Ciencia Latina Revista Científica Multidisciplinar, Ciudad de México, México.
ISSN 2707-2207 / ISSN 2707-2215 (en línea), julio-agosto 2025,
Volumen 9, Número 4.

https://doi.org/10.37811/cl_rcm.v9i2

LA APROPIACIÓN FRAUDULENTA POR MEDIOS ELECTRÓNICOS Y EL BIEN JURÍDICO PROTEGIDO

FRAUDULENT APPROPRIATION BY ELECTRONIC MEANS AND THE PROTECTED LEGAL ASSET

Ab. Andrea Marlene Altamirano Zavala
Pontificia Universidad Católica del Ecuador

DOI: https://doi.org/10.37811/cl_rcm.v9i3.19080

La Apropiación Fraudulenta por Medios Electrónicos y el Bien Jurídico Protegido

Ab. Andrea Marlene Altamirano Zavala[1]
aaltamirano@pucesa.edu.ec
https://orcid.org/0009-0004-1535-1396
Pontificia Universidad Católica del Ecuador Sede Ambato
Ambato-Ecuador

RESUMEN

La apropiación fraudulenta por medios electrónicos en Ecuador constituye una modalidad delictiva en crecimiento, vinculada directamente con el uso indebido de tecnologías digitales para obtener beneficios económicos ilegítimos. Este tipo de fraude se manifiesta a través de la manipulación de sistemas informáticos, suplantación de identidad digital, transferencias bancarias no autorizadas y estafas en plataformas virtuales. El Código Orgánico Integral Penal (COIP) ecuatoriano tipifica este delito de la apropiación fraudulenta por medios electrónicos, incorporando sanciones específicas para quienes usen medios electrónicos o tecnológicos con el fin de apropiarse ilícitamente de dinero o bienes ajenos. A pesar de esta normativa, la evolución constante de las técnicas cibernéticas supera en muchos casos la capacidad de respuesta institucional. Uno de los principales problemas que enfrenta el país frente a este delito es la limitada especialización de operadores judiciales y cuerpos investigativos en materia de cibercriminalidad. Además, existen vacíos en la cooperación interinstitucional, que pueden generar fallas en el debido proceso, identificación de los responsables y el rastreo de los fondos, problemas como la jurisdicción y competencia, a esto se suma la complejidad probatoria en entornos virtuales, todo esto es abordado analíticamente en el presente artículo mostrando la fragilidad de la protección de datos que en este caso es el bien jurídico protegido.

***Palabras clave*:** cibercrimen, bien jurídico, medios electrónicos, apropiación fraudulenta

[1] Autor principal
Correspondencia: aaltamirano@pucesa.edu.ec

Fraudulent Appropriation by Electronic Means and the Protected Legal Asset

ABSTRACT

Fraudulent appropriation through electronic means in Ecuador constitutes a growing criminal modality, directly linked to the misuse of digital technologies to obtain illicit economic benefits. This type of fraud is manifested through the manipulation of computer systems, digital identity theft, unauthorized bank transfers, and scams on virtual platforms. The Ecuadorian Comprehensive Organic Criminal Code (COIP) classifies this offense of fraudulent appropriation through electronic means, incorporating specific sanctions for those who use electronic or technological means to unlawfully appropriate money or other people's property. Despite this regulation, the constant evolution of cyber techniques often surpasses the institutional response capacity. One of the main problems the country faces in addressing this crime is the limited specialization of judicial operators and investigative bodies in the field of cybercrime. In addition, there are gaps in inter-institutional cooperation, which can result in due process failures, difficulties in identifying those responsible, and in tracing the funds. Issues such as jurisdiction and competence further complicate the situation. Added to this is the complexity of gathering evidence in virtual environments. All these aspects are analytically addressed in this article, highlighting the fragility of data protection, which in this case is the protected legal interest.

***Keywords*:** cybercrime, legal interest, electronic means, fraudulent appropriation

Artículo recibido 05 julio 2025
Aceptado para publicación: 25 julio 2025

INTRODUCCIÓN

Dentro del ámbito informático tenemos nuevos retos en lo referente al derecho, puesto que las diferentes facetas que presenta son un reto para mejorar su desenvolvimiento, puesto que el avance tecnológico es constante así como las condiciones de vida, y que el derecho debe evolucionar de la misma manera.

En el presente trabajo pretende abordar el tema del bien jurídico protegido, y la apropiación fraudulenta de bienes electrónicos, revisando conceptos, antecedentes y elementos de esta figura jurídica, realizando un análisis en sus diferentes facetas y la problemática que gira a su alrededor, como los problemas de identidad de autoría, dudas sobre la jurisdicción y competencia entre otros elementos que presentan novedades en su concepción.

Actualmente encontramos una interacción virtual mucho más fuerte, y que ello conlleva el uso de herramientas informáticas para la realización de transacciones económicas, lo cual es una oportunidad para el cometimiento de defraudaciones de forma anónima, haciendo más difícil su imputación y su investigación, además de las formas de cometimiento de estafa que involucran un ámbito internacional.

