El Fraude Electrónico desde el Contexto Jurídico Venezolano

Electronic Fraud from the Venezuelan Legal Context

Jhenesis Jhosuana Rodríguez Pacheco
Universidad de Carabobo. Facultad de Ciencias Jurídicas y Políticas. Valencia, Venezuela
iD ORCID: https://orcid.org/0000-0002-2884-4681
jhenesis.rodriguez@gmail.com

Recibido: 16-05-2022
Aceptado: 28-06-2022

Resumen

El uso inevitable de las tecnologías de la información y comunicación ha traído consecuencias muy positivas para el desarrollo de la humanidad en general; no obstante, como todo fenómeno visible desde el entorno sociológico del ser humano, ha configurado un espacio fértil para la manifestación de actos antijurídicos que vulneran los derechos de muchos individuos. El presente artículo tiene como objetivo general, analizar desde una visión reflexiva, cómo el delito informático del fraude ha evolucionado y cuál es el impacto de la regulación legal venezolana sobre este flagelo silente que afecta gravemente a una gran cantidad de personas a diario. La investigación se desarrolla empleando la metodología documental, recabando datos bibliográficos desde la doctrina y las normas jurídicas tanto nacionales como internacionales. Arroja como conclusión que, los delitos informáticos son un flagelo ampliamente difundido, el cual debe ser objeto de revisión permanente a nivel social y jurídico para evitar sus graves consecuencias en la privacidad y los datos.
Palabras Clave: Tecnología de la información, delito informático, fraude electrónico, derecho venezolano.

Abstract

The inevitable use of information and communication technologies has brought very positive consequences for the development of humanity in general; However, like any phenomenon visible from the sociological environment of the human being, it has configured a fertile space for the manifestation of unlawful acts that violate the rights of many individuals. The general objective of this article is to analyze from a reflective perspective, how the computer crime of fraud has evolved and what is the impact of Venezuelan legal regulation on this silent scourge that seriously affects a large number of people on a daily basis. The research is carried out using the documentary methodology, collecting bibliographic data from the doctrine and legal norms, both national and international.
Key words: Information technology, computer crime, computer fraud, venezuelan law.

A modo introductorio

Con la instauración de las tecnologías de la información y comunicación (TIC) en la vida social, se ha favorecido la productividad en actividades cotidianas, derivándose de forma implícita, una mayor rapidez en las labores y reducción en los costos. Asimismo, el acceso a medios electrónicos conlleva un uso acelerado de la virtualidad para el procesamiento de los datos requeridos diariamente para subsistir, por lo que, dentro de las múltiples tareas que actualmente

se ejecutan mediante las TIC, se encuentra el ejercicio profesional, el desarrollo laboral, el proceso educativo, las operaciones comerciales, entre otras.

No obstante, el uso de estos medios de comunicación implica también un riesgo a la privacidad, socavándose en muchos casos la protección de datos que se proporcionan para ejecutar las actividades cotidianas: frecuentemente se implementan, de manera delictiva, prácticas que persiguen la obtención maliciosa y fraudulenta de información valiosa, con el propósito de alcanzar un lucro o provecho ilegítimo, manipulando datos ajenos.

Esta clase de fenómenos perniciosos han sido regulados jurídicamente, siendo objeto de estudio por parte del Derecho Penal en diferentes cuerpos normativos, pues, engloban una serie de conductas antijurídicas que aun cuando son similares a otras figuras típicas, poseen como variante el manejo de un entorno informático que lo ajusta a los contextos telemáticos modernos, conociéndose así, desde el argot legal, como “delitos informáticos”.

