretos y de la Privacidad", Los artículos que modifica o agrega son: 128, 153, 153 bis, 155, 157, 157 bis, 173, 183, 184, 197, 255. El art. 157 bis ya había sido incorporado por la Ley 25.326 de Protección de Datos Personales (2000) pero fue modificado por la Ley 26.388.	**Art. 173 inc. 16**	El que defraudare a otro mediante cualquier técnica de manipulación informática que altere el normal funcionamiento de un sistema informático o la transmisión de datos.
BOLIVIA	Código Penal, Ley 1.768 (1997), Ley 3325 (2006)	La Ley 1.768 realiza una reforma general al Código Penal. Allí incorpora como Capítulo XI, del Título XII, del Libro Segundo del Código Penal, el de "DELITOS INFORMÁTICOS". Dentro de este capítulo, se incorporan 2 artículos: 363 bis y ter, en cuyos textos se tipifica algunos delitos informáticos	**Art. 363 bis**	(MANIPULACIÓN INFORMÁTICA). - El que con la intención de obtener un beneficio indebido para sí o un tercero, manipule un procesamiento o transferencia de datos informáticos que conduzca a un resultado incorrecto o evite un proceso tal cuyo resultado habría sido correcto, ocasionando de esta manera una transferencia patrimonial en perjuicio de tercero, será sancionado con reclusión de uno a cinco años y con multa de sesenta a doscientos días.
BRASIL	Ley 12.737 (2012), Ley 11.829 (2008)	La Ley 12.737 es una ley reciente (año 2012), en la cual se dispone la tipificación criminal de los delitos informáticos y otras providencias. En su regulación incorpora modificaciones para los artículos 154-A, 154-B, 266 y 298. Por su parte, la Ley 11.829 regula el Estatuto de la Niñez y la Adolescencia, para mejorar la lucha contra la producción, venta y distribución de pornografía infantil, así como tipificar como delito la adquisición y posesión de dicho material y otros comportamientos relacionados con la pedofilia en Internet.	**No encontrado.**	NO SE ENCONTRÓ PARA ESTE DELITO

CHILE	Ley 19.223 (1993), Ley 20.009 (2005), Ley 18.168 (2002)	La Ley 19.223 es una ley “Relativa a Delitos Informáticos” de acuerdo a su propio título, donde regula cuatro artículos, desde los cuáles se tipifican varios delitos informáticos. La Ley 20.009 regula la responsabilidad para el caso de robo, hurto o extravío de tarjetas de crédito, en cuyo texto se sancionan algunas conductas relacionadas con estos aspectos. La Ley 18.168 (modificada por diferentes normativas) regula de manera general las telecomunicaciones, incorporando algunos tipos penales sobre la interferencia o captación ilegítima de señales de comunicación.	**No encontrado**	NO SE ENCONTRÓ PARA ESTE DELITO
COLOMBIA	Ley 1.273 (2009), Ley 1366 (2009)	La ley 1.273, de reciente sanción legislativa (año 2009), modifica el Código Penal, creando un nuevo bien jurídico tutelado denominado "de la protección de la información y de los datos”. Se afirma que dicha normativa busca preservar integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones. A través de esta incorporación, suma el CAPITULO I, titulado "De los atentados contra la confidencialidad, la integridad y la disponibilidad de los datos y de los sistemas informáticos", a partir del cual regula una serie de artículos penales que van desde el artículo 269A hasta el artículo 269J. Adicionalmente se incorpora el artículo 58, considerando como agravante general “si la realización de alguna de las conductas punibles, se realicen utilizando medios informáticos, electrónicos o telemáticos”.	**Art. 269J**	Transferencia no consentida de activos. El que, con ánimo de lucro y valiéndose de alguna manipulación informática o artificio semejante, consiga la transferencia no consentida de cualquier activo en perjuicio de un tercero, siempre que la conducta no constituya delito sancionado con pena más grave, incurrirá en pena de prisión de cuarenta y ocho (48) a ciento veinte (120) meses y en multa de 200 a 1.500 salarios mínimos legales mensuales vigentes. La misma sanción se le impondrá a quien fabrique, introduzca, posea o facilite programa de computador destinado a la comisión del delito descrito en el inciso anterior, o de una estafa. Si la conducta descrita en los dos incisos anteriores tuviere una cuantía superior a 200 salarios mínimos legales mensuales, la sanción allí señalada se incrementará en la mitad.

COSTA RICA	Ley 9.048 (2012)	La Ley 9048 es una modificación importante del Código Penal de este país. Inicialmente reforma los artículos 167, 196, 196 bis, 214, 217 bis, 229 bis y 288 de la Ley Nº 4573. Por otro lado adiciona el inciso 6) al artículo 229 y un artículo 229 ter. Finalmente modifica la sección VIII del título VII del Código Penal, titulándolo "Delitos informáticos y conexos", donde regula desde el art. 230 hasta el art. 236. En esta modificación bastante integral, agrega una importante cantidad de delitos informáticos al Código Penal, desde los más tradicionales hasta algunos más modernos como la Suplantación de Identidad (art. 230) o el espionaje cibernético (art. 231).	**217 bis**	Estafa informática Se impondrá prisión de tres a seis años a quien, en perjuicio de una persona física o jurídica, manipule o influya en el ingreso, en el procesamiento o en el resultado de los datos de un sistema automatizado de información, ya sea mediante el uso de datos falsos o incompletos, el uso indebido de datos, programación, valiéndose de alguna operación informática o artificio tecnológico, o bien, por cualquier otra acción que incida en el procesamiento de los datos del sistema o que dé como resultado información falsa, incompleta o fraudulenta, con la cual procure u obtenga un beneficio patrimonial o indebido para sí o para otro. La pena será de cinco a diez años de prisión, si las conductas son cometidas contra sistemas de información públicos, sistemas de información bancarios y de entidades financieras, o cuando el autor es un empleado encargado de administrar o dar soporte al sistema o red informática o telemática, o bien, que en razón de sus funciones tenga acceso a dicho sistema o red, o a los contenedores electrónicos, ópticos o magnéticos.”
CUBA	Resolución 204/96, Resolución 6/96, Decreto Ley 199/99, Ley de Soberanía Nacional	En este país se ha podido acceder a la Resolución 204/96, la cual dispone el Reglamento sobre la Protección y Seguridad Técnica de los Sistemas Informáticos, junto a la Resolución 6/96 que pone en vigor el Reglamento sobre la Seguridad informática, con medidas establecidas para la protección y seguridad del Secreto Estatal. Por otro lado, el Decreto Ley 199/99 define como objetivo fundamental establecer y regular el Sistema para la Seguridad y Protección de la Información Oficial. Si bien no existe legislación específica para delitos informáticos, se han encontrado distintas posturas en la doctrina. Por un lado, se opina sobre la necesidad de regulación especial en la materia, y por otro se considera que por la forma en que están redactados algunos delitos y por la filosofía del Código cubano de sancionar por los valores atacados y por los medios empleados, los tipos penales ya existentes son aplicables.	**No encontrado**	NO SE ENCONTRÓ PARA ESTE DELITO

ECUADOR	Ley Nº 67/2002 (2002)	La Ley No. 67/2002 regula el Comercio Electrónico, Firmas y Mensajes de datos. En dicha norma, dentro del Capítulo I del Título V, titulado "DE LAS INFRACCIONES INFORMÁTICAS", el art. 57 afirma que "Se considerarán infracciones informáticas, las de carácter administrativo y las que se tipifican, mediante reformas al Código Penal, en la presente ley." En artículo siguiente, agrega y modifica varios artículos al Código Penal, incorporando diferentes figuras de delitos informáticos.	**Art. 563 inc. 2**	"Será sancionado con el máximo de la pena prevista en el inciso anterior y multa de quinientos a mil dólares de los Estados Unidos de Norteamérica, el que cometiere el delito, utilizando medios electrónicos o telemáticos." La pena de prisión de uno a cinco años y multa
EL SALVADOR	Decreto 1030 / 1997 (1997)	No se ha encontrado legislación específica en la materia. No obstante, posee la adaptación de ciertos delitos clásicos a las nuevas modalidades informáticas. Entre ellos, se pueden mencionar los artículos siguiente: 172, 185, 186, 190, 208 No.2, 216, 222 No. 2,228, 230, 231 y 302 del Código Penal de El Salvador.	**Art. 216 inc. 5**	ESTAFA AGRAVADA Cuando se realizare manipulación que interfiera el resultado de un procesamiento o transmisión informática de datos. Art. 215.- El que obtuviere para si o para otro un provecho injusto en perjuicio ajeno, mediante ardid o cualquier otro medio de engañar o sorprender la buena fe, será sancionado con prisión de dos a cinco años si la defraudación fuere mayor de doscientos colones.
GUATEMALA	Código Penal	Dentro del Código Penal, posee el Capítulo VII, titulado "De los delitos contra el derecho de autor, la propiedad industrial y delitos informáticos". Allí incorpora distintos artículos penales para las figuras de los delitos informáticos, en especial desde el artículo 274 inc. A hasta el inciso G.	**No encontrado**	NO SE ENCONTRÓ PARA ESTE DELITO
HAITI	no se encontró	No se ha encontrado legislación sobre la materia	**No encontrado**	NO SE ENCONTRÓ PARA ESTE DELITO
HONDURAS	Código Penal; Decreto 144/83	Si bien no se ha encontrado legislación especial en la materia, si posee la adaptación de ciertos delitos clásicos a las nuevas modalidades informáticas. Entre ellos podremos encontrar los artículos 214, 215, 223 y 254. Por otro lado, el Decreto 144/83 incorpora algunos delitos para tipificar la pornografía infantil a través del art. 149 y sus incisos al Código Penal.	**No encontrado**	NO SE ENCONTRÓ PARA ESTE DELITO
MEXICO	Reforma 75 del Código Penal Federal (1999)	Mediante reformas se crearon en el Código Penal Federal, los artículos 211 bis 1 al 211 bis 7, que buscaron tipificar los delitos informáticos clásicos teniendo en consideración la fecha de su incorporación. Se destaca la diferente que atentan contra los sistemas de cómputo que pueden o no, ser parte del sector financiero mexicano. Es importante destacar, que algunos Estados Mexicanos tienen además sus propias normas penales, incorporando otros delitos informáticos no analizados en este trabajo.	**No encontrado**	NO SE ENCONTRÓ PARA ESTE DELITO
NICARAGUA	no se encontró	No se ha encontrado legislación sobre la materia.	**No encontrado**	NO SE ENCONTRÓ PARA ESTE DELITO

PANAMÁ	Código Penal y sus reformas; Ley 51 (2008)	No se ha encontrado legislación especial en la materia. No obstante, posee la adaptación de ciertos delitos clásicos a las nuevas modalidades informáticas. Entre ellos pueden citarse los artículos 162 a 165, 180, 184, 185, 220, 237, 260, 283 a 286 y 421. Adicionalmente posee la Ley 51/2008 de Firma Electrónica, en la cual se regula penalmente sobre la falsificación de documentos.	**Art. 226 y 243**	Artículo 226. Quien, para procurarse para sí o para un tercero un provecho ilícito, altere, modifique o manipule programas, bases de datos, redes o sistemas informáticos, en perjuicio de un tercero, será sancionado con cuatro a seis años de prisión. La sanción será de cinco a ocho años de prisión cuando el hecho sea cometido por la persona encargada o responsable de la base de datos, redes o sistema informático o por la persona autorizada para acceder a estos, o cuando el hecho lo cometió la persona valiéndose de información privilegiada. Artículo 243. Quien, en beneficio propio o de un tercero, se apodere, ocasione la transferencia ilícita o haga uso indebido de dinero, valores u otros recursos financieros de una entidad bancaria, empresa financiera u otra que capte o intermedie con recursos financieros del público o que se le hayan confiado, o realice esas conductas a través de manipulación informática, fraudulenta o de medios tecnológicos, será sancionado con prisión de cuatro a seis años. La sanción será de seis a ocho años de prisión, cuando el hecho punible es cometido por un empleado, trabajador, directivo, dignatario, administrador o representante legal de la entidad o empresa, aprovechándose de su posición o del error ajeno.