Se comenta la importancia de tratar su estudio de una manera urgente y necesaria en una sociedad donde cada vez más dependemos de la tecnología y del conocimiento de sistemas virtuales e informáticos en todos los ámbitos. El ámbito informático desborda nuestra vida diaria, contemplando entonces la necesidad del progreso del derecho en estos aspectos, por lo cual finalmente se mostraran medidas preventivas y planteamiento de soluciones para evitar el cometimiento de estafas en medio digital.

METODOLOGÍA

La investigación será de tipo **cualitativo y documental**, con un análisis dogmático del derecho penal y una revisión de casos relevantes sobre apropiación fraudulenta en entornos electrónicos. Se combinará el estudio normativo con el análisis jurisprudencial y doctrinal.

El estudio se basará en:

- Revisión bibliográfica: Análisis de libros, artículos científicos, informes jurídicos y normativas nacionales e internacionales.
- Estudio de casos: Revisión de sentencias y resoluciones judiciales que evidencien cómo se interpreta y protege el bien jurídico afectado.

- Análisis comparado: Se compararán diferentes legislaciones para identificar tendencias y vacíos normativos.

La Cibercriminalidad

El internet como medio digital de expansión global ha facilitado la comisión de delitos, así como también los medios de persecución o enjuiciamiento. Se entiende por cibercrimen a las conductas de apropiación, disposición de información o información ilícita sin autorización con afectación a un bien jurídico. (Hernández, 2009) Es decir, vulnerando la seguridad informática y de redes de transmisión de datos, causando perjuicios personales y patrimoniales. Se observa también el desconocimiento general del manejo de internet y de nuevas tecnologías por parte de la ciudadanía, provocando que sea una fuente atractiva para la ciberdelincuencia, al existir facilidades para el cometimiento de tipos delictivos. Otra característica es el cometimiento instantáneo de varios delitos a la vez, ya que no existe mucho tiempo entre el inicio del ilícito y la consumación del acto. Es decir la rapidez aunque aparentemente sea una característica no tan importante, nos permite rescatar la mínima o nula capacidad de reacción por parte de la víctima frente al escaso riesgo del tiempo empleado en su cometimiento, lo que aventaja al autor del hecho.

También dentro de las características encontramos que puede existir el desconocimiento de la identidad de la víctima y del autor; respecto de la víctima se puede desconocer a quien va dirigido el ataque y por otro lado desconocimiento del autor incurriendo en el anonimato. (Rodríguez, 2019) Existen técnicas de encriptación de datos o empleo de sistemas que dificultan el rastreo del objeto por el cual se realiza el delito, y dificultan además su vinculación con el autor del delito.

Los datos informáticos y las bases de datos, son actualmente relevantes, por la necesidad de obtener información sea en medios mercantiles u otros contextos, por lo que se menciona la urgencia de proteger la información a fin de precautelar el capital económico y los datos personales. Por tanto el ciberdelito se comete a través de medios telemáticos como herramienta del delito, o porque la vulneración de sistemas sea su objetivo. Los sistemas informáticos se protegen de manera indirecta, mientras que los delitos vinculados al internet, salvaguardan en primer orden otros bienes jurídicos como la privacidad de datos o el patrimonio monetario, antes que la seguridad de la información. (Posada, 2017)

La doctrina nos indica que dentro de los cibercrímenes se castiga la acción que vulnera la seguridad de las funciones informáticas, pudiendo existir también la vulneración de otros bienes jurídicos colateralmente.

La seguridad de las funciones informáticas configura primero la confidencialidad de los datos, en segundo lugar la integridad y exactitud de la información, así como que exista la adecuada infraestructura de acceso que garantice su correcto funcionamiento, así como también exista la comprobación del envío o repudio de la información. (Posada, 2017) Es decir, el autor plantea que la seguridad de la información es en sí, un bien jurídico que necesita protegerse, ya que es exigible para el usuario un normal funcionamiento de los sistemas informáticos, y se garantice la protección a bases de datos en medios virtuales.

El registro y análisis de la información obtenida de dispositivos informáticos tiene algunas características de protección legal por la protección de la inviolabilidad del domicilio, la garantía del secreto de las comunicaciones, o material acerca de datos personales o íntimos, deben primero ser garantizados, para que no existan impugnaciones por la manera de obtenerlas. El acceso al contenido de un computador requiere de una autorización judicial específica que no debe confundirse con la orden para ingresar al domicilio, debido a que el juez no es un técnico en la materia, y debe ser apoyado por personal técnico como lo son peritos, que aseguren que esta copia de seguridad se ha obtenido con las garantías de integridad. (Perea, 2017) La doctrina como vemos ha debatido este punto ya que se tratan de datos privados, en todo caso siempre se debe tener las autorizaciones para obtener dichas pruebas. La sentencia STC 170/2003, de 29 de septiembre, declaró la vulneración del derecho por falta de las garantías procesales, por no identificarse determinado el domicilio del que fue recolectada la pieza informática. Varios autores señalan que el delito informático, supone una pluralidad de modalidades delictivas vinculadas con los computadores, existiendo varias conductas delictivas y no una sola. (Acurio, 2016)

La autora María Castillo entiende que delito informático es la acción envuelta en dolo, ocasionando un perjuicio a entidades con la intervención de dispositivos informáticos. Estos dispositivos funcionan como unidades de almacenamiento, son elementos que leen o escriben información en soportes de almacenamiento o memoria de un computador. (Castillo, 1989)

Por otro lado, las herramientas de explotación de los dispositivos informáticos cómo pueden ser computadores, teléfonos móviles, deben ser evacuadas en un corto plazo de tiempo a fin de conservar la información deseada, en la práctica este tipo de cosas no siempre son factibles.