En sus inicios, este tipo delictivo fue definido de numerosas formas ya que, no en todas las naciones existía una visión firme sobre los mecanismos de criminalidad que se dirigen a través de los medios tecnológicos. Sin embargo, diferentes doctrinarios se atrevieron a establecer conceptualizaciones primarias, destacándose por su pertinencia, la propuesta por Jijena (1994) que plantea como delito informático a “… toda acción típica, antijurídica y culpable, para cuya consumación se usa la tecnología computacional o se afecta a la información contenida en un sistema de tratamiento automatizado de la misma…” (p. 508)

Partiendo de esta concepción, se puede afirmar que es menester la concurrencia del uso de un medio tecnológico (equipo, dispositivo, plataforma, red, entre otros) y la afectación perjudicial de una información o dato que éste contenga, para que se evidencie la ejecución de un delito informático.

De esta manera se enfatiza que, a lo largo de su existencia, los delitos informáticos han presentado diferentes modalidades, demostrando un amplio alcance a nivel geográfico o poblacional, así como, respecto al perjuicio que se ocasiona mediante estas prácticas, poniendo en riesgo la seguridad cibernética a través de la manipulación de datos personales, económicos, identidad o de valor.

Igualmente, se afirma que el aumento de delitos informáticos es proporcional al uso de las TIC, pues, el grado de interacción telemática actual, inevitablemente expone a la humanidad a estos fenómenos. Específicamente en Venezuela, se han presenciado múltiples casos relacionados a delitos informáticos que, en su mayoría, persiguen fines económicos. Sin embargo, dentro de la dinámica social se cuenta con normas jurídicas que regulan especialmente la criminalidad informática.

La Ley Especial contra los Delitos informáticos, vigente desde 2001, es la norma venezolana que rige la protección integral de las TIC y sus sistemas, previniendo y sancionando aquellos delitos ejecutados a través de ellos o en su perjuicio. En el referido texto legal, se plasman delitos que afectan intereses jurídicos específicos, como aquellos que atentan contra los niños y adolescentes, el orden económico, la propiedad, la privacidad de las personas y de las comunicaciones.

El presente estudio, esboza un análisis reflexivo sobre uno de los delitos tipificados en esta Ley especial: el fraude como delito informático. Cuando se trata el fraude relacionado con herramientas de tecnología e información, se hace referencia a uno de los crímenes silentes más populares en los últimos años, puesto que, el *modus operandi* para su efectividad, es la mimetización de instrucciones falsas o fraudulentas en sistemas informativos, con la finalidad de obtener de manera injusta un provecho. Esta práctica ilícita es frecuente, principalmente a través de plataformas, correos electrónicos y redes sociales, por lo que, se vislumbra como un atentado claro a la privacidad de datos personales y económicos de muchos individuos.

Para comprender de manera clara el alcance del fraude informático se estudia, en principio, su regulación a nivel internacional, su penalidad dentro del orden jurídico venezolano, los diferentes contextos en los que comúnmente se origina este delito.

Generalidades sobre los delitos informáticos

La incorporación de tipos penales en el estudio de la ciencia jurídica se observa como un proceso poco sencillo, que se realiza en paralelo a la experimentación de fenómenos sociales y su impacto en el orden colectivo. Con el apogeo de las tecnologías de la información en la entrada del siglo XXI, se visualizaba que el uso de estas herramientas multifuncionales podía originar grandes beneficios que, cambiarían sin lugar a dudas, las relaciones interpersonales.

Particularmente, la Ley Especial contra los Delitos Informáticos define las Tecnologías de la Información en su artículo 2 literal “a” de la siguiente manera:

> Tecnología de Información: rama de la tecnología que se dedica al estudio, aplicación y procesamiento de datos, lo cual involucra la obtención, creación, almacenamiento, administración, modificación, manejo, movimiento, control, visualización, transmisión o recepción de información en forma automática, así como el desarrollo y uso del “hardware”, “firmware”, “software”, cualesquiera de sus componentes y todos los procedimientos asociados con el procesamiento de datos.