PARAGUAY	Código Penal – Ley 1.160 (1997), Ley 2.861	No se ha encontrado legislación especial referida a la materia. Sin embargo, a partir de distintas reformas al Código Penal Paraguayo, se han adaptado algunos delitos para la posibilidad de comisión a través de las nuevas tecnologías y en otros casos se ha incorporado tipos penales específicos (como el caso del art. 175 de Sabotaje de Computadoras). Los artículos son 144, 146, 173 a 175, 188, 189, 220, 239, 248 y 249.	**Art. 188**	Operaciones fraudulentas por computadora 1º El que con la intención de obtener para sí o para otro un beneficio patrimonial indebido, influyera sobre el resultado de un procesamiento de datos mediante: 1. programación falsa; 2. utilización de datos falsos o incompletos; 3. utilización indebida de datos; o 4. Otras influencias indebidas sobre el procesamiento, y con ello, perjudicara el patrimonio de otro, será castigado con pena privativa de libertad de hasta cinco años o con multa.
PERÚ	Ley 27.309 (2000), Ley 28.251 (2004)	La Ley 27309 incorpora al Código Penal del Perú los Delitos Informáticos, a través de un artículo único que modifica el Título V del Libro Segundo del Código Penal, promulgado por Decreto Legislativo No 635, introduciendo allí los artículos 207 – A – B y C y 208. En otro orden, la Ley 28.251 actualizó e incorporó distintos delitos contra la integridad sexual, entre ellos, tipificando la pornografía infantil, a través de la modificación del art 183-A. Además Perú posee la Ley 28.493 (2005) que regula el uso del correo electrónico no solicitado (spam), sin embargo en la misma no incluye ningún tipo de sanción penal.	**No encontrado.**	NO SE ENCONTRÓ PARA ESTE DELITO
PUERTO RICO	Ley 146/2012 (Código Penal) + Ley de Espionaje Cibernético 1165 (2008)	No se ha encontrado legislación especial al respecto. Sin embargo, Puerto Rico ha optado por la modificación de los tipos penales clásicos, a fin de adaptarlos para su comisión a través de las nuevas tecnologías. Por otro lado, a través de la Ley de Espionaje Cibernético Nº 1165/2008 si se han incorporado algunos delitos penales especiales para estas figuras relacionados con el espionaje.	**Art. 203**	Fraude por medio informático. Toda persona que con el propósito de defraudar y mediante cualquier manipulación informática consiga la transferencia no consentida de cualquier bien o derecho patrimonial en perjuicio de un tercero o del Estado, será sancionada con pena de reclusión por un término fijo de ocho (8) años. Si la persona convicta es una persona jurídica será sancionada con pena de multa hasta treinta mil dólares ($30,000). El tribunal también podrá imponer la pena de restitución.

REPUBLICA DOMINICANA	Ley Nº 53-07 (2007)	Posee una Ley Especial contra Crímenes y Delitos de Alta Tecnología. Dicha norma regula una parte general, conteniendo algunos principios y conceptos, y posteriormente tipifica los delitos informáticos según el bien jurídico afectado. Además, incluye un capítulo dedicado al aspecto procesal penal, así como en la propia normativa genera un órgano encargado de la recepción de denuncias, investigación y persecución de los delitos informáticos.	**Art. 14 y 15**	art 14. Obtención Ilícita de Fondos. El hecho de obtener fondos, créditos o valores a través del constreñimiento del usuario legítimo de un servicio financiero informático, electrónico, telemático o de telecomunicaciones, se sancionará con la pena de tres a diez años de prisión y multa de cien a quinientas veces el salario mínimo. Artículo 15.- Estafa. La estafa realizada a través del empleo de medios electrónicos, informáticos, telemáticos o de telecomunicaciones, se sancionará con la pena de tres meses a siete años de prisión y multa de diez a quinientas veces el salario mínimo
URUGUAY	Ley 18.600 (2009), Ley 17. 520 (2002), Ley 17.815 (2004), Ley 18.383 (2008), Ley 18.515 (2009)	Si bien no se ha encontrado legislación especial en la materia, se han encontrado diferentes normativas parcialmente aplicables a la materia. El art. 7 de la Ley 17.815, afirma que “constituye delito de comunicación la comisión, a través de un medio de comunicación, de un hecho calificado como delito por el Código Penal o por leyes especiales.”, permitiendo así la aplicación de los tipos clásicos del CP. La Ley N° 17.520, penaliza el uso indebido de señales destinadas exclusivamente a ser recibidas en régimen de abonados. La Ley Nº 17.815 regula la violencia sexual, comercial o no comercial cometida contra niños, adolescentes e incapaces que contenga la imagen o cualquier otra forma de representación.	**No encontrado.**	NO SE ENCONTRÓ PARA ESTE DELITO
VENEZUELA	Gaceta Oficial Nº 37.313 (2001)	Posee una ley especial sobre Delitos Informáticos. Contiene 33 artículos y están clasificados en 5 Capítulos a saber: Contra sistemas que utilizan TI; Contra la propiedad; Contra la privacidad de las personas y las comunicaciones; Contra niños y adolescentes; Contra el orden económico.	**Art. 14**	Fraude. Todo aquel que, a través del uso indebido de tecnologías de información, valiéndose de cualquier manipulación en sistemas o cualquiera de sus componentes, o en la data o información en ellos contenida, consiga insertar instrucciones falsas o fraudulentas, que produzcan un resultado que permita obtener un provecho injusto en perjuicio ajeno, será penado con prisión de tres a siete años y multa de trescientas a setecientas unidades tributarias.

4 RESULTADOS

4.1 Identificación de las garantías del reglamento y de las políticas establecidas por la red social Facebook respecto a la seguridad jurídica para el comprador a través de este medio.

Para el desarrollo de este objetivo, se entró analizar los reglamentos y políticas internas de la red social Facebook, con este trabajo de la matriz de análisis se pudo evidenciar que tan seguros están los usuarios de esta red social que tiene ciento de usuarios a nivel mundial y nacional y que a diario producen cientos de contratos de compraventa.

Una de las principales preocupaciones de este grupo de investigadores es las estafas que se producen cuando algunas personas crean cuentas falsas o hackean las de personas o páginas que te gustan. Para hacer caer a cientos de usuarios con tentadoras ofertas, una problemática que pareciera no tener solución. Son muchas las estrategias que crean los ciberdelincuentes para engañar a los usuarios que no son precavidos o prevenidos.

Los estafadores usan estas cuentas falsas o comprometidas con el fin de engañarte para que les des dinero o información personal. Si recibiste un mensaje que crees que puede ser una estafa, no respondas y reporta el mensaje a Facebook. Siempre va tener una oferta tentadora para hacer caer aquellos usuarios sin prevención.

La gente tiene en Facebook muchas posibilidades, pueden hacer Amigos, chatear, compartir actualizaciones de Estado, postear Comentarios, compartir Links, etiquetar Fotos, postear Videos, unirse a Grupos, crear Páginas, diseñar Polls (encuestas), y jugar juntos usando Aplicaciones. Usan Facebook para promover causas, intereses, e incluso así mimos. Facebook permite al mundo ser más abierto y estar conectado dando a sus usuarios las herramientas para interactuar y compartir de todas las formas imaginables. Parafraseando al superhéroe con un gran poder implicar una gran responsabilidad. Tal y como una ciudad marca sus aceras, y los peatones miran ambos lados de la calle antes de cruzar, la seguridad en Facebook es una responsabilidad compartida entre Facebook y las personas que utilizan su plataforma. (McCarthy, Watson & Weldon, 2014).

Cada día la tecnología crece e igualmente las estrategias de ciberdelincuentes que buscan estafar y engañar, por tal motivo son muchas las modalidades de Estafa y hurto por parte de los ceberlincuente en esta red social, a continuación, puedes ver algunas estafas habituales que puedes encontrar:

Estafas románticas: generalmente, los estafadores románticos envían mensajes a personas que no los conocen, argumentando que se están divorciando, que enviudaron o que su relación de pareja no pasa por un buen momento. Establecerán relaciones en internet con la esperanza de recibir dinero para vuelos o visados. Su objetivo es ganarse tu confianza, por lo que pueden conversar contigo durante semanas antes de pedir dinero alguno (Facebook, 2015). Se debe tener muchas precauciones y no confiar en nadie, en esta modalidad son muchos los usuarios que cae en engaño y estafa sin tener nada que hacer.

Estafas relacionadas con la lotería: este tipo de estafas se llevan a cabo desde cuentas o páginas que se hacen pasar por alguien que conoces o de una organización (por ejemplo, una agencia gubernamental o Facebook). Los mensajes afirmarán que estás entre los afortunados ganadores de un sorteo de lotería y que recibirás una importante suma de dinero a cambio de una pequeña tarifa. Es posible que el estafador te pida que le proporciones información personal, como la dirección postal o los detalles de tu cuenta bancaria (Facebook, 2015). Como se puede evidenciar los ciberdelincuentes se ensañan en todas las estrategias inimaginables para poder concretar su actuación ilícita

Estafas relacionadas con los préstamos: este tipo de estafadores envían mensajes y dejan publicaciones en los que ofrecen préstamos instantáneos con un bajo tipo de interés, a cambio de una pequeña comisión que debe abonarse por adelantado (Facebook, 2015). Son muchas las ofertas tentadoras, se debe tener mucho cuidado y tener mucha precaución por parte de los usuarios, es decir existen una serie de irregularidades y vacíos que los ciberdelincuentes se aprovechan para estafar a diarios a cientos de usuarios.