Para la delincuencia la ciber acción puede ser programable y automatizada, esto quiere decir que para el cometimiento del delito un sujeto aborda el sistema informático, y produce una acción programada con alcance determinado de espacio y tiempo, así se ejemplifica con la ejecución automática, sincronizada y reiterativa de ataques cibernéticos situados en diferentes países, cuyo sistema ha sido diseñado especialmente para enviar programas dañinos a cualquier parte del mundo. Estos ataques consisten en vulnerar sistemas o equipos, o ejecutar un ataque concreto mediante la utilización del sistema contra datos registrados. La posibilidad de programar permite que se ejecute el hecho delictivo aun cuando las personas no están conscientes de ello, o sin la posibilidad de tener una injerencia física. (Posada, 2017)

El Bien Jurídico Protegido

El bien jurídico protegido en general es la información, que es un derecho fundamental recogido en las constituciones de los países. Los bienes jurídicos de fondo en el ámbito económico, dependiendo del delito serían el patrimonio, respecto de fraudes informáticos y malversación de datos, la confidencialidad de los datos, respecto de bancos de datos y de datos de intimidad personal, en general nos referimos a la seguridad en medios informáticos. (Acurio, 2016)

Para José Luis Ripollés existen principios estructurales garantistas de la intervención penal, primero el principio de lesividad, es decir que debe tratarse de un comportamiento que tenga una afectación social en su conjunto, podemos hacer distinción del derecho penal con el derecho moral. Respecto del principio de mínima intervención basado en la fragmentariedad, subsidiariedad y proporcionalidad, además de la neutralización de la víctima refiriéndose a las medidas de reparación a la víctima por el delincuente. (Ripollés, 2017)

Para determinar cuál es el bien jurídico vulnerado debemos observar que es lo que se debe proteger, al hablar del bien jurídico, hacemos mención de ciertos valores que deben protegerse como el derecho a la vida, la integridad, el patrimonio económico.

Biding señala que el bien jurídico lo estipula el legislador puesto que éste valora que es importante como necesidad social. (Martínez, 2017) Entenderemos al bien jurídico como aquella pieza vulnerable que el estado protege de ser lesionado, para lo cual el mismo debe ser garantista frente a la oportuna actitud dañosa que pueda presentarse, y es por esto todo el engranaje jurídico penal, sancionatorio para proteger estos bienes. El bien jurídico parte además del modelo democrático y político que tiene un país, puesto que su escala de valores está plasmada en su sistema jurídico. Varios autores señalan que estos bienes pueden ser individuales y colectivos, donde pongan en riesgo el orden social preestablecido, en donde el estado tiene que mover su aparataje institucional para intervenir salvaguardando la Constitución y el orden económico social. (Martínez, 2017)

Los ciberdelitos pueden abarcar conductas que pueden vulnerar varios bienes jurídicos como la intimidad, el patrimonio económico, el honor, etc., a través de sistemas informáticos. El Derecho penal, es una herramienta de control social ya que precautela el orden, y en tal virtud se señala que el delito de estafa informática busca la estabilidad de las relaciones económicas y sociales mediante el uso de herramientas virtuales.

La estafa según el art. 248.2 del Código Penal Español

Dentro de la legislación española tenemos la estafa informática, el objeto del engaño es producir en la víctima su consentimiento para que se realice el acto de disposición patrimonial, haciendo comparación con el delito de hurto donde no se verifica entrega voluntaria, así como en la apropiación indebida no hay engaño. La sentencia del Tribunal Superior segunda sala de lo Penal de la Jurisdicción española, habla de que el engaño debe ser idóneo. «Es preciso que exista una relación de causalidad entre el engaño que provoca el error y el acto de disposición que da lugar al perjuicio, de donde se obtiene que aquél ha de ser precedente o, al menos, concurrente, al momento en que tal acto tiene lugar. El engaño debe ser la causa del error; el error debe dar lugar al acto de disposición y éste ha de ser la causa del perjuicio patrimonial». (STS 358/2015, de 10 de junio) Este acto voluntario que realiza la víctima lógicamente carece de conciencia, puesto que solamente se requiere que exista un acto voluntario.

No existe un consentimiento voluntario, principio básico para la legalidad de la celebración de actos y contratos, de acuerdo a la normativa civil, puesto que el consentimiento se ve viciado por el error, y este producido por el engaño.