En principio, las consecuencias del uso de las nuevas tecnologías son favorables para el manejo de datos y la trasmisión expedita de información, pero, la ausencia de controles que reglamentaran la interacción del hombre con estas herramientas implicaba, para aquel momento histórico, un gran riesgo. Como es conocido, en la actualidad TIC son instrumentos que se encuentran en permanente actualización, tanto a nivel informático como en sus características físicas. Esa evolución busca generar entornos amigables, cómodos, eficaces al almacenar datos y, sobre todo, rapidez en el uso.
Además, hoy se persigue que estos mecanismos conserven la privacidad de datos, lo cual, para sus inicios, era un problema ignorado: los equipos utilizados inicialmente tenían como propósito establecer la comunicación remota y al ser novedoso, la regularización jurídica era casi inexistente, por lo que surgió en paralelo, su uso delictivo como un factor negativo.

El manejo de la internet y su incorporación en herramientas tecnológicas como los móviles, originó también el desarrollo de diferentes formas de captación indebida de información: datos, imágenes, contraseñas, identificación, correos, inclusive accesos a redes sociales, son algunas de las artimañas que los ciberdelincuentes han diseñado para sustraer criminalmente y causar perjuicios en la web a nivel mundial; no obstante, la problemática surge cuando se manifiestan estas conductas y no existe la regulación jurídica que le otorgue una sanción.

Al respecto, Ojeda et al. (2010) establecieron lo siguiente:

> … las entidades que desarrollaban o trabajaban en los escenarios informáticos del mundo, comenzaron a generar instrumentos de control y sanción a quienes en forma inescrupulosa utilizaban la informática para delinquir. Sin embargo, se encontró que los entes encargados de sancionar a quienes hacían uso ilegal y delictivo de las herramientas informáticas, no tenían cómo judicializar a los nuevos delincuentes. La ley inglesa sirvió para que otros países –en especial aquellos donde la internet tenía más desarrollo– se sumaran al esfuerzo de discutir y promulgar leyes orientadas a proteger y sancionar la violación de la información… (p. 45).

Era imperioso que la desregulación del uso de las TIC diera paso a la creación de normas jurídicas que previnieran y/o sancionaran estas conductas. Esta necesidad tenía carácter global, pues la cibercriminalidad no radica en un país, sino que tenía presencia en distintos lugares debido a la globalización.

En 2001, Europa se tomó con seriedad esta temática, unificando criterios y dando origen a una norma jurídica internacional, relevante incluso para la actualidad: el Convenio sobre la cibercriminalidad. Este cuerpo normativo elaborado por el Consejo de Europa, consta de 48 artículos y es también conocido como Convenio de Budapest, siendo creado para luchar por la protección de los intereses públicos y particulares inmersos en el uso y desarrollo de las TIC, así como prevenir vulneraciones a la privacidad, la identidad de personas y la integridad de los sistemas, conformándose así, como una normativa vital.

De acuerdo a su contenido, se contemplan medidas que debe adoptar cada nación parte, en cuanto a los siguientes delitos:

- Delitos contra la confidencialidad, la integridad y la disponibilidad de los datos y sistemas informáticos.
- Delitos informáticos.
- Delitos relacionados con el contenido.
- Delitos relacionados con infracciones a la propiedad intelectual y de los derechos afines.
- Otras formas de responsabilidad y sanción.

En el momento en que se promueve la creación de este Convenio sobre la Cibercriminalidad como norma europea que tipifica delitos informáticos, en Suramérica, específicamente en el territorio venezolano, nace una normativa legal que tipifica y sanciona esta materia para el orden interno y que es conocida como “Ley Especial contra los delitos informáticos”. Es así como se constata que, la evolución tecnológica y el acceso amplificado a la internet despertó la necesidad para muchas naciones del planeta, de generar leyes que controlaran el uso de los sistemas informáticos más allá de lo que la tecnoética podía plantear.

Nacimiento de los delitos informáticos en el territorio venezolano

El avance tecnológico del nuevo siglo (XXI) se afianzó en la gran mayoría de los países del planeta, por tanto, Venezuela no pudo escapar de este proceso transformador. El uso de equipos de telecomunicación, computadores, redes, entre otros sistemas, creó en la sociedad venezolana gran expectativa hacia el porvenir. La proyección de las tecnologías de comunicación e

información como un elemento esencial para la vida cotidiana, especialmente en el tema de la participación y suministro de datos, era indudable, lo que conllevó al uso incrementado de la informática, pero al mismo tiempo, también la cibercriminalidad tuvo lugar en muchos escenarios cotidianos.

