Universidad Abierta Interamericana

2022

Abogacía

"LAS DEFRAUDACIONES INFORMÁTICAS EN LA ÉPOCA DE PANDEMIA Y LA IMPLICANCIA DEL PRINCIPIO DE LEGALIDAD"

Tutora: de Líbano Elorrieta, Desirée Aylén

Alumna: Scandizzo, Iona Anabella

Correo electrónico: ionascandizzo@hotmail.com

Teléfono: +542974205384

Carrera: Abogacía

Título a obtener: Abogada

Área temática: Derecho Penal

Fecha de entrega: 3 de agosto de 2022

“Nada tiene tanto poder para ampliar la mente como la capacidad de investigar de forma sistemática y real todo lo que es susceptible de observación en la vida”.

Marco Aurelio

Agradecimientos

A Mariela y Christian, mis padres, que confiaron en mí y me dieron esta hermosa oportunidad. Gracias por acompañarme en cada paso.

A mis abuelos, que siempre se alegraron por mis logros, que estuvieron presentes a pesar de la distancia. En especial, a mi abuela Matilde, que ya no está entre nosotros, pero aun así me hizo sentir acompañada en todo momento.

A mis amigas de la vida que siempre estuvieron al pie del cañón e hicieron más fácil el proceso.

A Jordán, Guillermina, Micaela y Franco, mis compañeros de la carrera, que se terminaron convirtiendo en mis amigos y en un pilar fundamental en este camino.

A mi tutora, Desirée, por la paciencia, comprensión, predisposición y su tiempo dedicado desde el primer día.

Índice

Resumen 7
Área temática 7
Problemática 7
Justificación jurídica 8
Metodología 8
Objetivos 8
Hipótesis 9
Introducción 9
Marco normativo 10
Marco Teórico-Referencial 10
Definición de delito 10
Delitos informáticos 11
Estafas y otras defraudaciones 12
Estafa informática 12
Manipulación informática 12
Principio jurídico 12
Principio de legalidad 12
Tecnología 13
Informática 13
Sistemas informáticos 13
Capítulo I 15
I. Sistemas informáticos 16
II. Historia y evolución de los ordenadores 18
III. El Internet y el ciberespacio 22
IV. Avance de la ciberdelincuencia 24
Capítulo II 27
I. Delitos informáticos 28

I. a) Definición 28
I. b) Características 31
I. c) Clasificación 33
II. Normas convencionales 34
II. a) Convenio de Budapest 34
II. b) Ley Nacional de Delitos Informáticos (N° 26.388) 36
Capítulo III 39
I. Estafas y defraudaciones informáticas 40
II. Estructura típica del tipo penal 43
II. a) Aspecto objetivo 44
II. b) Aspecto subjetivo 46
III. Defraudaciones informáticas en pandemia 47
Capítulo IV 54
I. Phishing 55
I. a) Pharming 60
I. b) Smishing 61
II. Vishing 62
III. Carding 62
IV. Hacking 63
V. Cracking 63
VI. Warez 65
VII. Ransomware 65
VIII. Viruking 66
Capítulo V 67
I. Introducción 68
II. Principio de legalidad 68
III. Características 70
i. Lex Scripta 70

ii. Lex Previa 71
iii. Lex Stricta 71
iv. Lex Certa 72
Conclusión 75
Referencias 78
Bibliografía 78
Legislación 79
Otros 79
Jurisprudencia 85

Resumen

En el presente trabajo de investigación se analiza cómo incide el principio constitucional de legalidad, sobre todo la *lex certa*, en el tipo penal de defraudación informática encontrado en el artículo 173, inciso 16 del Código Penal de la Nación.

Se desarrollarán los sistemas informáticos y la transmisión de datos, sus respectivas definiciones, el origen y cómo fueron evolucionando al pasar los años. También se indagará sobre la manera en que los delincuentes emplean estos sistemas informáticos para cometer delitos, lo que también generó que en el período pandémico estos tipos de delitos aumentarán exponencialmente.

A tal fin profundizaremos sobre los delitos informáticos, sus características y clasificación, con la finalidad de introducir y facilitar lo que respecta a las estafas informáticas. De igual modo, se enunciarán cuáles son las normas en materia de ciberdelincuencia que existen en Argentina, ahondando lo que determina cada una.