En el numeral 2 del art. 248 del código penal español menciona que se consideran reos de estafa «b) Los que fabricaren, introdujeren, poseyeren o facilitaren programas informáticos específicamente destinados a la comisión de las estafas previstas en este artículo.» (art.248.2 LECrim) Destacando que la sola posesión de este tipo de programas es penalizado, ya que el tenerlas confirma la culpabilidad, entonces podemos entender que si una persona lo tiene, cuál es su pretensión, se convierte en un elemento que apoya la materialidad del acto delictivo.

La utilización de tarjetas de crédito en cajeros automáticos sin consentimiento, pueden ser de tres tipos, primero el uso no consentido de la tarjeta por una tercera persona, segundo uso abusivo de la tarjeta por parte de su titular, tercero utilización de tarjeta alterada o falsa. Este último es común puesto que hoy en día se conoce la reproducción de tarjetas de crédito o débito, sin embargo en estos casos la acción directa es con el cajero más no con la víctima. (Devia, 2017) La jurisprudencia nos habla de que debe existir la evidencia de la manipulación del mecanismo informático o artificio semejante, es decir, que la trasferencia que se presume la estafa haya sido realizada por medios informáticos.

Cabe señalar que esta tipología está en su auge por el comercio electrónico, en donde el usuario como el empresario se pueden ver afectados. El fraude dentro de esta modalidad se da por la ausencia de pago, o por la suplantación de personalidad de quien realmente realiza la adquisición, cargando el pago a una tercera persona que desconoce de dicha transacción. (Fernández, 2007) La captación de datos de tarjeta puede darse inclusive mediante vía telefónica, o correo electrónico, para posteriormente cometer el fraude. El Banco de España en reiteradas ocasiones ha indicado que los mismos bancos deben cubrir los fraudes cuando el usuario es víctima de uso indebido de tarjeta, siempre que éste haya denunciado rápidamente el robo o pérdida. El banco puede alegar negligencia del cliente, para relevar su responsabilidad

En Ecuador existe la figura de Apropiación fraudulenta por medios electrónicos, tipificada en el Artículo 190 del COIP, aborda la problemática de los delitos informáticos, estableciendo sanciones claras para quienes, mediante el uso fraudulento de tecnologías, afecten el patrimonio de terceros. Su correcta aplicación es esencial para garantizar la seguridad en el entorno digital y la protección de los bienes jurídicos involucrados.

Esto representa un esfuerzo por sancionar delitos informáticos, pero enfrenta retos en su aplicación debido a la evolución de las tecnologías, problemas de jurisdicción, dificultades probatorias y falta de especialización judicial.

El delito de apropiación fraudulenta por medios electrónicos plantea varios problemas en su aplicación e interpretación. Algunos de los principales desafíos son creación de perfiles falsos y suplantaciones de identidad para desviar la responsabilidad, la recolección de pruebas digitales es compleja, ya que los datos pueden ser eliminados o encriptados**.** Se requiere peritaje informático especializado para demostrar la manipulación de sistemas. Problemas en la cadena de custodia de la evidencia digital. Puede existir confusión al establecer e tipo penal a aplicarse, entre estafas electrónicas, fraudes informáticos y apropiación fraudulenta, lo que genera problemas al tipificar los casos.

Problemáticas alrededor de La Apropiación fraudulenta por medios electrónicos en Ecuador.

Identificación del autor

El anonimato en este tipo de delitos es un problema puesto que existe el riesgo de evadir responsabilidad por cuanto el delincuente no necesariamente utiliza su propio sistema informático, sino que también existen programas en dónde se oculta la dirección verdadera de la persona que emite el mensaje ya sea por correo electrónico o por algún otro IP. (Temperini, 2017) Por esta situación se convierte más aún complicada la investigación ya que al ser delitos perpetrados por internet, es necesario mantener herramientas de investigación adecuadas sobre tecnología, que contribuyan en el esclarecimiento de estos delitos.

Por otro lado tenemos lo que llamamos el internet profundo (*Deep web*), puesto que mucha de la información de este tipo de internet no está debidamente sustentada adecuadamente, es decir, sus contenidos no están señalados por los motores de búsqueda tradicionales, por eso se la conoce también como internet superficial, tiene ciertas restricciones de acceso. Esto nos lleva a pensar que es un medio más adecuado para registrar acciones o movimientos camuflados propiciando el ocultamiento de datos, entonces es menester que la ciencia vaya también a la par de estas situaciones para poder garantizar a la sociedad la privacidad y la tranquilidad respecto de la privacidad de la información y de sus movimientos económicos. (Temperini, 2017)

Jurisdicción y competencia

Podemos determinar que existen problemas para la persecución del enjuiciamiento respecto de delitos de defraudación económica perpetrados por internet, en donde la dimensión del tiempo y el espacio cambian, haciendo que las fronteras físicas entre países no existan, puede cometerse un acto delictivo en un sitio y las consecuencias de este hecho ser generadas en otro.