Robo de token de acceso: se compartió un enlace contigo que te pide acceder a tu cuenta o página de Facebook. A pesar de que el enlace pueda parecer que procede de una aplicación legítima, es una forma que tienen algunas personas y empresas de obtener acceso a tu cuenta y difundir spam. Estos modos de delinquir son los más usados y conocidos por la sociedad,

aún falta mucho por hacer, pero la verdadera solución es ser precavidos y mantener la prevención necesaria para no abrir esos espacios que hoy en día se aprovechan estos delincuentes (Facebook, 2015). No se pude seguir cayendo en estas malas conductas de los Estafadores, son cientos de usuarios que a diario caen como víctimas de estos delincuentes que trabajas para mejora sus artimañas.

Muchos usuarios victimas ven este problema como algo que el gobierno nacional es el único culpable, pero no entrar a revisar que la mejor forma para no caer en manos de estos delincuentes es mantener una cultura de prevención y precaución, hay una serie de vacíos e inconvenientes que la legislación no ha podido mejorara por los pasos agigantados que crece la tecnología, es decir la mejor solución es que cada usuaria tome sus propias precauciones y alternativas para mejora su negocios y compraventa en esta red social.

Con este trabajo de investigación se pudo obtener un conjunto de medidas que llevaran a los usuarios a mantener la tranquilidad en el momento de usa esta red social de Facebook para realizar contratos comerciales como la compra venta por lo tanto se entrar a revisar cada una de las medidas estipuladas por Facebook para evitar ser víctima de estafas, presta especial atención a lo siguiente:

Desconfía de las personas que no conozcas y que te pidan dinero. Es humano evitar el peligro. Si ves que un piano te cae encima, automáticamente te quitas de debajo. Si ves un correo de un timador, vas a borrarlo e informar de que es spam. En Facebook, identificar a los timadores es más complicado dado que los mensajes parecen provenir de una persona que conoces y en la que confías. Luego, ¿cómo descubrir una impostura en Facebook? (McCarthy, Watson & Weldon, 2014). Es de suma importancia entrar a revisar y entender cada una de estas medidas o estrategias para mejorar la experiencia como usuarios de las redes sociales en especial la del Facebook.

Muchos de estos ciberdelincuentes siempre piden el dinero por adelantado, por eso siempre ten desconfianza de esas páginas que siguen estas clases de conductas, no se entiende por hay gente que cae y no desconfía de esta clase de actuaciones, se debe tener malicia indígena para hacer esta clase de negociaciones, no caigas en estos errores que

cientos de usuarios lo han hecho, si te piden la plata por adelantado desconfía y mejor verifique la información de la página o el perfil del vendedor antes de enviar el dinero.

Una de las estrategias más usada y que no se entiende por qué muchos usuarios caen en las redes de los ciberdelincuentes es pagar por adelantado por el producto ofrecido, por tal motivo Desconfía de personas que te pidan pagos por adelantado para recibir préstamos, premios u otras ganancias. Como se reseña en esta oportunidad cada una de estrategias de estos ciberdelincuentes, lleva a pensar por que los usuarios son tan ilusos, con solo una propuesta u oferta tentadora, llegan a desembolsar cantidades de dinero sin ninguna precaución o prevención.

Facebook también efectúa comprobaciones para detectar páginas web maliciosas o que envían spam. Si añades WOT a las comprobaciones que efectúa Facebook consigues una herramienta más para tu arsenal contra los hackers. Ambas comprobaciones trabajan juntas proporcionando un sistema de alerta conjunto si intentas visitar una web de la que se ha informado contiene malware, phishing, o spam. (McCarthy, Watson & Weldon, 2014). Se debe tener una cultura y prevención, no se puede seguir confiando en nada y para eso la página de esta red, capacita o enseña cómo evitar ser engañado o estafado por grupos delincuenciales que se ensañan en dañar la confianza de la compraventa por medio del Facebook.

Pero además de delincuentes informáticos propiamente tales, otros tipos de delincuentes han encontrado espacios propicios en los distintos medios de comunicación electrónicos, para desarrollar sus crímenes, como los pedófilos que buscan generar relaciones de confianza online con menores de edad, para luego aprovecharse de ellos hasta llegar a secuestrarlos u asesinarlos. Estafadores, defraudadores, falsificadores, secuestradores, proxenetas, traficantes de armas, de drogas, de personas, de pornografía, de información, sicarios y terroristas que agregan esta tenebrosa lista que utiliza el ciberespacio y las redes para multiplicar sus negocios, sus ilícitas ganancias y manifestaciones criminales (Rodríguez, 2011).

Fraude Informático: Esta acción ilícita consiste en realizar estafas mediante técnicas específicas utilizadas por los delincuentes. Entre los más importantes se encuentra el En las

redes sociales en la actualidad se ofrecen muchos servicios que son aparentes ofertas de fácil acceso y que llaman fácilmente la atención de los usuarios, medios que son utilizados constantemente para generar la consecución de este delito (Rodríguez, 2001). Más que el trabajo que hacen las autoridades, se requiere crear una cultura de prevención entre los usuarios, muchos de estas víctimas no leen ni revisan las políticas y reglamentos de la página Facebook y por tal motivo son víctimas de los delincuentes,

Entre otras de las modalidades de contante uso de engaño y estafa, es aquella conducta donde los usuarios piden a la víctima cambiar de canal y hablar por otros medios, por tal motivo desconfía de personas que te pidan trasladar la conversación a otro canal distinto de Facebook (como otro correo electrónico). La confianza ha sido la principal problemática de los usuarios, muchos caen en las redes sin saber quién está detrás del computador. Debe llamar la atención cuando la otra parte te pide cambiar de canal tales como Messenger o Wasatch.

Los desarrollos de las tecnologías de información y comunicación como las redes sociales generan infinidad de cambios y repercusiones en el comportamiento humano produciendo transformaciones de los ámbitos jurídicos y sociales de todo el mundo. En este artículo se pretende describir los comportamientos que se pueden reconocer como delitos informáticos en dichas redes y como se está adecuando la normatividad en Colombia a este crecimiento constante de las tecnologías de información y comunicación para prevenir, proteger y establecer un adecuado manejo. Para concluir que las nuevas prácticas delictivas en Colombia están a la mano de la aplicación de los avances tecnológicos, pero a pesar de esto en Colombia existen las bases legales a partir de las cuales se puede empezar a combatir las diferentes modalidades de delitos informáticos, analizando e interpretando la norma existente para identificar su alcance, obteniendo así elementos de juicio para desarrollar políticas y estrategias en este tema. (Rodríguez, 2011).

Muchos de estos delincuentes se ganan la confianza de sus víctimas, Desconfía de las personas que afirmen ser amigos o familiares en situaciones de emergencia. Para poder describir y comprender, cuáles de la gran variedad y clases de hechos y actos que se presentan hoy día en las llamadas redes sociales se pueden encuadrar en los delitos informáticos, es necesario saber primero que significa una red social y posteriormente definir

el concepto de delito informático, para caracterizar claramente cuáles de las actividades allí presentes y que desarrollan las personas que hacen parte de estas redes podrían legalmente sancionarse como dichos actos que lesionan los derechos y libertades de las personas y organizaciones. Y así posteriormente encaminar la normatividad de un país hacia el control legal de estas redes para brindarles a todos sus usuarios las herramientas legales específicas para defenderse, prevenir y sancionar este creciente ambiente digital.

Hay que ser más que prevenido, mantener esa cultura de desconfianza con todo aquel usuario o página que ofrece mercancía por esta red social, averiguar primero cuanto tiene de creada y si otros amigos o usuarios ya han comprado con ellos, es imposible determinar realmente quien está detrás de la computadora, pero si hay alternativas que pueden ayudar a identificar parte del perfil y que puedan brindar un poco de confianza.

Las rede sociales son sitios web que ofrecen servicios y funcionalidades de comunicación diversos para mantener en contacto a los usuarios de la red. Se basan en un software especial que integra numerosas funciones individuales: blogs, wikis, foros, chat, mensajería, entre otros, en una misma interfaz y que proporciona la conectividad entre los diversos usuarios de la red. Son redes de relaciones personales, también llamadas comunidades, que proporcionan sociabilidad, apoyo, información y un sentido de pertenencia e identidad social. Estas están conformadas por grupos de personas con algunos intereses similares, que se comunican a través de proyectos. Existe un cierto sentido de pertenencia a un grupo con una cultura común: se comparten unos valores, unas normas y un lenguaje en un clima de confianza (Redes sociales, 2012).

Son muchos los beneficios que trae esta red social, por eso se quiere dejar claridad que no todos los perfiles son falsos o que siempre va ser estafado si hace compraventa por este medio, no por el contrario lo que se busca es mejorar para aprovechar al máximo este medio, pero si se quiere dejar varios consejo para no caer en las redes de los ciberdelincuentes: Mensajes o publicaciones con faltas de ortografía o errores gramaticales, Las páginas representan a empresas grandes, organizaciones o personajes públicos que no están verificados. Hay que estar muy atento y no olvidar la cultura de verificación y desconfianza antes de negociar por esta red social.

4.2 Derecho comparado del tratamiento de los delitos informáticos en Latinoamérica, en especial el delito de la estafa a través de internet y las redes sociales.

De acuerdo a diferentes estudios actuales, los delitos informáticos son los de mayor crecimiento en los últimos años, con una proyección cada vez mayor. La posibilidad de su comisión a través de Internet permite que, sin mayores complicaciones, el delincuente pueda estar en un determinado país, utilizar servicios de otro, para finalmente atacar a una o más víctimas de un tercer país interviniente. Esta característica de tras nacionalidad demanda un desafío para el Derecho y en especial para los sistemas jurídicos penales, que deben concebir la necesidad de ciertos niveles mínimos de coordinación, que permitan un combate eficaz de este tipo de actividad delictiva. En este marco, la presente investigación tiene por objeto analizar la situación de los delitos informáticos en la región, en su aspecto material sustantivo, a través de un desarrollo de derecho comparado sobre los diferentes países de Latinoamérica.

Como metodología, se ha trabajado en la búsqueda y recolección de la legislación vigente en cada país, destacando sus características generales. Desde allí, previa determinación del alcance, se ha configurado la realización de un cuadro comparativo que permite identificar qué países poseen sanción penal de los delitos informáticos más comunes. A modo de conclusión se lograron obtener estadísticas actualizadas con un ranking de países de acuerdo al estado de situación en la regulación penal de los delitos informáticos más importantes, así como la lista de delitos informáticos menos sancionados. (Ignacio, 2015). Es importante saber cada uno de los desarrollos en los estados latinoamericanos para ver los vacíos a nivel nacional.

Las actividades informáticas delictivas están en crecimiento a nivel global, incluyendo a América Latina. El incremento de la delincuencia informática encuentra algunas de sus respuestas en una gran variedad de factores, cuyo desarrollo ya ha sido trabajado ampliamente por la doctrina. El incremento de tecnología disponible, tanto para el delincuente como las víctimas, combinado con el escaso conocimiento o información sobre cómo protegerse de los posibles delitos que se pueden sufrir a través de las nuevas

tecnologías, otorga a los delincuentes las llaves a las puertas de un inmenso campo fértil de potenciales víctimas de ataques.