Todo ello con el objeto de inmiscuirnos en lo que respecta a las estafas informáticas, analizando el tipo penal y la redacción del mismo. Asimismo, explicaremos cuáles son los modos en los que los ciberdelincuentes cometen este tipo de delito.

Finalmente, determinaremos si la figura típica se ajusta al principio de legalidad, para lo cual explicaremos su significado y desglosaremos sus características, enfocándonos principalmente en la ley cierta.

Área temática

El presente trabajo estará enfocado, principalmente, en el **derecho penal,** entendido éste como aquella rama del derecho que se encarga de regular la potestad estatal de castigar, determinando lo que es punible y sus consecuencias.

Por otro lado, se abordará el **derecho constitucional** mediante el análisis del principio de legalidad.

Problemática

Puesto a que la tecnología avanza de manera apresurada y la población va adaptándose a ella, aumentando así el uso de medios informáticos, los ciberdelincuentes encontraron su provecho en el ascenso inmensurable del empleo del internet y de las

nuevas tecnologías por parte de los ciudadanos argentinos y para beneficiarse de ello intentando distintas maniobras para obtener un aumento en su patrimonio.

Ahora bien, a las diferentes maniobras delictivas mediante el empleo de las nuevas tecnologías, le sería aplicable el delito previsto por el art. 173 inc. 16 del CP. No obstante, es menester analizar si dicha normativa trastoca el principio de legalidad, particularmente la *lex certa*, por cuanto en su amplia redacción habilita la aplicación del tipo penal a gran cantidad de maniobras diferentes y hasta desconocidas a la fecha.

Justificación jurídica

La relevancia jurídica radica en determinar si la redacción del tipo penal de defraudaciones informáticas (artículo 173 inciso 16 del Código Penal de la Nación) trastoca el principio constitucional de legalidad, especialmente la exigencia de ley cierta y, por lo tanto, debería ser modificado o si es preciso mantenerlo, entendiéndolo como una forma de flexibilizar el principio sin vulnerarlo.

Metodología

La metodología empleada será la de una discusión teórica proponiéndonos la elaboración y desarrollo del tema, utilizando la recolección de datos relevantes para luego analizarlos.

Además, se aplicará el método hipotético-deductivo ya que propondremos una hipótesis particular a partir de datos generales.

Objetivos

a. Objetivos generales:

   Identificar de manera concreta cómo incide el principio constitucional de legalidad, específicamente la *lex certa*, en el artículo 173, inciso 16 del Código Penal de la Nación, y si el tipo penal conculca dicho precepto constitucional.

b. Objetivos particulares:

   i. Definir a los sistemas informáticos, profundizando en su origen y evolución;

ii. Profundizar en qué consisten ciberdelitos, especialmente la defraudación informática;
iii. Exponer acerca del principio constitucional de legalidad, haciendo hincapié en la ley cierta.
iv. Determinar y explicar las distintas tácticas utilizadas por los estafadores informáticos para realizar su cometido;
v. Analizar el aumento de estafas informáticas durante la pandemia del *Covid-19*;
vi. Determinar si el principio constitucional de legalidad se encuentra afectado por la redacción del delito de defraudación informática.

Hipótesis

La forma en la que se encuentra redactado el tipo penal de defraudación informática (art. 173 inc. 16 del Código Penal de la Nación) permite abordar las diversas maniobras de comisión del delito sin afectar el principio constitucional de legalidad.

Introducción

El avance tecnológico provocó no solo un cambio en la vida cotidiana de las personas, sino que también un aumento en la comisión de estafas a través de sistemas informáticos. Esto produjo que el Estado argentino tenga que subsanar estos daños que se causaban mediante la tecnología y el Poder Legislativo sancionó la ley 26.388 que modificó el Código Penal de la Nación e incluyó -entre otras figuras penales- a las defraudaciones informáticas dentro del cuerpo normativo en su artículo 173 inciso 16.

Durante el período pandémico, los ciudadanos comenzamos a utilizar aún más los medios tecnológicos, ya que las actividades cotidianas, laborales o educativas solo podían realizarse virtualmente. En esta época, las estafas informáticas incrementaron mucho más.

Partiendo de ahí, se analiza el tipo penal de defraudación informática y, para ello, consideramos pertinente desarrollar respecto de los sistemas informáticos y cómo los delincuentes se aprovechan de ellos para obtener un beneficio económico, es decir, las modalidades a partir de las cuales el delito quedaría configurado.