Los delitos cometidos a través del uso del internet como fraudes en las transacciones comerciales electrónicas, estafas, defraudaciones electrónicas, plantean los mismos problemas de otras conductas delictivas respecto de la jurisdicción y competencia. Por ejemplo, puede existir coincidencia de la ejecución de la acción u omisión con el lugar del resultado, ahí nos encontramos en la disyuntiva de dónde se genera la competencia, si se prefiere el lugar donde se dieron los resultados o el lugar dónde fueron ejecutados. Los principios penales se ven trastocados por esta circunstancia, y evidencia la fragilidad de los mismos. (Cárdenas, 2008)

La Sentencia del Tribunal de Justicia de la Comunidad Europea de 7 de marzo de 1995, «caso Shevill», es un referente en estos conflictos, consideró que en un supuesto de difamación se podía ejercitar la acción de reparación, en países donde hubo perjuicios, en base a este caso el estado Francés aprobó a sus jueces nacionales como jueces sin fronteras, esto en función del principio universal del derecho internacional. (Ventas, 2017) La jurisdicción viene determinada por el lugar en donde se cometió la infracción en el ámbito penal, en el caso de delitos económicos cometidos dentro del territorio español, cuando estas instituciones lo cometen y no están radicadas en el territorio, si bien la dirección de las empresas nos ayuda a determinar la ubicación de la mismas, no siempre coincidirá con el lugar del cometimiento de la infracción.

La Teoría del resultado nos indica que donde se produzca el resultado final de un delito es el lugar que genera la competencia, es decir, identificar el lugar donde se producen los resultados delictivos, toda esta teoría se basa en que el derecho penal busca cuidar de los bienes jurídicos. (Ventas, 2017) *La Teoría de la ubicuidad nos* señala que para que un Estado ejerza jurisdicción sobre un delito, bastaría con que se haya producido la conducta o el resultado en el mismo estado. Es decir, observamos dos tipos de competencia según esta teoría, se habla de que se respeta la soberanía territorial, el alcance de esta competencia dependerá de lo que se entienda por lugar de la conducta, o lugar del resultado, pero

en la práctica vemos problemas respecto de la ubicación del servidor electrónico con resultados que se generan en otros territorios. (Alonso, y Esparza 2017)

Esta situación trae problemas de competencia puesto que la víctima desconoce el lugar de donde proviene el delito, además de que el autor puede cometer el acto ilícito desde un computador no fijo, y que se puede redireccionar a través de servicios de Internet, a otros sitios incluso países diversos. El Tribunal Supremo de España ha realizado pronunciamientos respaldando el principio de ubicuidad. El acto delictivo que se comete desde el territorio nacional, o incluso si este se comete desde afuera pero con consecuencias en el territorio, es decir, es suficiente con que se relacione uno de estos elementos para poder determinar la competencia dentro de la jurisdicción española. (Alonso *et al*. 2017)

El carácter transnacional de este tipo delitos es notorio, la cantidad de negocios y nuevas formas financieras a nivel nacional e internacional han requerido la implementación de sistemas informáticos para la consolidación de negocios, lo cual propicia el aumento de fraudes por estos medios. Existen varias organizaciones internacionales como la (OCDE), organización de cooperación y desarrollo económico, que reguló varios problemas que se sucitan en el campo informático, así como también la (ONU), organización de naciones unidas, ha elaborado un manual de prevencion y control de la criminalidad realizada por medio de computadores. (Suárez, 2006)

Problemas que plantean las diligencias de investigación tecnológica sobre las garantías procesales

Hacemos referencia también a la teoría del fruto del árbol envenenado dónde nos manifiesta que la prueba derivada de un hecho ilícito se ve contaminada, y carece de valoración probatoria. También es menester hacer una valoración respecto de pruebas obtenidas de forma directa o de forma indirecta. La Corte Suprema de Estados Unidos ha señalado que una prueba ilícita, conlleva también la falsedad o ilicitud de la información y elementos de la misma. Encontramos teorías como la del descubrimiento Inevitable, en donde encontramos una prueba de un hecho ilícito pero que era un hecho inevitable su descubrimiento, o que sea conocida. También tenemos la teoría de la proporcionalidad concediendo cierta flexibilidad de la valoración de la prueba ilícita, frente al excesivo poder del estado. (De la Rosa y Guerrero 2014)

Dentro de un estado de derecho lo que se pretende es perseguir la verdad y que ésta verdad coincida con la verdad procesal, siempre con respeto a las garantías fundamentales de la persona. El hecho de valorar una prueba con fuente lícita, muestra legitimidad en la decisión del juzgador, el cual deberá buscar un fundamento que sea el soporte para su decisión, que no sea objetable, que sea clara y que sea capaz de sustentar un razonamiento jurídico. La prueba finalmente es todo aquello que acredite una aseveración garantizada constitucionalmente, permitiendo que ésta prueba sea impugnada y objetada en la audiencia de juicio. (De la Rosa *et al*.2014)