Dada las circunstancias de incertidumbre que se forjaron ante la innovación tecnológica, dentro del territorio venezolano se adoptaron medidas rápidas para crear un cuerpo jurídico que pudiera tipificar cada una de las conductas vulnerantes de derechos que eran perceptibles dentro de la sociedad de la comunicación, contextualizado con los antecedentes criminológicos que se observaban en el conglomerado social del país para ese entonces. De esta manera, se creó la Ley Especial contra los Delitos Informáticos, un instrumento legal realmente novedoso y sin precedentes que sancionaría los tipos penales vinculados al uso inadecuado de los sistemas de información, redes, dispositivos y manipulación de datos, incorporándose al ordenamiento interno venezolano como norma especial de la materia penal.

Dicha Ley Especial se promulga como mecanismo idóneo para dar solución a ese conflicto que de *facto* produjo la utilización exacerbada de las TIC en la nación venezolana: se promovió y extendió el uso de las herramientas tecnológicas que involucraban el suministro de datos para su configuración e individualización, sin tener un método efectivo para impedir actos fraudulentos o delictivos, por tanto, era menester una actuación legislativa expedita que aminorara esa inseguridad informática que se presentaba en el ciudadano, adecuando así el Derecho a las nuevas realidades.
Al respecto, Mendoza y Urdaneta (2010) establecen que, dentro de las grandes complejidades derivadas de esa evolución tecnológica continua, destacan los vacíos legales que son expuestos ante la velocidad con la que penetran las TIC dentro de la sociedad y, asimismo, examinan otra serie de dificultades, a saber:

Uno de los problemas más complejos que las nuevas tecnologías plantean al derecho, lo constituye la regulación de aquellos actos antijurídicos que utilizan la tecnología telemática como medio o fin en la comisión de delitos. Factores como la naturaleza técnica de estos delitos, su extraterritorialidad, la necesidad de adiestramiento constante, la falta de convenios y acuerdos internacionales en esta materia, lo complejo y costoso de las herramientas necesarias para perseguirlos, la continua actualización de la tecnología telemática y la falta de cultura de seguridad informática, son elementos a considerar al momento de realizar cualquier análisis sobre esta materia, sobre todo al momento de elaborar leyes que los penalicen. (p. 121)

Sin lugar a dudas, la Ley Especial contra los Delitos Informáticos representó en el año 2001, un trabajo arduo tanto a nivel académico, jurídico como legislativo, puesto que, se diseñó como un orden sancionatorio futurista que pretendía alcanzar con gran amplitud, los supuestos de hecho que implicaran de una u otra manera, transgresiones a los derechos de los individuos, encuadrado en la óptica imparable y mutable del mundo informático.

Para el tratamiento de esta nueva especie de delitos, en este cuerpo normativo penal se incorporaron artículos que describen la intención del agente y la sanción correspondiente, comprendiendo delitos de carácter informático que atentaren contra:

- Los sistemas que utilizan tecnologías de la información (Capítulo I)
- La propiedad (Capítulo II)
- La privacidad de las personas y de las comunicaciones (Capítulo III)

- Niños, niñas y adolescentes (Capítulo IV)
- El orden económico (Capítulo V)

Englobando asimismo dentro de su texto legal, la penalización de delitos como el acceso indebido, el espionaje informático, la falsificación de documentos, el hurto, la violación a la privacidad, la pornografía infantil, apropiación de propiedad intelectual, entre otros. Esta norma rescata el carácter responsable y preventivo que debe impregnarse en todas las políticas del Estado para la promoción de una cultura informática segura que implícitamente conlleve el correcto uso de los sistemas y las comunicaciones telemáticas. Con la Ley Especial contra los Delitos Informáticos se previó desde los inicios de la digitalización y la telematización en Venezuela, la sanción a las conductas antijurídicas, sin necesidad de que el administrador de justicia invocare o se adhiriera a otras normas penales que no rigieran específicamente la esfera de las TIC, ya que, su ámbito de aplicación no es restringido y los supuestos de hecho tipificados sobre los cuales se extiende, contemplan las diferentes maneras modernas de comunicarse y los nuevos espacios de almacenamiento de información.