Por otro lado, el crecimiento sostenido del mercado negro de la información, funciona como motor que impulsa una importante masa de ataques informáticos, principalmente destinados a obtener bases de datos con información personal y datos para poder saber si la victima tiene buen estado económico para caer en las redes de los ciberdelincuentes,

De acuerdo a uno de los estudios de mayor relevancia mundial en delitos informáticos, en el cuál se han entrevistado más de 13.000 adultos en 24 países, para el año 2012, se calculó que los costos directos asociados con los delitos informáticos que afectan a los consumidores en el mundo ascendieron a US$ 110.000 billones en doce meses. El mismo estudio revela que por cada segundo 18 adultos son víctimas de un delito informático, lo que da como resultado más de un millón y medio de víctimas de delitos informáticos cada día, a nivel mundial (Ignacio, 2015).

Como producto de la presente investigación, se han elaborado cuatro tablas con los resultados obtenidos. En la Tabla Nº 1, se puede observar la primera etapa de los resultados, indicándose por país, la legislación vigente y pertinente en materia de delitos informáticos, junto a un breve resumen de las observaciones realizadas sobre el marco jurídico aplicable. La Tabla Nº 2 dispuesta a continuación, es producto del análisis de las normativas citadas, de acuerdo a la metodología y los criterios ya desarrollados en el apartado correspondiente. Dicho cuadro expresa la situación para cada uno de los países, y para cada uno de los delitos informáticos considerados en la investigación, indicándose si se ha encontrado o no una sanción penal que los reprima, y en su caso, cuál sería el artículo aplicable para esa conducta.

Si bien la investigación en toda su extensión incluye los textos completos de cada uno de los artículos señalados en el cuadro, por cuestiones prácticas de la extensión máxima permitida oficialmente por la organización de este Congreso, no ha sido posible su incorporación, dejándose solamente indicando el artículo. Posteriormente, y basados en los resultados de las primeras dos tablas, se han generado otras dos tablas a partir de cálculos estadísticos

Por tal motivo se entrar analizar cada uno de los países latinoamericanos para entrar en contesto de que pasa en casa país:

Argentina; A partir de junio de 2008, la Ley 26.388 conocida como la “ley de delitos informáticos” ha incorporado y realizado una serie de modificaciones al Código Penal argentino. Es decir, la misma no regula este tipo de delitos en un cuerpo normativo separado del Código Penal (CP.) con figuras propias o independientes, sino que dicha ley modifica, sustituye e incorpora figuras típicas a diversos artículos del CP. actualmente en vigencia. Se modificó el Epígrafe del Capítulo III cuyo nuevo título es "Violación de Secretos y de la Privacidad", Los artículos que modifica o agrega son: 128, 153, 153, 155, 157, 157 bis, 173, 183, 184, 197, 255. El art. 157, ya había sido incorporado por la Ley 25.326 de Protección de Datos Personales (2000) pero fue modificado por la Ley 26.388.

Argentina es unos de los Estados donde mayor incidencia ha hecho la ley, es decir ha sido un referente para muchos Estados, no se puede olvidar que este país ha tenido reconocimiento por su labor tanto legislativa como de sus autoridades para brindar una mejor seguridad jurídica de los usuarios de las redes sociales que desean hacen compraventa.

Bolivia; la Ley 1.768 realiza una reforma general al Código Penal. Allí incorpora como Capítulo XI, del Título XII, del Libro Segundo del Código Penal, el de "DELITOS INFORMÁTICOS". Dentro de este capítulo, se incorporan 2 artículos: 363 bis y ter, en cuyos textos se tipifica algunos delitos informáticos. El estado boliviano tiene un atraso para brindar protección a sus ciudadanos.

Brasil; La Ley 12.737 es una ley reciente (año 2012), en la cual se dispone la tipificación criminal de los delitos informáticos y otras providencias. En su regulación incorpora modificaciones para los artículos 154-A, 154-B, 266 y 298. Por su parte, la Ley 11.829 regula el Estatuto de la Niñez y la Adolescencia, para mejorar la lucha contra la producción, venta y distribución de pornografía infantil, así como tipificar como delito la adquisición y posesión de dicho material y otros comportamientos relacionados con la pedofilia en Internet. Es un referente importante para la legislación de otros Estados. (Ignacio, 2015).

Chile; La Ley 19.223 es una ley “Relativa a Delitos Informáticos” de acuerdo a su propio título, donde regula cuatro artículos, desde los cuáles se tipifican varios delitos informáticos.

La Ley 20.009 regula la responsabilidad para el caso de robo, hurto o extravío de tarjetas de crédito, en cuyo texto se sancionan algunas conductas relacionadas con estos aspectos. La Ley 18.168 (modificada por diferentes normativas) regula de manera general las telecomunicaciones, incorporando algunos tipos penales sobre la interferencia o captación ilegítima de señales de comunicación.

Costa Rica; La Ley 9048 es una modificación importante del Código Penal de este país. Inicialmente reforma los artículos 167, 196, 196 bis, 214, 217 bis, 229 bis y 288 de la Ley Nº 4573. Por otro lado adiciona el inciso 6) al artículo 229 y un artículo 229 ter. Finalmente modifica la sección VIII del título VII del Código Penal, titulándolo "Delitos informáticos y conexos", donde regula desde el art. 230 hasta el art. 236. En esta modificación bastante integral, agrega una importante cantidad de delitos informáticos al Código Penal, desde los más tradicionales hasta algunos más modernos como la Suplantación de Identidad (art. 230) o el espionaje cibernético (art. 231).

Cuba; En este país se ha podido acceder a la Resolución 204/96, la cual dispone el Reglamento sobre la Protección y Seguridad Técnica de los Sistemas Informáticos, junto a la Resolución 6/96 que pone en vigor el Reglamento sobre la Seguridad informática, con medidas establecidas para la protección y seguridad del Secreto Estatal. Por otro lado, el Decreto Ley 199/99 define como objetivo fundamental establecer y regular el Sistema para la Seguridad y Protección de la Información Oficial. Si bien no existe legislación específica para delitos informáticos, se han encontrado distintas posturas en la doctrina. Por un lado, se opina sobre la necesidad de regulación especial en la materia, y por otro se considera que por la forma en que están redactados algunos delitos y por la filosofía del Código cubano de sancionar por los valores atacados y por los medios empleados, los tipos penales ya existentes son aplicables.

Ecuador; La Ley No. 67/2002 regula el Comercio Electrónico, Firmas y Mensajes de datos. En dicha norma, dentro del Capítulo I del Título V, titulado "DE LAS INFRACCIONES INFORMÁTICAS", el art. 57 afirma que "Se considerarán infracciones informáticas, las de carácter administrativo y las que se tipifican, mediante reformas al Código Penal, en la presente ley." En artículo siguiente, agrega y modifica varios artículos al Código Penal, incorporando diferentes figuras de delitos informáticos.

El Salvador; No se ha encontrado legislación específica en la materia. No obstante, posee la adaptación de ciertos delitos clásicos a las nuevas modalidades informáticas. Entre ellos, se pueden mencionar los artículos siguiente: 172, 185, 186, 190, 208 No.2, 216, 222 No. 2, 228, 230, 231 y 302 del Código Penal de El Salvador.

Guatemala; Dentro del Código Penal, posee el Capítulo VII, titulado "De los delitos contra el derecho de autor, la propiedad industrial y delitos informáticos". Allí incorpora distintos artículos penales para las figuras de los delitos informáticos, en especial desde el artículo 274 inc. A hasta el inciso G.

Haití; unos de los países que llama la atención porque no tiene ni avances tecnológicos pero desde allí se produce muchos hechos delictivos, igualmente que África y países europeos. Es un país muy pobre en tecnología pero con grandes avances delictivos, no se puede desarrollar esta investigación sin seguir avanzando en otros Estados latinoamericanos.

Honduras; Si bien no se ha encontrado legislación especial en la materia, si posee la adaptación de ciertos delitos clásicos a las nuevas modalidades informáticas. Entre ellos podremos encontrar los artículos 214, 215, 223 y 254. Por otro lado, el Decreto 144/83 incorpora algunos delitos para tipificar la pornografía infantil a través del art. 149 y sus incisos al Código Penal.

México; Mediante reformas se crearon en el Código Penal Federal, los artículos 211 al, que buscaron tipificar los delitos informáticos clásicos teniendo en consideración la fecha de su incorporación. Se destaca la diferente que atentan contra los sistemas de cómputo que pueden o no, ser parte del sector financiero mexicano. Es importante destacar, que algunos Estados Mexicanos tienen además sus propias normas penales, incorporando otros delitos informáticos no analizados en este trabajo.

Panamá; No se ha encontrado legislación especial en la materia. No obstante, posee la adaptación de ciertos delitos clásicos a las nuevas modalidades informáticas. Entre ellos pueden citarse los artículos 162 a 165, 180, 184, 185, 220, 237, 260, 283 a 286 y 421. Adicionalmente posee la Ley 51/2008 de Firma Electrónica, en la cual se regula penalmente sobre la falsificación de documentos.

Paraguay; No se ha encontrado legislación especial referida a la materia. Sin embargo, a partir de distintas reformas al Código Penal Paraguayo, se han adaptado algunos delitos para la posibilidad de comisión a través de las nuevas tecnologías y en otros casos se ha incorporado tipos penales específicos (como el caso del art. 175 de Sabotaje de Computadoras). Los artículos son 144, 146, 173 a 175, 188, 189, 220, 239, 248 y 249.

Perú; La Ley 27309 incorpora al Código Penal del Perú los Delitos Informáticos, a través de un artículo único que modifica el Título V del Libro Segundo del Código Penal, promulgado por Decreto Legislativo No 635, introduciendo allí los artículos 207 – A – B y C y 208. En otro orden, la Ley 28.251 actualizó e incorporó distintos delitos contra la integridad sexual, entre ellos, tipificando la pornografía infantil, a través de la modificación del art 183-A. Además Perú posee la Ley 28.493 (2005) que regula el uso del correo electrónico no solicitado (spam), sin embargo en la misma no incluye ningún tipo de sanción penal.

Puerto Rico; No se ha encontrado legislación especial al respecto. Sin embargo, Puerto Rico ha optado por la modificación de los tipos penales clásicos, a fin de adaptarlos para su comisión a través de las nuevas tecnologías. Por otro lado, a través de la Ley de Espionaje Cibernético Nº 1165/2008 si se han incorporado algunos delitos penales especiales para estas figuras relacionados con el espionaje.

República Dominicana; Posee una Ley Especial contra Crímenes y Delitos de Alta Tecnología. Dicha norma regula una parte general, conteniendo algunos principios y conceptos, y posteriormente tipifica los delitos informáticos según el bien jurídico afectado. Además, incluye un capítulo dedicado al aspecto procesal penal, así como en la propia normativa genera un órgano encargado de la recepción de denuncias, investigación y persecución de los delitos informáticos.