Gimeno Sendra hace distinción entre la prueba ilícita y la prueba prohibida, el mismo que menciona que la prueba ilícita es la obtenida infringiendo algún procedimiento manifestado en la ley de manera general, aquella obtenida de manera dolosa y empleando algún mecanismo fraudulento, la prueba prohibida es la que surge a partir de la violación de los derechos fundamentales. No se admitirá prueba de todo aquello mediante mecanismos considerados como reprobables contra la dignidad y moral de la persona. La prueba que se haya obtenido a través de la investigación policial o provenga de juzgado, vulnerando derechos fundamentales de la persona investigada, la misma deberá considerarse como no existente, puesto que no se puede admitir una prueba obtenida sin los respectivos permisos o notificaciones realizadas a las personas que deben emitir su autorización. La posición del Tribunal Constitucional de España en sentencia STC 114/1984, de 29 de noviembre, en donde respecto a la prueba ilícita señala que se proclama la inadmisibilidad procesal de las pruebas obtenidas mediante la violación de derechos fundamentales, y la prueba prohibida es la que surge de la ilicitud por ser su origen viciado. (Giner, 2008)

Como señala Carnelutti el verdadero objetivo del proceso es la búsqueda de la verdad, por lo tanto, la validez de la prueba debe ser producida y fundada bajo los derechos fundamentales del ordenamiento constitucional. También podemos observar una prueba ilícita emanada de una nulidad de pleno derecho, es decir, la obtenida contraviniendo disposición legal expresa. La prueba ilícita es aquella que proviene de una ilegalidad insubsanable para su validez. En materia probatoria observamos la proyección del garantismo del derecho, notablemente en la obtención de la prueba ilícita y prohibida. Para Couture el proceso penal protege al individuo del juzgador, expresa ese garantismo del individuo susceptible y vulnerable frente al estado representado por el poder público (González, 2005).

Debe prevalecer el principio de razonabilidad y de proporcionalidad de los actos de poder que determina cualquier prohibición de una decisión arbitraria, este derecho al debido proceso se consagra como un derecho fundamental, para resguardar las garantías en todo proceso penal y resguardar la tutela judicial. Se garantiza el acceso a la justicia entendida como la posibilidad de acceso a los órganos jurisdiccionales para las partes procesales y reconocer un interés legítimo.

La tutela judicial constituyen todas las herramientas e instrumentos que el estado otorga para poder hacer efectivos los derechos del ciudadano. Según sentencia TS 282/2019 de 23 Mayo del 2019, señala: Reconocer que todas las personas tienen derecho a obtener la tutela judicial efectiva de los jueces y tribunales en el ejercicio de sus derechos e intereses legítimos, es decir proteger derechos fundamentales de todas las personas según el Art. 24 CE, siendo el derecho de todas las personas, y así obtener la tutela, es decir, la protección de los órganos jurisdiccionales, esa protección es respecto de cualquier derecho e intereses legítimos, reconocidos por el ordenamiento, y todo ello sin que en ningún caso pueda producirse indefensión. Cabe recordar que la tutela judicial efectiva nace en protección del propio individuo, recalcando que los ciudadanos no ejercen una auto tutela. (Alonso *et al*. 2017)

CONCLUSIONES

La globalización ha hecho que el derecho penal tome otras aristas dentro de la legislación, ya que la dinámica económica, nos lleva a otras dimensiones mediáticas, es un proceso económico, tecnológico, político, social y cultural a escala mundial que consiste en la creciente comunicación e interdependencia entre los distintos países del mundo uniendo sus mercados, a través, de una serie de transformaciones sociales, políticas y económicas, en donde el uso del internet es clave en esta transformación. Mientras tanto hoy en día los gobiernos van perdiendo atribuciones en algunos ámbitos que son tomados por la sociedad civil, en un fenómeno que se ha denominado sociedad red, el activismo cada vez más gira en torno a las redes sociales y medios telemáticos, que si bien tienen sus aspectos positivos, también son utilizadas para beneficios personales, pueden tener fines delictivos, estafas o infracciones a través de estos medios, entonces es necesario que el derecho penal, se actualice con la evolución de la sociedad en estos aspectos, y camine a la par de lo que la sociedad requiere que se penalice.

El sistema actual en donde nos desenvolvemos con el uso de sistemas informáticos y herramientas digitales, como cuentas de banco, el uso de tarjetas de crédito y el acceso a otro tipo de sistemas

informáticos que únicamente se respaldan con claves, sin tener garantías de seguridad en las transacciones económicas, y que por el contrario hemos registrado su vulnerabilidad, por cuanto las herramientas de investigación no son tan efectivas, observamos que no todos los delitos son factibles de ser llevados a juicio por parte de la fiscalía general, ya que ésta debe tener elementos para poder hacerlo, la investigación desarrollada por ésta a pesar de tener a su disposición la policía judicial no son suficientes, por el avance tecnológico, dejando también en claro que al incorporar esta prueba en la audiencia oral debe cumplir con todas las garantías para hacerse efectiva y por ende ser tomada en cuenta por el juez en su valoración probatoria.

Por otro lado, las garantías constitucionales que deben cumplirse al recabar la prueba deben proteger los derechos fundamentales de las partes, por lo cual se hace más difícil y complicada la investigación, ya que debido a ello, esas pruebas pueden no ser efectivas en la audiencia de juicio o en su valoración, debido a que se deben precautelar los principios generales del derecho, en lo que es la valoración de la prueba, y que la misma sea útil en la motivación del juzgador.