Finalmente brindaremos una conclusión a fin de establecer si la forma en la que se encuentra redactado el tipo penal en análisis conculca el principio de legalidad o si es constitucionalmente admisible ante el avance tecnológico de la nueva era. En consecuencia, ahondaremos en el precepto constitucional abarcando cada exigencia del mismo, especialmente en la ley cierta.

Marco normativo

En noviembre del año 2001 se firmó el primer y único acuerdo internacional que tiene como objetivo proteger a la sociedad frente a los delitos informáticos y los delitos en internet. La finalidad del **Convenio de Budapest** es crear las leyes adecuadas, mejorar las técnicas de investigación y aumentar la cooperación entre los países parte.

Entró en vigencia en el mes de julio del 2004 y fue ratificado por más de cincuenta países, incluida la Argentina, la cual se adhirió en el año 2018 mediante la sanción de la ley N° 27.411. Aun habiendo aprobado el mismo, los legisladores decidieron reservarse ciertas temáticas justificando tales.

Por otro lado, la ley de **delitos informáticos** (N° 26.388) que modifica, sustituye e incorpora figuras típicas en el Código Penal de la Nación.

Y, en particular, interesa desarrollar el artículo 173 inciso 16 del Código Penal de la Nación.

Marco Teórico-Referencial

Definición de delito

Para Carrara[1] el delito es "la infracción de la ley del Estado, promulgada para proteger la seguridad de los ciudadanos, resultante de un acto externo del hombre, positivo o negativo, moralmente imputable y políticamente dañoso". Para él no es ni una conducta ni una prohibición legal, sino que es un ente jurídico, la lesión de un derecho por obra de una acción u omisión humana y la infracción de la ley del Estado.[2]

El Dr. Zaffaroni[3] entiende que un delito es una conducta humana que tiene a la tipicidad, antijuricidad y culpabilidad como caracteres positivos. Esto quiere decir

[1] Carrara, F. "*Programa di Diritto Criminale",* Editor Tip. Giusti, Sapienza - Università di Roma (Biblioteca Interdipartimentale di Scienze Giuridiche - Filosofia del Diritto Giorgio Del Vecchio, 1867.
[2] Fontán Balestra, C. "*Tratado de Derecho Penal"*, Tomo I, Abeledo Perrot, 2° edición, Buenos Aires, 1980, pág. 326
[3] Zaffaroni, E. R. "*Estructuras Básicas del Derecho Penal"*, EDIAR, 1° edición, 2009, págs. 57, 59.

que, para que aquella conducta humana sea un delito debe generar un pragma conflictivo de bienes ajenos y prohibido con relevancia penal por una fórmula legal que es el tipo o supuesto de hecho legal (tipicidad); la conflictividad del pragma no debe estar resuelta por el orden jurídico mediante ningún precepto permisivo que ratifique la libertad constitucional (antijuricidad) y el injusto debe serle reprochable al agente en forma personal, lo que no sucede cuando no le era exigible un comportamiento conforme al derecho en la concreta situación constelacional en que actuó.

Delitos informáticos

La doctrina todavía no ha encontrado un concepto unívoco respecto a los delitos informáticos, ni existe una norma en Argentina que establezca algún punto de partida para aceptar o criticar jurídicamente su significado, pero internacionalmente se han propuesto diferentes definiciones de éstos.

En un principio, se puede definir al delito informático como aquella actividad ilegal encuadrada en las figuras tradicionales y que se configura al utilizar ilegalmente un medio electrónico o digital. Esto quiere decir que, es un requisito esencial que el medio para cometer la ilegalidad sea la informática.[4] Éstos ilícitos deben ser relativos a la intimidad, la libertad, la integridad sexual, entre otros.

La **Organización de Naciones Unidas** (ONU) establece que los delitos informáticos se configuran con la utilización de una computadora, pero este criterio ha quedado desactualizado ya que, la tecnología ha avanzado y se han creado otras herramientas informáticas que pueden llegar a ser más idóneas que una computadora.