En definitiva, la Ley especial sobre delitos informáticos se vislumbra como un enlace entre la ciencia jurídica tradicional, organizativa, coactiva y sancionatoria para el control social y, las nuevas tecnologías libres y dinámicas. Representa la regularización ideal sobre el flujo permanente de datos que cada persona genera día a día en la red, incluso a través del uso normal de dispositivos comunes como teléfonos y computadores, advirtiendo y castigando actos que pueden ser catastróficos para personas naturales y jurídicas como las estafas en línea y la suplantación de la identidad digital, por lo que, se puede aseverar que fue el primer paso legislativo que acertadamente tomó Venezuela, con la firme finalidad de establecer una política de seguridad informática y digital.
Por último, se debe resaltar que en esta norma jurídica se plasma el tipo penal objeto de análisis de esta investigación: el fraude informático, estipulándolo dentro del Capítulo II como un delito contra la propiedad y estableciendo al sujeto activo culpable, una sanción que comprende pena corporal de prisión y una pena de carácter pecuniaria.

El fenómeno del fraude y su evolución dentro de la sociedad

Antes de adentrar en el estudio jurídico del fraude informático, es necesario hacer referencia a la esencia del fraude desde una óptica clásica. En primer lugar, se puede afirmar que el fraude como delito, es conocido y evidenciable a lo largo de la historia de la humanidad. Este tipo penal tiene como característica particular, el aprovechamiento de la manipulación, la falsedad y el engaño por parte del sujeto activo con el objetivo de lograr un beneficio indebido, utilizando y afectando principalmente la confianza.

Para definirlo doctrinariamente, se puede señalar la conceptualización suministrada por García (2018) quien observa que “El fraude es un delito intencional en el cual el delincuente daña el patrimonio ajeno valiéndose de engaños o aprovechándose del error de la víctima y lo comete …omissis…” (s/p)

Conociendo esta definición básica del delito de fraude, se hace menester puntualizar cuáles son aquellos elementos que constituyen y distinguen al fraude clásico de cualquier otro crimen. Para dar respuesta a ese planteamiento, Cano (2011) aporta lo siguiente:

- En primer lugar, para que exista un fraude, y no un simple robo o hurto, debe haber una *confianza defraudada.*

- El medio por el cual alguien se aprovecha de esta confianza es el de una *representación falsa de hechos materiales.*
- Esta representación es *creída* por la persona a la cual está destinada, mientras que *el defraudador no cree en ella.*
- El defraudador obtiene un *beneficio indebido* a partir de lo que la persona defraudada *hace o deja de hacer* en virtud de la falsa representación. (p. 22)

Es así entonces como el tipo penal del fraude está orientado a generar una lesión, principalmente en el patrimonio del sujeto pasivo, de manera instantánea y, que se materializa con efectividad cuando el agente dispone de ese interés económico o patrimonial engañosamente apropiado (beneficio obtenido injustamente). De igual forma, la conducta antijurídica del fraude ha incursionado en diferentes ámbitos de la cotidianidad: se han presenciado fraudes en el marco del contexto empresarial, laboral, fiscal, electoral, entre otros. Sin embargo, es menester especificar que, únicamente pueden ser víctimas de fraude las personas físicas pues, sólo ellas poseen la capacidad necesaria para ser engañadas y suministrar información patrimonial en beneficio (indebido) del sujeto criminal.