Otro aspecto es la vulnerabilidad de nuestros sistemas informáticos ya que no existen las restricciones y las seguridades necesarias para poder mantener datos, inclusive protegidos dentro de los sistemas de computación, muchos de ellos son *hackeables*, es decir, que pueden ser susceptibles a que se extraiga información a través de virus informáticos, correos no deseados que dañan el computador y logran su acometido. El delincuente informático en el medio virtual puede estudiar nuestras preferencias, captando con esto datos para poder cometer un fraude, como por ejemplo enviar una propaganda acerca de alguna inversión o aprovechar cualquier interés para compras y obtener sus datos.

El derecho a la intimidad y privacidad en las comunicaciones se ve afectado, pero tampoco significa que esté permitido realizar cualquier acción por internet, y peor desde el anonimato. El uso de herramientas tecnológicas sofisticadas ha dado pie para la creación de este tipo de estafas por la accesibilidad internacional, rompiendo fronteras, a la vez que al observar la eficacia de las herramientas tecnológicas el delincuente las va mejorando precisamente por los resultados que obtiene.

El ámbito en donde se realizan este tipo de delitos no tiene fronteras, por lo cual también nos lleva a pensar que la persecución de los mismos es complicada, ya que la víctima y al acusador pueden encontrarse en países distintos, y no siempre existen convenios de extradición entre los países, ni una

legislación que ampare un ordenamiento jurídico homogéneo y para la aplicación del derecho se recurre al análisis análogo, en relación al derecho comparado aplicado en otros países para solucionar vacíos.

La vulnerabilidad de los sistemas tiene relevancia puesto que al existir movimientos económicos en internet, no se requiere tanto de conocimiento especializado, puesto que sólo se necesita un computador, y por lo mencionado en el presente trabajo existen programas que se difunden en la *deep web* o internet profundo, de fácil acceso, y no existe legislación para normar este tipo de contenidos en la web. Cabe recalcar que también a medida que el derecho penal debe evolucionar, a medida que se descubren nuevas formas delictivas, tomando en cuenta la doctrina y el avance jurisprudencial, hay quienes cuestionan la intromisión del estado respecto de la regulación de medios virtuales, puesto que se puede considerar que existe menos libertad, pero que de igual forma debe existir control dentro de este ámbito.

Las personas que ejecutan manipulaciones informáticas pueden ser personas que trabajan en una misma empresa, cuestión que hace más factible el delito y dificulta su detección, también favorece el que no existan denuncias al respecto.

La ejecución del acto delictivo tiene la ventaja de poder ser ejecutarlo a distancia, en tiempo real, y sin dejar rastros por los cambios de IP que mencionamos en el texto, no siempre dando alerta a la víctima, que al no darse cuenta, no pueda realizar alguna acción para contrarrestarlo. Se analiza también la dificultad que existe para la investigación de los actos perpetrados por internet, las herramientas que se disponen para probar dichos actos, se sabe de la falta del personal especializado para perseguir estos delitos, y el constante avance tecnológico que encuentra nuevas formas cada vez más sofisticadas.

La actividad económica sale de las fronteras nacionales, debido a que las transacciones las realizan con empresas ubicadas en otros países en donde se rigen otras legislaciones, por lo cual también es una dificultad para su correcta persecución, trayéndonos conflictos de jurisdicción. Existen conjeturas acerca de que el internet debería convertirse en un tipo de jurisdicción, pero que no es aplicable ya que cada país tiene su propio sistema punitivo y sancionatorio. También en cuanto a las pruebas podemos observar que a través de los medios telemáticos estas pruebas pueden llegar a eliminarse o cambiarse, puesto que existe información encriptada, y que por el derecho a la intimidad y a la privacidad de la información, ésta no puede ser descifrada, lo que obstaculiza su investigación.

Dentro de las posibles soluciones para perseguir y castigar de forma más efectiva este tipo de delitos, están en primer lugar que se dispongan de los recursos, medios y herramientas necesarias para la investigación de delitos informáticos, para que exista una adecuada gestión de datos y archivos informáticos, correctamente almacenados y conservados, con la finalidad que sean útiles procesalmente. Otro punto es mejorar la cooperación entre estados para que ésta área se desarrolle a nivel jurídico y técnico, es decir, que exista cooperación internacional judicial y policial, a fin de conllevar las diferencias con las legislaciones de otros estados, y mejorar la persecución de la cibercriminalidad.

Por otro lado, es necesaria la adopción de medidas preventivas, como un medio efectivo para contrarrestar la delincuencia cibernética y evitar las estafas en medios virtuales, concientizar a la ciudadanía en el ámbito de prevención en el uso de sistemas informáticos.