Uruguay; Si bien no se ha encontrado legislación especial en la materia, se han encontrado diferentes normativas parcialmente aplicables a la materia. El art. 7 de la Ley 17.815, afirma que “constituye delito de comunicación la comisión, a través de un medio de comunicación, de un hecho calificado como delito por el Código Penal o por leyes especiales.”, permitiendo así la aplicación de los tipos clásicos del CP. La Ley N° 17.520, penaliza el uso indebido de

señales destinadas exclusivamente a ser recibidas en régimen de abonados. La Ley Nº 17.815 regula la violencia sexual, comercial o no comercial cometida contra niños, adolescentes e incapaces que contenga la imagen o cualquier otra forma de representación.

Venezuela; Posee una ley especial sobre Delitos Informáticos. Contiene 33 artículos y están clasificados en 5 Capítulos a saber: Contra sistemas que utilizan TI; Contra la propiedad; Contra la privacidad de las personas y las comunicaciones; Contra niños y adolescentes; Contra el orden económico.

Por último se revisara la legislación Colombiana; La ley 1.273, de reciente sanción legislativa (año 2009), modifica el Código Penal, creando un nuevo bien jurídico tutelado denominado "de la protección de la información y de los datos". Se afirma que dicha normativa busca preservar integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones. A través de esta incorporación, suma el CAPITULO I, titulado "De los atentados contra la confidencialidad, la integridad y la disponibilidad de los datos y de los sistemas informáticos", a partir del cual regula una serie de artículos penales que van desde el artículo 269A hasta el artículo 269J. Adicionalmente se incorpora el artículo 58, considerando como agravante general "si la realización de alguna de las conductas punibles, se realicen utilizando medios informáticos, electrónicos o telemáticos".

4.3 Indagación sobre la efectividad de las autoridades competentes para contra restar el accionar de los estafadores por medio de la red social Facebook en Colombia.

En Colombia no existe una ley que determine específicamente tipos penales que definan los delitos que se presentan con mayor frecuencia en Colombia en las redes sociales, lo que es necesario para sancionar correctamente estas modalidades delictivas que afectan una sociedad completa. En este país se deben diseñar políticas criminales encaminadas a prevenir la realización de estos delitos, políticas que tengan como base la enseñanza a la comunidad del correcto uso y manejo de las redes sociales para de esta forma minimizar los riesgos existentes en ellas.

Los delitos informáticos son conductas que día a día se presentan en mayor cantidad en las redes sociales afectando gravemente derechos constitucionales prácticamente de todos los miembros de la sociedad. Se deben hacer trabajos contundentes que mejores la seguridad jurídica de los colombianos.

La seguridad en las redes sociales y el suministro de información personal debe hacerse con todas las precauciones necesarias, y para que los usuarios de las redes tengan esta conciencia, los mecanismos y organismos del estado deben ayudar a crear una nueva cultura que conlleve a las personas a protegerse en este espacio digital que puede afectar fácilmente la vida e integridad de cada ciudadano. las nuevas tecnologías de información y comunicación como las redes sociales además de ser el medio donde se presentan delitos como bullying, phising, perfiles falsos, pornografía infantil, y toda clase de daños, fraudes y robos informáticos, también es el medio que están utilizando delincuentes comunes para llegar a la realización de delitos clásicos que se comenten personalmente como; secuestros, amenazas, estafas, acosos, hurtos, entre otros (Rodríguez, 2011).

El constante avance tecnológico y el avance de los delitos a la par de las nuevas formas de comunicación en el mundo no deben estar separadas de las correspondientes reformas y creaciones legales, nuevas normas que abarquen y contemplen las posibles vulneraciones a los derechos constitucionales para que las personas puedan tener opciones y medios dónde acudir para denunciar y protegerse frente a cualquier delito en las redes sociales.

Se entrara rápidamente a ver conceptos de delitos informáticos para entrar en contexto de lo que pasa en Colombia, para empezar se revisara a Julio Téllez Valdez (2007) en su libro derecho informático, enfoca el delito informático desde el punto de vista típico y atípico y lo define como “actitud contraria a los intereses de las personas en que se tiene a los computadores como instrumento o fin (concepto atípico) o las conductas típicas, antijurídica o culpables en las que se tienen los computadores como instrumento o fin.

Alberto Suarez Sánchez (2009), por su parte señala: “en conclusión, el delito informático está vinculado no solo a la realización y una conducta delictiva a través de miembros o elementos informáticos, o a los comportamientos ilícitos en los que aquellos sean su objeto,

sino también a la afectación de la información per se cómo bien jurídico tutelado, diferente de los intereses jurídicos tradicionales.

Rodríguez (2007) el delito informático es la realización de una acción que, reuniendo las características que delimitan el concepto delito sea llevada a cabo utilizando un elemento informático y/o telemático, o vulnere los derechos del titular de un elemento informático.

La constitución política establece normalmente normas que tocan directamente con la información y por ende se convierten en el sustento de firmeza superior para fundar los llamados delitos informaticos.es así como encontramos en el artículo 15 de la Carta, en lo concerniente a la intimidad de las personas y el artículo 20 relativo al derecho de información. Artículo 15. Todas las personas tienen derecho a su intimidad personal y familiar y a su buen nombre, y el Estado debe respetarlos y hacerlos respetar. De igual modo, tienen derecho a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en bancos de datos y en archivos de entidades públicas y privadas.

Es entonces claro que la constitución política de Colombia si otorga a través de su principia listica y de normas que consagran derechos fundamentales, tales como los articulo 15 y 20, un respaldo suficiente como para que el legislador consagre normas tendientes a desarrollar lo que se conoce mundialmente como delitos informáticos. En estos artículos se plasma una idea inicial a partir de la cual se puede formular de acuerdo al avance de la tecnología y las comunicaciones una nueva reglamentación que proporcione seguridad jurídica en el uso de las redes sociales frente a los delitos informáticos.

Aspectos jurisprudenciales Las altas corporaciones que tiene dentro de sus funciones la de administrar justicia y velar porque el ordenamiento jurídico no atente contra la carta constitucional, no han tenido una actividad jurisprudencial notoria frente al tema de los llamados delitos informáticos pues no han producidos pautas o líneas jurisprudenciales contundentes y esto se da por la ausencia de normas que estén en esa sintonía tecnológica (Rodríguez, 2012).

El código penal colombiano en su capítulo VII del libro segundo del título III: delitos contra la libertad individual y otras garantías, trata sobre la violación a la intimidad, reserva e interceptación de comunicaciones: Articulo 192. Violación ilícita de comunicaciones.

Artículo 193. Ofrecimiento, venta o compra de instrumento apto para interceptar la comunicación privada entre personas. Artículo 194. Divulgación y empleo de documentos reservados. Artículo 195. Acceso abusivo a un sistema informático. Artículo 196. Violación ilícita de comunicaciones o correspondencia de carácter oficial. Artículo 197. Utilización ilícita de redes de comunicaciones. Estos artículos son concordantes con el artículo 357: "daño en obras en los servicios de comunicaciones, energías y combustibles (Código penal, 599/2000).

Otra norma que habla sobre los delitos informáticos en Colombia fue la ley 679 de 2001, que estableció el estatuto para prevenir y contrarrestar la explotación, la pornografía y el turismo sexual con niños menores de edad. De igual manera, consagra prohibiciones para los proveedores o servidores, administradores o usuarios de redes globales de información, respecto a alojar imágenes, textos, documentos o archivos audiovisuales que exploten a los menores en aptitudes sexuales o pornográficas. Sin embargo, la norma no contiene sanciones legales, si no administrativas, pues siendo simple prohibición, deja un vacío que quita eficacia a la ley, cuando se trata de verdaderos delitos informáticos.

La ley 1273 de 2009 trae importantes figuras tipificadas en las cuales se identifican actuaciones que llegan a convertirse en delitos informáticos presentes en las redes sociales y que tipificación del delito se pueden aplicar a la norma para después exigirse una sanción y así tener un marco jurídico aplicable a las diferentes conductas que se están presentando en las redes sociales que vulneran y afectan los derechos de los diferentes usuarios. Algunas de esas figuras de la ley 1273 de 2009 que se incorporaron al código penal son:

Artículo 1 de la ley 1273 de 2009, incorporar al código penal el artículo 269A y complementa el tema relacionado con "el acceso abusivo a un sistema informático", que se manifiesta cuando el pirata informático o hacker aprovecha la vulnerabilidad en el acceso a los sistemas de información, o las deficiencias en los procedimientos de seguridad informática establecidos por las organizaciones, para extraer beneficios económicos o para indagar o demostrar la capacidad y recursos que ofrece la tecnología de información. Cuando se presenta este abuso, en muchos casos se observa que proviene de los mismos usuarios del sistema y de los empleados.

El articulo 269B contempla como delito la obstaculización ilegitima del sistema informático o redes de telecomunicación y se originan cuando el hacker informático bloquea en forma ilegal un sistema o impide el sistema por un tiempo, hasta cuando tiene un beneficio por lo general económico. Aquí también se enmarca el acceso a cuentas de correo electrónico sin el debido consentimiento de los respectivos usuarios y el manejo o bloqueo de las claves obtenidas de distinta forma. El articulo 269C plantea la infracción relacionada con la "interpretación ilícita de datos informáticos", también considerada en el artículo 3 del título 1 de la convención de Budapest de 2001 (Ley 599, 2000).

Se presenta cuando una persona valiéndose de los recursos tecnológicos, obstruye datos sin autorización legal, en su sitio de origen, en el destino o en el interior de un sistema informático, o de emisiones electromagnéticas de un sistema electromagnético que los trasporte. El delito relacionado con los "daños informáticos" está contemplado en el artículo 269D y se comete cuando una persona que, sin estar autorizada, modifica, altera, daña, borra, destruye o suprime datos del programa o de documentos electrónicos, en los recursos de las TIC. El articulo 269 E contempla el delito vinculado con el "uso de software malicioso" técnicamente denominado malware, ya generalizado en internet. Se presenta cuando se produce, adquieren, venden, distribuyen, envían, introducen o extraen del país software o programas de computador que producen daños en los recursos de las TIC.

Por otro lado, los constantes y permanentes procesos de globalización con sus atractivos avances y posibilidades de desarrollo para toda la humanidad impulsada por la tecnología de las comunicaciones y la informática, se convierten hoy en día en el prototipo perfecto para las relaciones personales y organizacionales de todo el mundo. Llevando esto a que se produzcan cambios importantes en los comportamientos sociales, económicos y políticos de las personas y países, pero también esto lleva al mismo tiempo a un proceso peligroso en el que se desarrolla una nueva delincuencia, que, al utilizar los sistemas de información y comunicación del mundo, lograron posicionarse en uno de los riesgos más inminentes para la seguridad, la vida y la protección de los bienes de las personas y las organizaciones de todos los países.