Ahora bien, la extensión del fraude se ha amplificado de tal forma, que inclusive las tecnologías de información y comunicación en los últimos años, han figurado como canales utilizados por cibercriminales para implantar dolosamente en sistemas y redes, mecanismos engañosos de captación con el fin de recabar datos relevantes que puedan ser manipulados y generar a su favor, un provecho injusto en perjuicio del titular de la información. De esta forma, el fraude manifiesta una nueva versión que básicamente se apoya en el manejo de las TIC para incentivar esa conexión entre el autor delictivo y el sujeto pasivo, presentando, además, diferentes matices.

Por otro lado, también es válido acotar que los casos actuales de fraude informático podrían depender en gran porcentaje del acceso a internet, e igualmente, se pueden vincular a otros delitos de carácter informático por la similitud en el modo operante. Inclusive, suele confundirse el fraude informático con otros delitos como el espionaje electrónico o la suplantación de identidades, pues, por lo general, éstos son ejecutados por los ciberdelincuentes mediante sistemas y artificios bastante parecidos a los requeridos para cometer el fraude informático, pero, cada delito se caracteriza por el daño específico que genera en la víctima.

En este orden de ideas, Mayer y Oliver (2020) exponen que es necesario delimitar con exactitud el concepto de "fraude informático", puesto que:

> ... una adecuada delimitación del fraude informático plantea la conveniencia de abandonar una aproximación laxa a dicho concepto y, por el contrario, destinar esfuerzos a definirlo de manera estricta, sobre la base de tres elementos copulativos: la conducta, el resultado y el ánimo del agente. Pero, antes de emprender esa tarea, resulta necesario deslindar al fraude informático de otros comportamientos con los que tradicionalmente ha sido vinculado a nivel doctrinal y normativo... (p. 156)

El fraude informático, al igual que los demás delitos de esta materia, tiene como característica principal la transformación constante, por lo que es de suma importancia que, tanto a nivel doctrinario como legal, se establezca una conceptualización concreta que oriente al jurista en el momento de estudiar el ánimo del sujeto actuante.

Fraude como tipo penal informático: Visión desde la legislación venezolana

Como se ha explicado a lo largo de esta investigación, la Ley Especial contra los Delitos Informáticos es la norma jurídica regente que tipifica el fraude informático, específicamente en su artículo 14, que manifiesta:

> Artículo 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.

El legislador clasificó el fraude informático como un delito contra la propiedad, debido a que su propósito principal es originar en el sujeto pasivo o víctima, un perjuicio netamente patrimonial. Al ser inicialmente de carácter económico, es uno de los cibercrímenes más comunes dentro del colectivo: el uso vertiginoso de las redes sociales, la mensajería instantánea, el uso de correos electrónicos, la digitalización de la banca y las operaciones financieras vía web, han sido caldo de cultivo para que, dentro de la delincuencia organizada venezolana, se ideen nuevas formas de fraude.

En los últimos años, las situaciones de fraude informático han afectado principalmente a adolescentes y adultos mayores, siendo este sector de la población, quien utiliza con mayor frecuencia los canales digitales y el internet, interactuando en plataformas o redes sociales abiertamente durante más cantidad de horas al día. El uso de los dispositivos móviles y de computadores para la agilización de las tareas cotidianas, sin tomar las medidas de seguridad cibernética, generan mayor riesgo para estos grupos vulnerables, por lo que encajan fácilmente en el perfil de víctima que persiguen la delincuencia informática.

La realización del fraude informático se produce comúnmente cuando la víctima accede a un sistema, alguno de sus componentes, red o base de datos que haya sido alterado de manera maliciosa, e ingresa la información necesaria para que se materialice el perjuicio en contra de su propiedad o patrimonio. Claramente, el canal empleado por el agente es una tecnología de la información y comunicación, e incluso, puede generar el hecho fraudulento de manera extraterritorial y/o sin conocer personalmente a la víctima, puesto que, únicamente se requiere la manipulación de la TIC para la obtención indebida del provecho injusto perseguido.