REFERENCIAS BIBLIOGRAFICAS

Acurio del P, S. (2016). *Delitos Informáticos: Generalidades*. Revista PUCE. Recuperado en marzo de 2021 de https://www.oas.org/juridico/spanish/cyb_ecu_delitos_inform.pdf

Alonso, L. A., & Esparza, L. I. (2017). Los retos procesales de la criminalidad informática desde una perspectiva española. *Revista Novum Jus*, 11(1), 39-72. https://doi.org/10.14718/NovumJus.2017.11.1.2

Castillo, M. C. (1989). *El delito Informático*. Congreso sobre Derecho Informático, 22-24.

Cárdenas, C. (2008). El lugar de comisión de los denominados ciberdelitos. *Política Criminal Revista Electrónica Semestral de Políticas Públicas en Materias Penales*, (6), A2-6, 1-14. Recuperado en junio de 2020 de http://repositorio.uchile.cl/handle/2250/126580

Devia, E. A. (2017). *Delito informático: Estafa informática del artículo 248.2 del código penal* (Tesis doctoral). Universidad de Sevilla, Facultad de Derecho.

De la Rosa, P., & Guerrero, V. (2014). La prueba ilícita en el sistema acusatorio, una mirada a las regulaciones española, alemana y americana en torno a su prohibición y excepciones. *Revista Académica de Investigación Tlatemoani*, (16), 181-210. Recuperado en marzo de 2021 de file:///C:/Users/Pc/Downloads/Dialnet-LaPruebaIlicitaEnElSistemaAcusatorio-7345930.pdf

Fernández, J. G. (2007). Respuesta penal frente a fraudes cometidos en internet: estafa, estafa informática y los nudos de la red. *Revista de derecho penal y criminología*, (19), 2da Época,

217-243. Recuperado en marzo de 2021 de http://revistas.uned.es/index.php/RDPC/article/view/24951

Giner, C. A. (2008). Prueba prohibida y prueba ilícita. *Anales de Derecho*, (26), 579-590. Recuperado en marzo de 2021 de https://revistas.um.es/analesderecho/article/view/113751

González, J. M. (2005). El proceso penal español y la prueba ilícita. *Revista de derecho Valdivia*, 18(2), 187-211. Recuperado en marzo de 2021 de http://dx.doi.org/10.4067/S0718-09502005000200009

Hernández, L. D. (2009). El delito informático. *Cuaderno del Instituto Vasco de Criminología EGUZKILORE*, (23), 227-243. Recuperado en abril de 2021 de https://www.ehu.eus/documents/1736829/2176697/18-Hernandez.indd.pdf

Martínez, J. C. (2017). *El delito de blanqueo de capitales* (Tesis doctoral). Universidad Complutense de Madrid, Departamento de Derecho Procesal.

Perea, I. L. (2017). Nuevas tecnologías aplicadas. *Revista de los Estudios de Derecho y Ciencia Política*, (24), 64-76. Recuperado en marzo de 2021 de https://dialnet.unirioja.es/servlet/articulo?codigo=6207444

Posada, R. (2017). El cibercrimen y sus efectos en la teoría de la tipicidad: de una realidad física a una realidad virtual. *Revista Nuevo Foro Penal Universidad EAFIT*, 13(88), 72-112. Recuperado en marzo de 2021 de https://dialnet.unirioja.es/servlet/articulo?codigo=6074006

Ripollés, J. L. (2017). El bien jurídico protegido en el derecho penal garantista. *Jueces para la democracia*, (30), 3-4. Recuperado en abril de 2021 de https://dialnet.unirioja.es/servlet/articulo?codigo=174728

Rodríguez, I. (2019). *Los delitos económicos en internet* (Tesis doctoral). Universidad de Barcelona.

Suárez, A. (2006). La estafa informática. *Derecho Penal y Criminología*, 27(81), 195-223. Recuperado en abril de 2021 de https://revistas.uexternado.edu.co/index.php/derpen/article/view/991

Temperini, M. (2017). *Deep web, anonimato y cibercrimen*. FIADI. Recuperado el 18 de junio de 2020 de http://fiadi.org/deep-web-anonimato-y-cibercrimen

Ventas, R. (2007). La aplicación del principio de universalidad en la persecución de los delitos cometidos a través del juego por internet. *Revista electrónica de derecho del centro*

universitario de la Ciénega, (4), 7-10. Recuperado en junio de 2020 de http://letrasjuridicas.cuci.udg.mx/index.php/letrasjuridicas/article/view/36/36

Legislación citada

España. (1995). *Ley Orgánica 10/1995, de 23 de noviembre, del Código Penal*. Boletín Oficial del Estado, 24 de noviembre de 1995. Recuperado de https://www.boe.es/buscar/pdf/1995/BOE-A-1995-25444-consolidado.pdf

Asamblea Nacional del Ecuador. (2014). *Código Orgánico Integral Penal*. Registro Oficial Suplemento 180. Recuperado de https://es.wikipedia.org/wiki/C%C3%B3digo_Org%C3%A1nico_Integral_Penal

Jurisprudencia referenciada

La sentencia STS 807/2003, de 03 de marzo, Sala 2ª de lo Penal.

La sentencia STS 358/2015, de 10 de junio, Sala 2ª en lo Penal.