Colombia frente a estos dos fenómenos actuales, uno positivo como lo es el avance global de la tecnología de información y comunicaciones, y el otro negativo como lo son los

delincuentes y delitos informáticos, como algunos gobiernos de países de todo el mundo que han venido tomando conciencia de la creciente amenaza y han comenzado a implementar avances tecnológicos, jurídicos y sociales para enfrentar fuertemente los riesgos que generan dichos delitos, debe entonces nuestro país diseñar y promover sistemas, destinar inversión, políticas y herramientas de seguridad legal e informática para combatir el delito sin dejar atrás la constante capacitación y preparación especial del talento humano para manejar por parte de los entes jurídicos, informáticos y en general toda la sociedad estas herramientas de seguridad y prevención.

Se debe trabajar en grupo para generar una cultura integral apoyada en los propios recursos que ya existen en el país y sus fortalezas internas, para saber cuáles fortalezas necesitan consolidarse, al lado del conocimiento y el aprovechamiento claro y eficaz del estado, la ley y la sociedad misma, además de buscar el apoyo internacional de mecanismos que aporten en el tema. Entonces, para neutralizar esta creciente ola de delitos informáticos, toda la sociedad acompañada del estado, de los jueces y de todos los administradores de justicia, que deben estar preparados no solo en el conocimiento de la ley y la jurisprudencia, sino en el apropiado conocimiento del contexto tecnológico deben unirse en un objetivo común como una ofensiva contra el delito informático logrando una conciencia organizacional y ciudadana sobre la seguridad informática.

Colombia con la ley 1273 de 2009 logro acceder al grupo de países que se han preparado con herramientas un poco más eficaces para contrarrestar las acciones del cibercriminal en sectores importantes como la economía, la organización financiera y régimen legal. Con este trabajo de delimitación de los riesgos posibles en este tema se puede llegar al camino correcto para diseñar, plasmar estrategias, orientar políticas y crear normas acompañadas de procedimientos que no estén tan limitados y que sean suficientes para que ayuden en el futuro a controlar cualquier amenaza sobre la sociedad en general.

Además de todas estas medidas en Colombia es necesario otro tipo de implementaciones de todo tipo para combatir a tiempo los delitos informáticos. Es necesario en Colombia que existan primordialmente políticas criminales encaminadas a prevenir, proteger y sancionar estas acciones, políticas que después se traduzcan en normas y leyes que tipifiquen toda la variedad de conductas que día a día aparecen y crecen en las redes sociales en Colombia,

normatividades que encuadren en un marco jurídico, tanto, la descripción detallada de cada una de las posibles conductas típicas, las características de los actores que cometen estas conductas y las características de las persona víctimas de las mismas, para posteriormente establecer específicamente las sanciones de dichos delitos.

Por esto para combatir entonces el delito informático y su alta complejidad dada por el constante cambio al que estos se ven expuestos por el desarrollo de las tecnologías de información y comunicación y para evitar que esta clase de delitos sigan vulnerando bienes jurídicos y derechos de toda la sociedad, se deberían crear nuevos tipos penales que protejan los bienes jurídicos que se están viendo afectados como el patrimonio, la información, la privacidad, entre otros, y derechos como el derecho a la intimidad, a la honra, a la libertad, al buen nombre y muchos otros derechos que con las actuaciones de los delincuentes cibernéticos se afectan día a día. Tipos penales que enmarquen específicamente como conductas constitutivas de delitos informáticos comportamientos indebidos en las diferentes modalidades de sistemas informáticos y de comunicación que atenten contra los derechos de las otras personas u organizaciones.

Es cierto, como ya se ha resaltado, que la ley colombiana no define el delito informático como tal, y menos, define las conductas delictivas presentes en las redes sociales, pues lo que se ha hecho es regular ciertos casos relativos a fraudes y accesos no permitidos a sistemas de información, pero es importante tener en cuenta que, a pesar de que no exista una clara definición de que es o no es un delito informático se puede tomar del código penal y el código de procedimiento penal para el manejo de dichos delitos, pues estos traen definidos, delimitados y regulados muchísimos delitos conocidos como delitos clásicos que son susceptibles de ser cometidos en un entorno informático y es allí precisamente, donde el juzgador, los abogados y los investigadores deben encontrar la relación para poder aplicar la ley.

Por último, cabe rescatar que en Colombia se está trabajando en los diferentes organismos de control del estado para tratar de ser proactivos frente a los nuevos delitos informáticos, implementando diferentes unidades de investigación y tratamiento de las denuncias sobre estos delitos para así con miras en resultados específicos tomar medidas de prevención y

sanción, identificando rápidamente acciones que deben tomarse para la consecución de resultados en este tipo de ilícitos.

5 DISCUSIÓN

5.1. La seguridad jurídica del comprador a través de la red social Facebook en el Estado colombiano

Para el desarrollo de este trabajo de investigación, se entró analizar los reglamentos y políticas internas de la red social Facebook, con este trabajo de la matriz de análisis se pudo evidenciar que tan seguros están los usuarios de esta red social que tiene ciento de usuarios a nivel mundial y nacional y que a diario producen cientos de contratos de compraventa.

Una de las principales preocupaciones de este grupo de investigadores es las estafas que se producen cuando algunas personas crean cuentas falsas o hackean las de personas o páginas que te gustan. Para hacer caer a cientos de usuarios con tentadoras ofertas, una problemática que pareciera no tener solución. Son muchas las estrategias que crean los ciberdelincuentes para engañar a los usuarios que no son precavidos o prevenidos.

Los estafadores usan estas cuentas falsas o comprometidas con el fin de engañarte para que les des dinero o información personal. Si recibiste un mensaje que crees que puede ser una estafa, no respondas y reporta el mensaje a Facebook. Siempre va tener una oferta tentadora para hacer caer aquellos usuarios sin prevención.

La gente tiene en Facebook muchas posibilidades, pueden hacer Amigos, chatear, compartir actualizaciones de Estado, postear Comentarios, compartir Links, etiquetar Fotos, postear Videos, unirse a Grupos, crear Páginas, diseñar Polls (encuestas), y jugar juntos usando Aplicaciones. Usan Facebook para promover causas, intereses, e incluso así mimos. Facebook permite al mundo ser más abierto y estar conectado dando a sus usuarios las herramientas para interactuar y compartir de todas las formas imaginables. Parafraseando al superhéroe con un gran poder implicar una gran responsabilidad. Tal y como una ciudad marca sus aceras, y los peatones miran ambos lados de la calle antes de cruzar, la seguridad en Facebook es una responsabilidad compartida entre Facebook y las personas que utilizan su plataforma. (McCarthy, Watson & Weldon, 2014).

A pesar que existe la reglamentación y las políticas internas de la red social Facebook, esta no sirve para mucho, pues está en manos del usuario brindar su propia seguridad y estrategias para no ser víctima de los ciberdelincuentes, esta red social no se hace responsable de muchas conductas que pudiesen controlarse de mejor manera desde la plataforma web.

De acuerdo a diferentes estudios actuales, los delitos informáticos son los de mayor crecimiento en los últimos años, con una proyección cada vez mayor. La posibilidad de su comisión a través de Internet permite que, sin mayores complicaciones, el delincuente pueda estar en un determinado país, utilizar servicios de otro, para finalmente atacar a una o más víctimas de un tercer país interviniente. Esta característica de tras nacionalidad demanda un desafío para el Derecho y en especial para los sistemas jurídicos penales, que deben concebir la necesidad de ciertos niveles mínimos de coordinación, que permitan un combate eficaz de este tipo de actividad delictiva. En este marco, la presente investigación tiene por objeto analizar la situación de los delitos informáticos en la región, en su aspecto material sustantivo, a través de un desarrollo de derecho comparado sobre los diferentes países de Latinoamérica.

Como metodología, se ha trabajado en la búsqueda y recolección de la legislación vigente en cada país, destacando sus características generales. Desde allí, previa determinación del alcance, se ha configurado la realización de un cuadro comparativo que permite identificar qué países poseen sanción penal de los delitos informáticos más comunes. A modo de conclusión se lograron obtener estadísticas actualizadas con un ranking de países de acuerdo al estado de situación en la regulación penal de los delitos informáticos más importantes, así como la lista de delitos informáticos menos sancionados. (Ignacio, 2015). Es importante saber cada uno de los desarrollos en los estados latinoamericanos para ver los vacíos a nivel nacional.

Las actividades informáticas delictivas están en crecimiento a nivel global, incluyendo a América Latina. El incremento de la delincuencia informática encuentra algunas de sus respuestas en una gran variedad de factores, cuyo desarrollo ya ha sido trabajado ampliamente por la doctrina. El incremento de tecnología disponible, tanto para el delincuente como las víctimas, combinado con el escaso conocimiento o información sobre

cómo protegerse de los posibles delitos que se pueden sufrir a través de las nuevas tecnologías, otorga a los delincuentes las llaves a las puertas de un inmenso campo fértil de potenciales víctimas de ataques.

En Colombia no existe una ley que determine específicamente tipos penales que definan los delitos que se presentan con mayor frecuencia en Colombia en las redes sociales, lo que es necesario para sancionar correctamente estas modalidades delictivas que afectan una sociedad completa. -En nuestro país se deben diseñar políticas criminales encaminadas a prevenir la realización de estos delitos, políticas que tengan como base la enseñanza a la comunidad del correcto uso y manejo de las redes sociales para de esta forma minimizar los riesgos existentes en ellas.

Los delitos informáticos son conductas que día a día se presentan en mayor cantidad en las redes sociales afectando gravemente derechos constitucionales prácticamente de todos los miembros de la sociedad. Se deben hacer trabajo contundente que mejores la seguridad jurídica de los colombianos.

La seguridad en las redes sociales y el suministro de información personal debe hacerse con todas las precauciones necesarias, y para que los usuarios de las redes tengan esta conciencia, los mecanismos y organismos del estado deben ayudar a crear una nueva cultura que conlleve a las personas a protegerse en este espacio digital que puede afectar fácilmente la vida e integridad de cada ciudadano. -las nuevas tecnologías de información y comunicación como las redes sociales además de ser el medio donde se presentan delitos como bullying, phising, perfiles falsos, pornografía infantil, y toda clase de daños, fraudes y robos informáticos, también es el medio que están utilizando delincuentes comunes para llegar a la realización de delitos clásicos que se comenten personalmente como; secuestros, amenazas, estafas, acosos, hurtos, entre otros (Rodríguez, 2011).

El constante avance tecnológico y el avance de los delitos a la par de las nuevas formas de comunicación en el mundo no deben estar separadas de las correspondientes reformas y creaciones legales, nuevas normas que abarquen y contemplen las posibles vulneraciones a los derechos constitucionales para que las personas puedan tener opciones y medios dónde acudir para denunciar y protegerse frente a cualquier delito en las redes sociales.