La conceptualización plasmada en la Ley Especial antes mencionada es tan amplia que podría abarcar supuestos de hecho como el "*phishing*" o el "*pharming*" que son modalidades modernas utilizadas por la cibercriminalidad para captar datos financieros de sus víctimas mediante correos electrónicos o páginas web falsas, con el fin de defraudar sus cuentas bancarias. Con estos dos últimos delitos, se puede observar cómo evoluciona constantemente el crimen en la red, poniéndose de manifiesto incluso en plataformas como *Whatsapp* o *Instagram.*

La sanción contemplada por la Ley Especial contra los Delitos Informáticos para el fraude es dual: el legislador establece una sanción de tipo corporal caracterizada por la pena de prisión de entre tres (3) a siete (7) años y, además una pena de índole pecuniaria que abarca desde trescientas (300) hasta setecientas (700) unidades tributarias; no obstante, por lo general los delincuentes que se dedican a esta clase de cibercrímenes cometen otros delitos como, por

ejemplo, asociación para delinquir, ya que, normalmente son grupos de delincuencia organizada los que operan para perjudicar de esta manera a muchos ciudadanos.

Fraude y hurto informático: diferencias según la Ley Especial Contra los Delitos Informáticos

Al realizar un estudio pormenorizado de las normas legales que componen la Ley Especial contra los Delitos Informáticos de 2001, se puede percibir con gran facilidad que los supuestos de hecho tipificados guardan una similitud bastante particular y, esto se debe, a que el medio de ejecución material es siempre una herramienta TIC. Es por este motivo, que se presenta con gran frecuencia mucha confusión en estudiantes de Derecho cuando analizan la norma o, en los ciudadanos en general cuando son víctimas de estos delitos y, es recurrente, la vinculación que se realiza entre el fraude y el hurto informático.

No obstante, más allá del conocimiento popular que se tiene sobre estas 2 clases de delitos informáticos, es de gran importancia resaltar que ambos tipos penales son diferentes, tal es así, que ambos está contemplados por separado en la Ley especial nacional. Específicamente cuando se hace alusión al delito de hurto informático, se debe hacer mención del artículo 13 de la Ley, que contempla taxativamente lo siguiente:

> Artículo 13. Hurto. Quien, a través del uso de tecnologías de información, acceda, intercepte, interfiera, manipule o use de cualquier forma un sistema o medio de comunicación para apoderarse de bienes o valores tangibles o intangibles de carácter patrimonial sustrayéndolos a su tenedor, con el fin de procurarse un provecho económico para sí o para otro, será sancionado con prisión de dos a seis años y multa de doscientas a seiscientas unidades tributarias.

Si se observa con detenimiento el contenido del artículo y el espíritu del legislador en la redacción, se puede claramente afirmar que el hurto involucra la firme intencionalidad de ≪*apoderarse de bienes o valores tangibles o intangibles de carácter patrimonial sustrayéndolos de su tenedor*≫, esa intención de tomar para sí un bien mediante la manipulación de una TIC, arrebatándolo de su titular, es lo que distingue el hurto del fraude informático.

Como bien se ha explicado, el fraude se fundamenta en la manipulación de un sistema tecnológico o cualquiera de sus componentes para así conseguir introducir instrucciones falsas que permitan al agente alcanzar un provecho injusto, por tanto, cuando se suscita el fraude electrónico, no precisamente se persigue con inmediatez la apropiación de un bien que posea la víctima.

Estos dos delitos dentro de la cotidianidad venezolana, son bastante populares y han afectado el patrimonio de muchos individuos, por ello generalmente están relacionados; no obstante, es necesario el establecimiento de una distinción bien definida a fin de que jurídicamente no sean objeto de confusión por los administradores de justicia.

Conclusiones generales

Los delitos informáticos, a pesar de su popularidad y gran impacto en la población tanto venezolana como mundial, debido a los perjuicios que genera la cibercriminalidad, no han sido objeto de un estudio profundo a nivel doctrinario o jurisprudencial. Es necesario que, aquellos

conocedores y profesionales del Derecho, incentiven la creación de una cultura sobre seguridad informática en la sociedad, que tenga como propósito la prevención y erradicación efectiva de esta clase de flagelo que afecta a niños (as), adolescentes y adultos.