La ley 1273 de 2009 trae importantes figuras tipificadas en las cuales se identifican actuaciones que llegan a convertirse en delitos informáticos presentes en las redes sociales y que tipificación del delito se pueden aplicar a la norma para después exigirse una sanción y así tener un marco jurídico aplicable a las diferentes conductas que se están presentando en las redes sociales que vulneran y afectan los derechos de los diferentes usuarios. Algunas de esas figuras de la ley 1273 de 2009 que se incorporaron al código penal son:

Artículo 1 de la ley 1273 de 2009, incorporar al código penal el artículo 269A y complementa el tema relacionado con "el acceso abusivo a un sistema informático", que se manifiesta cuando el pirata informático o hacker aprovecha la vulnerabilidad en el acceso a los sistemas de información, o las deficiencias en los procedimientos de seguridad informática establecidos por las organizaciones, para extraer beneficios económicos o para indagar o demostrar la capacidad y recursos que ofrece la tecnología de información. Cuando se presenta este abuso, en muchos casos se observa que proviene de los mismos usuarios del sistema y de los empleados.

Este trabajo es de suma importancia por el aporte que da para todos los usuarios a nivel general, la idea es que no sigan cayendo en las redes de los ciberdelincuentes, y que a pesar que existe una normatividad en el país y modificaciones al código penal, la verdadera solución está en mano de cada uno de nosotros, se debe ser más prevenidos y precavidos a la hora de negociar o hacer compraventa por esta res social.

Se deja un buen aporte para todos los usuarios de esta red social de Facebook este trabajo dejo entrever, primeramente, que esta red social debe realizar un mejor trabajo con respecto a la reglamentación y políticas de sanción, a nivel de Latinoamérica falta mucho trabajo para contra restar este delito y brindar confiabilidad a los usuarios de Facebook, hay Estados que aún no han legislado y dejan a sus asociados en manos de los ciberdelincuentes, y por último en Colombia las autoridades competentes realizan a diarios un trabajo de prevención y a diarios eliminan redes de delincuentes pero la ley es insuficiente para dar el castigo ejemplar.

6 CONCLUSIONES

Los reglamentos y las políticas internas de la red social Facebook, hacen un conjunto de estrategias que evitan de alguna manera a que los usuarios sean víctimas de engaños o estafas, pero más que estas reglas, se puede concluir que lo que verdaderamente pude ayudar a contra restar esta problemática es mantener una cultura de prevención y precaución, ya que son imaginable las estrategias usada por los ciberdelientes.

Muchos usuarios no les interesan las políticas ni las reglas de la página, razón por la cual son presa fácil para los ciberdelincuentes, hay que hacer más realistas de la vulnerabilidad siempre que se está haciendo negocios o compraventa por medio de esta red social; la verdad es que no siempre es culpa de la ley sino de los usuarios mal informados y confiados que no proveen el peligro de negociar por este medio.

A nivel general se puede concluir que en Latinoamérica se mantienen Normatividad exclusiva para lograr la seguridad jurídica de los usuarios de Facebook. Pero que hay mucho por hacer, hay países como Paraguay, Haití entre otros que la legislación no se ha interesado por mejorar y aceptar la problemática que viven sus ciudadanos.

En Colombia, existe una preocupación desde el legislador, se han hecho modificaciones al código penal y se trata de mejorar día a día, el inconveniente está en que la tecnología avanza a pasos agigantados, en cambio las leyes y legislación ha quedado un poco atrasada para hacer un trabajo eficaz frente a los ciberdelincuentes.

En Colombia no existe una ley que determine específicamente tipos penales que definan los delitos que se presentan con mayor frecuencia en Colombia en las redes sociales, lo que es necesario para sancionar correctamente estas modalidades delictivas que afectan una sociedad completa. -En nuestro país se deben diseñar políticas criminales encaminadas a prevenir la realización de estos delitos, políticas que tengan como base la enseñanza a la comunidad del correcto uso y manejo de las redes sociales para de esta forma minimizar los riesgos existentes en ellas.

En Colombia se está trabajando en los diferentes organismos de control del estado para tratar de ser proactivos frente a los nuevos delitos informáticos, implementando diferentes unidades de investigación y tratamiento de las denuncias sobre estos delitos para así con miras en resultados específicos tomar medidas de prevención y sanción, identificando rápidamente acciones que deben tomarse para la consecución de resultados en este tipo de ilícitos.

7 RECOMENDACIONES

Que Facebook cree una mejor manera para que los antes de crear una cuenta en esta red social, verdaderamente lean el reglamento y las políticas y así mejorar la cultura de los ciudadanos ante la gran abundancia de delitos informáticos a través de esta red social, muchos le dan acepto a los reglamentos, pero no los leen como debería ser.

Recomendarle a la red social de Facebook, que realice videos y publicaciones gráficas para llegar a todos sus usuarios como estrategia para contra restar la vulnerabilidad de sus cibernautas, es que, al entrar a revisar el reglamento y las políticas, estas son muy extensas en testo y por tal motivo nadie las lee.

Crear a nivel de Latinoamérica una autoridad competente que se especialice solo en estudiar como contra restar la Ciberdelincuencia, igualmente recordar a los legisladores la importancia de la problemática que a diario afecta a miles de usuarios de las redes sociales, la tecnología avanza a pasos agigantados y de igual forma debe de avanzar la legislación.

Recomendarle a Estados que están atrasados en combatir esta clase de delitos, como Paraguay, Haití entre otros, de que no se puede dejar abierto la brecha para los delincuentes, es responsabilidad de los Estados mantener las seguridades jurídicas de sus ciudadanos, estos países deberían seguir la ruta de países desarrollados que mantienen contantemente creando estrategias con soluciones efectivas.

Las autoridades competentes en el país han hecho una labor esencial para la lucha de los delitos de estafa a través dela compraventa en la red social Facebook, pero hace falta mucho por hacer, llama la atención el alto índice de victimas diarias, por tal motivo se les recomienda más publicidad y capacitación para los ciudadanos y una campaña para promover la prevención en Colombia.

Por ultimo recomendar a todos los usuarios de la red social Facebook ser más precavidos y estar en contante capacitación a través de la página de la policía nacional, no confiar en nadie y antes de hacer cualquier negociación verificar la información, es hora de cambiar la cultura del colombiano y no dejar que siga creciendo estos hechos delictivos.

8. REFERENCIAS BIBLIOGRÁFICAS

Álvarez, G, & Pérez, P. (2004). Seguridad informática para la empresa y particulares. Madrid: McGraw-Hill.

Baeza, M. 2002. De las metodologías cualitativas en investigación científico social. Diseño y uso de instrumentos en la producción de sentido " Concepción: Editorial de la Universidad de Concepción.

Barbosa, C. (2006). Teoría del Delito. Tipo objetivo, en Lecciones de Derecho Penal. Parte General. Universidad Externado de Colombia. Bogotá, Colombia.

Beltramone, G, Herrera, R, & Zabale, E. (1998). Nociones básicas sobre los delitos informáticos. Disponible en: http://rodolfoherrera.galeon.com/delitos.pdf.

Buitrago, R. (1996). El Delito Informático Revista Derecho Penal y Criminología Vol. 18. No. 59.

Cacales Martinez, A., Real García, J., & Benedicto Marcos, B. (12 de 2011). LAS REDES SOCIALES EN INTERNET. Recuperado el 02 de 07 de 2015, de http://edutec.rediris.es/Revelec2/Revelec38/pdf/Edutece_38_Cascales_Real_Marcos. Pdf.

Cesáreo, A. (2003). Derecho al a intimidad y el correo electrónico: innovación o invasión. Revista Jurídica Universidad de Puerto Rico, No. 72.

Flick U. (2007). Introducción a la investigación cualitativa. Madrid: Morata Paideia; Consultado en: http://www.redalyc.org/pdf/3497/349733228009.pdf.

Granda, G. (03 de 2015). Metodología para el análisis forense de datos e imágenes de acuerdo a las leyes del Ecuador. Recuperado el 01 de 06 de 2015, de http://dspace.ups.edu.ec/bitstream/123456789/8943/1/UPS-CT005203.pdf.

Guerrero, M. (2002). La Ciberdelincuencia: La Ley Patriótica y sus efectos globales en las regulaciones nacionales y en particular en el caso colombiano Revista Derecho privado Vol. 16. No. 29.

González, J. (1996). "Aproximación al tratamiento penal de los ilícitos patrimoniales con medios o procedimientos informáticos". Revista de la Facultad de Derecho de la Universidad Complutense.

Gurvitch, G. (2001). Elementos de Sociología Jurídica, Albolote (Granada), Editorial COMARES, S.L.

Herrera, C. (2010). Hacia una correcta hermenéutica penal: delitos informáticos vs. Delitos electrónicos. Recuperado el 01 de 04 de 2018, de http://dspace.ucuenca.edu.ec/bits-tream/123456789/2673/1/tm4391.pdf.

Jiménez, R. & Rodríguez, J. (1998). El mundo digital y la guardia civil. Revista Iberoamericana de Derecho Informático, No. 27-29.

Kuhn, Thomas S. (1971). *La estructura de las revoluciones científicas*. México, D. F.: Fondo de Cultura Económica. ISBN 9788437500461.

Márquez, C. (2002). El delito informático: La información y la comunicación en la esfera penal Editorial: Bogotá: Editorial Leyer.

Ojeda, J., Rincón, F., Arias, M & Daza, L. (2010). Delitos informáticos y entorno jurídico vigente en Colombia. Cuadernos de Contabilidad, 11 (28), 41-66. Consultado en: http://www.scielo.org.co/scielo.php?script=sci_arttext&pid=S0123. El día 22 de mayo de 2017.

Perrin, S. (2005). Palabras en Juego: Enfoques Multiculturales sobre las Sociedades de la Información. Estados Unidos: C & Editions.

Piaggi, A. (2001). "El Comercio Electrónico y el nuevo escenario de los negocios". En: ALTERINI, Atilio Aníbal, DE LOS MOZOS José Luis y Carlos Alberto SOTO (Directores). Contratación Contemporánea. Contratación electrónica y protección al consumidor". Bogotá: Temis.

Requena Santos, F. (2011). EL CONCEPTO DE RED SOCIAL. Recuperado el 01 de 07 de 2015, de http://www.reis.cis.es/REIS/PDF/REIS_048_08.pdf

Rincón, J. & Naranjo, V. (2011). Delito informático electrónico, de las telecomunicaciones y de los derechos de autor y normas complementarias en Colombia. U.S.C, Universidad Santiago de Cali.

Rodríguez, J. (2011). Análisis de los delitos informáticos presentes en las redes sociales en Colombia para el año 2011 y su regulación. Consultado en: file:///K:/%C2%A0/proyecto%20de%20investigacion/ricardo/Delitos%20en%20las%20Redes%20Sociales.pdf. El día 15 de septiembre de 2017.

Sánchez, Daniel. (1997). La estafa frente al problema de la informática. Revista Parlamentaria, No. 3.

Santander, A., Carbajal, N., Silva, C., & Villanueva, M. (2004). Compraventa Por Internet Y Situación Del Consumidor En El Perú. Facultad de Derecho de la Pontificia Universidad Católica del Perú y miembros de la Asociación Civil Foro Académico.

Sarzana, C. (1979). Criminalitá e tecnología‖ en Computers Crime, Rassagna penitenziaria e criminología, Roma Italia.

Serrano, K. (2016) Los delitos ejecutados mediante la red social Facebook y su relación con el código orgánico integral penal ecuatoriano. Universidad regional autónoma de los andes. Tesis de grado previa la obtención del título de abogada de los tribunales de la república.

Superintendencia Financiera de Colombia (2008). Circular externa 014 de 2008. Información sobre transacciones efectuadas a través de los canales de distribución dispuestos por las entidades vigiladas.

Scott, M. (2001). "El Comercio Electrónico Global y el Derecho: El rol de las regulaciones estatales en el Siglo Veintiuno". En: Derecho de Alta Tecnología nº 139. Año XII.

Taber, J. (1980). Una encuesta de los estudios de delitos informáticos. Estados Unidos: Informática y Derecho Journal.

Téllez, J. (2005). Derecho informático. 3ª ed. México: McGraw Hill. Consultado en: http://www.scielo.org.co/scielo.php?script=sci_arttext&pid=S0123. El día 22 de mayo de 2017.

Vickery, B. (1970). Técnicas de recuperación de información. Londres: Butterworths. Recuperado en: http://www.scielo.org.ar/scielo.php?script=sci_arttext&pid=S1851-17402007000100004.

Vedel, Tierry. (1996). Políticas sobre las autopistas de la información. Revista Internacional de Policía Criminal, No. 457.

Velásquez, F. (2010). Manual De Derecho Penal Parte General. Ediciones Jurídicas Andrés Morales. Bogotá, Colombia.

Wiener, N. (1980). Cibernética y Sociedad. México: Editorial México

Woodcock, J. (2001). Diccionario de informática e Internet de Microsoft. Editorial: McGraw-Hill Interamericana. Barcelona, España.

NORMATIVIDAD:

Colombia, Congreso Nacional de la República (1991). Constitución Política, Bogotá, Leyer.

Colombia, Congreso Nacional de la República. (2009). Ley 1273. Por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado - denominado "de la protección de la información y de los datos"- y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones. Bogotá.

Colombia, Congreso Nacional de la República (2009). Ley 1336. Por medio de la cual se adiciona y robustece la Ley 679 de 2001, de lucha contra la explotación, la pornografía y el turismo sexual con niños, niñas y adolescentes. *Diario Oficial No. 47.417*, 21 de julio de 2009.

Colombia, Congreso Nacional de la República (2001). Ley 679. Por medio de la cual se expide un estatuto para prevenir y contrarrestar la explotación, la pornografía y el turismo sexual con menores, en desarrollo del artículo 44 de la Constitución. *Diario Oficial No. 44.509*

Colombia, Congreso de la República (2000). Ley 599 de 2000, por la cual se expide el Código Penal. *Diario Oficial No. 44.097.*

Colombia, Congreso de la República (1993). Ley 44 de 1993, por la cual se modifica y adiciona la Ley 23 de 1982 y se modifica la Ley 29 de 1944. *Diario Oficial No. 40.740.*

Colombia, Congreso de la Republica. (1999). Ley 527. Ley de Comercio Electrónico. Diario Oficial Colombiano No. 43.673, Bogotá, Colombia. 21 de agosto de 1999. [3] Ley 594 de 2000, Ley de Archivo. Diario Oficial Colombiano No. 44.093, Bogotá, Colombia.

Colombia, Congreso de la Republica. (2006). Ley 1032, Sistemas de Comunicaciones y asuntos de Derechos de Autor, Diario Oficial Colombiano No. 46.307, Bogotá, Colombia.

Colombia, Presidencia de la Republica. (1971). Decreto 410, Código de Comercio. Diario Oficial Colombiano No.33.339, Bogotá, Colombia.

INSTRUMENTOS INTERNACIONALES:

Consejo de Europa. (2001). Convenio sobre los delitos Ciberdelincuencia. Serie de tratados Europeo N°185. Budapest. Hungría.

Organización de las Naciones Unidas ONU. (1969). Convención Americana sobre Derechos Humanos. Editorial Investigaciones Jurídicas

Organización de las Naciones Unidas ONU. (1970). Carta de las Naciones Unidas, Delitos informáticos. EEUU. New York.

Organización de las Naciones Unidas ONU. (1966). Pacto Internacional de Derechos Civiles y Políticos, aprobada por la Asamblea General en su resolución 2200.

ANEXOS

Anexo 1. Matriz Metodológica

INSEGURIDAD JURÍDICA DEL COMPRADOR A TRAVÉS DE LA RED SOCIAL FACEBOOK EN COLOMBIA.						
OBJETIVO GENERAL	**OBJETIVOS ESPECÍFICOS**	**CATEGORÍA**	**DIMENSIÓN**	**FUENTE**	**TÉCNICA E INSTRUMENTO**	**ITEM**
Analizar la inseguridad jurídica del comprador a través de la red social Facebook en el Estado colombiano	1) Identificar las garantías del reglamento y de las políticas establecidas por la red social Facebook respecto a la seguridad jurídica para el comprador a través de este medio	Garantías de seguridad en la red social Facebook	* Análisis del reglamento y políticas de Facebook y sus garantías	Reglamento del usuario del Facebook	Matriz de análisis desde el reglamento y políticas del Facebook	Entrar en el contexto de la realidad que viven los usuarios respecto al reglamento y políticas de la red social Facebook.
	2) Comparar el tratamiento de los delitos **informáticos** en Latinoamérica, en especial el delito de la estafa a través de internet y las redes sociales.	Tratamiento de los delitos informáticos en Latinoamérica	Conocer las cualidades y anomalías de cada una de las legislaciones	Marco normativo de las legislaciones frente a este delito	Matriz de análisis derecho comparado sobre los delitos informáticos en Latinoamérica	Buscar los vacíos jurídicos más relevantes de la legislación en Latinoamérica especialmente la colombiana.
	3) Indagar la efectividad de las autoridades competentes para contra restar el accionar de los estafadores por medio de la red social Facebook en Colombia	Efectividad de la autoridades contra este delito	Estrategias para contrarrestar el delito de estafa de compra venta en Facebook	Funcionarios policía y fiscalía	Entrevista Semi-estructurada	1) Desde la experiencia en su cargo, cuales son las estrategias aplicadas por las autoridades competentes para contra restar la estafa a través de las redes sociales. 2) Desde su conocimiento, cual es el aporte de la normatividad en brindar garantía jurídica a los compradores del Facebook. 3) Para usted, la normatividad existente es suficiente para garantizar seguridad jurídica ante la constate evolución de la tecnología. 4) Cual cree que es la mayor debilidad de las autoridades competentes para contra restar este accionar delictivo. 5) Que recomendaciones deben seguir los usuarios del Facebook que quiere hacer comprar a través del Facebook.

Anexo 2. Formato de Instrumentos aplicados

INSEGURIDAD JURÍDICA DEL COMPRADOR ATRAVES DE LA RED SOCIAL FACEBOOK EN COLOMBIA.

Entrevista Dirigida a: Funcionarios con conocimientos en el área disciplinar y de las autoridades competentes como (Fiscalía y Sijin de la Policía Nacional)

Nombre funcionario: LEONARDO ARDILA QUIJANO
Entidad: SIJIN DE LA POLICIA NACIONAL (METROPOLITANA DE CUCUTA)

Objetivo: Indagar la efectividad de las autoridades competentes para contra restar el accionar de los estafadores por medio de la red social Facebook en Colombia.

Guion de entrevista:

Somos estudiantes de la Universidad Simón Bolívar sede Cúcuta, Como parte de nuestro proyecto de investigación del programa de Derecho, estamos realizando esta entrevista acerca de las **INSEGURIDAD JURÍDICA DEL COMPRADOR ATRAVES DE LA RED SOCIAL FACEBOOK EN COLOMBIA.** La información brindada en esta encuesta es de carácter confidencial y solo con propósitos académicos, solo será utilizada para los propósitos de investigación. Agradecemos de antemano su colaboración.

1) ¿Desde la experiencia en su cargo, cuales son las estrategias aplicadas por las autoridades competentes para contra restar la estafa a través de las redes sociales?
2) ¿Desde su conocimiento, cual es el aporte de la normatividad en brindar garantías jurídicas a los compradores del Facebook.?
3) ¿Para usted como funcionario disciplinar, la normatividad existente es suficiente para garantizar seguridad jurídica ante la constate evolución de la tecnología?
4) ¿Cuál cree usted como funcionario disciplinar, que es la mayor debilidad de las autoridades competentes para contra restar este accionar delictivo?
5) ¿Qué recomendaciones deben seguir los usuarios del Facebook que quiere hacer comprar a través del Facebook?

Anexo 3. Acta de Validación

INSEGURIDAD JURÍDICA DEL COMPRADOR ATRAVES DE LA RED SOCIAL FACEBOOK EN COLOMBIA.

Entrevista Dirigida a: Funcionarios con conocimientos en el área disciplinar y de las autoridades competentes como (Fiscalía y Sijin de la Policía Nacional)

Nombre funcionario: JHON JAIRO CARDENAS

Entidad: FISCALIA GENRAL DE LA NACION REGIONAL NORTE DE SANTANDER

Objetivo: Indagar la efectividad de las autoridades competentes para contra restar el accionar de los estafadores por medio de la red social Facebook en Colombia.

Guion de entrevista:

Somos estudiantes de la Universidad Simón Bolívar sede Cúcuta, Como parte de nuestro proyecto de investigación del programa de Derecho, estamos realizando esta entrevista acerca de las **INSEGURIDAD JURÍDICA DEL COMPRADOR ATRAVES DE LA RED SOCIAL FACEBOOK EN COLOMBIA.** La información brindada en esta encuesta es de carácter confidencial y solo con propósitos académicos, solo será utilizada para los propósitos de investigación. Agradecemos de antemano su colaboración.

1) ¿Desde la experiencia en su cargo, cuales son las estrategias aplicadas por las autoridades competentes para contra restar la estafa a través de las redes sociales?
2) ¿Desde su conocimiento, cual es el aporte de la normatividad en brindar garantías jurídicas a los compradores del Facebook.?
3) ¿Para usted como funcionario disciplinar, la normatividad existente es suficiente para garantizar seguridad jurídica ante la constate evolución de la tecnología?
4) ¿Cuál cree usted como funcionario disciplinar, que es la mayor debilidad de las autoridades competentes para contra restar este accionar delictivo?
5) ¿Qué recomendaciones deben seguir los usuarios del Facebook que quiere hacer comprar a través del Facebook?