De igual forma, es obligatorio concientizar a la población sobre los alcances, *modus operandi* y daños que generan los ciberdelincuentes mediante estos delitos; educando, asimismo, a las personas para que oportunamente denuncien este tipo de casos y generen la posibilidad de desarticular las redes delictivas que operan en la sombra del internet.

La conciencia sobre la privacidad de los datos personales, el resguardo de la información confidencial, el conocimiento de la Ley Especial contra los Delitos Informáticos, el respeto a la identidad digital de las demás personas y la actuación segura en las redes, son algunas de las medidas que se pueden ejecutar diariamente para evitar la materialización de más delitos informáticos.

Mitigar el crecimiento de estos crímenes es responsabilidad de todos los ciudadanos, además, se debe exigir una política de Estado que vigile continuamente la operatividad de las normas jurídicas pertinentes y su correcta aplicación; por su parte, los administradores de justicia están llamados a analizar, estudiar y comprender las trascendencias de estos tipos penales, puesto que, son fenómenos que se han ido afianzando con el tiempo y que evolucionan al paso que avanza la tecnología.

Referencias

Cano, D. (2011) Contra el fraude: Prevención e Investigación en América Latina. Ediciones Granica. Argentina. Disponible en: https://books.google.co.ve/books?id=lwkdBgAAQBAJ&printsec=frontcover&dq=Contra+el+fraude:+Prevenci%C3%B3n+e+Investigaci%C3%B3n+en+Am%C3%A9rica+Latina&hl=es&sa=X&redir_esc=y#v=onepage&q=Contra%20el%20fraude%3A%20Prevenci%C3%B3n%20e%20Investigaci%C3%B3n%20en%20Am%C3%A9rica%20Latina&f=false

García, R. (2018) El delito de fraude y sus modalidades. Ediciones Fiscales ISEF. ISBN-978-607-541-082-1, México. Disponible en: https://books.google.co.ve/books?id=pJdxDwAAQBAJ&printsec=frontcover&dq=el+delito+de+fraude+y+sus+modalidades&hl=es&sa=X&redir_esc=y#v=onepage&q=el%20delito%20de%20fraude%20y%20sus%20modalidades&f=false

Jijena, R. (1994) La criminalidad informática: situación de lege data y lege ferenda en Chile. *Informática y derecho: Revista iberoamericana de derecho informático*, (4), 507-514. Disponible en: https://dialnet.unirioja.es/servlet/articulo?codigo=251086

Ley Especial los contra Delitos Informáticos. 2001. Gaceta Oficial de la República Bolivariana de Venezuela Nro. 37.313.

Mayer, L. Oliver, G. (2020). El delito de fraude informático: concepto y delimitación. *Revista Chilena de Ciencia y Tecnología, 9*(1). pp.151-184 Disponible en: DOI: 10.5354/0719-2584.2020.53447

Mendoza, E. Urdaneta, E. (2005). La telemática y los delitos informáticos en Venezuela. *Revista Electrónica de Estudios Telemáticos. 4*, (1), . 124-140. Universidad Rafael Belloso Chacín Disponible en: https://dialnet.unirioja.es/servlet/articulo?codigo=2967374

Ojeda. R. et al. (2010). Delitos informáticos y entorno jurídico vigente en Colombia. *Cuadernos de Contabilidad.11* (28). Disponible en: http://www.scielo.org.co/scielo.php?script=sci_arttext&pid=S0123-14722010000200003

Acerca de la autora

Jhenesis Jhosuana Rodríguez Pacheco.
Abogada (UC). Maestrante en Derecho del Trabajo. Profesora adscrita al departamento de Derecho Romano de la Facultad de Ciencias Jurídicas y Políticas de la Universidad de Carabobo. jhenesis.rodriguez@gmail.com.
ORCID iD: https://orcid.org/0000-0002-2884-4681