En el año 1983 la **Organización de Cooperación y Desarrollo Económico** definió a los delitos informático como *"cualquier comportamiento antijurídico, no ético o no autorizado, relacionado con el procesado automático de datos y/o transmisiones de datos."*

Y, para cerrar la idea, Miguel Á. Davara Rodríguez determina que el crimen cibernético es *"la realización de una acción que, reuniendo las características que delimitan el concepto de delito, sea llevada a cabo utilizando un elemento informático y/o telemático, o vulnerando los derechos del titular de un elemento informático, ya sea hardware o software", "nos estamos refiriendo solamente, a la comisión de un delito por medios informáticos o telemáticos, ya que la comisión de*

[4] Sorbo, H. D. "*Delitos Informáticos - Aspectos a tener en cuenta de la Ley 26.388"*, 2013. Disponible en: http://server1.utsupra.com/doctrina1?ID=articulos_utsupra_02A00376672921

otros delitos en los que alguna forma interviene un elemento informático, se encontrará sin duda dentro del Derecho Penal General".

Estafas y otras defraudaciones

El legislador ha optado por no realizar una definición de la estafa, sino que ha decidido mencionar las diferentes formas que resultan punibles. Sin embargo, del texto legal se puede entender que el delito consiste de una defraudación causada mediante ardid o engaño.

Antón Oneca define a la **estafa** como *"la conducta engañosa, con ánimo de lucro injusto, propio o ajeno, que determinando un error en una o varias personas las induce a realizar un acto de disposición, consecuencia del cual es un perjuicio en su patrimonio o en el de un tercero."*.

Estafa informática

Es la producción de un daño patrimonial cuantificable mediante un comportamiento externo, impropio de un proceso automatizado informático, que altera los datos gestionados por éste, con ánimo lucro y en perjuicio de un tercero.

Manipulación informática

Es cualquier modificación del resultado de un proceso automatizado de datos que se produzca a través de la introducción de nuevos datos, de la alteración de los existentes en el computador, en cualquier de las fases de su procesamiento o tratamiento informático.

Principio jurídico

Los principios jurídicos son esencias contenidas en las normas jurídicas (escritas o no escritas, como la costumbre y la jurisprudencia). Son las "ideas fundamentales" o básicas del Derecho, que lo definen y explican ontológicamente. Determinan la unidad de sentido, la conexión sistemática y material del sistema normativo.[5] [6]

Principio de legalidad

El principio de legalidad es conocido universalmente por el apotegma "*nullum crimen, nulla poena sine praevia lege poenali"* **-no hay delito, no hay pena,**

[5] Beladiez R., M. *"Los Principios Jurídicos*", Tecnos, 1° edición, Madrid, 1994, pág. 17.
[6] Cassagne, J. C. "*Los Principios Generales del Derecho*", Abeledo-Perrot, Buenos Aires, 1992, págs. 29 y 30

sin ley penal previa-, donde el autor pone de relieve el rol funcional que cumple la ley, para la determinación de la infracción punible y de la sanción penal.[7]

El Diccionario Panhispánico del Español Jurídico lo define como el principio jurídico según el cual no puede castigarse una acción u omisión si no está prevista como delito en una ley y que prohíbe el cumplimiento de las penas y de las medidas de seguridad en forma distinta de la prevista por la ley.

Tecnología

El término tecnología tiene origen griego (*tekne logos)* que hace referencia al conocimiento o ciencia del arte, técnica u oficio. Así pues, la tecnología es el conjunto de conocimientos, métodos y procedimientos orientados hacia la producción de bienes y servicios que satisfacen determinadas necesidades humanas[8].

Para llevarla a cabo se requiere de la aplicación de leyes y principios científicos, ya que la tecnología tiene sus fundamentos en la ciencia.

Informática

La palabra **informática** es un neologismo derivado de los vocablos información y automatización, sugerido por Phillipe Dreyfus en 1962. En sentido general, podemos considerar que la informática es un conjunto de técnicas destinadas al tratamiento lógico y automatizado de la información con miras a una adecuada toma de decisiones.[9]

Sistemas informáticos

Es un conjunto integrado de procesos, principalmente formales, desarrollados en un entorno usuario-computador que […] recopilan, procesan y distribuyen selectivamente la información necesaria para la operatividad habitual.[10]

También puede entenderse como un conjunto de componentes interrelacionados que recuperan, procesan, almacenan y distribuyen información para soportar la toma de decisiones, la coordinación y el control de una organización.[11]

---

[7] López Pérez, Luis. *"El Principio de Legalidad Penal"*, 2021. Disponible en: https://www.studocu.com/pe/document/universidad-cesar-vallejo/derecho-penal-i/principio-de-legalidad/14313160

[8] Cruz R., J. E. "*El Avance Tecnológico"*, 2009. Disponible en: http://www.rvcmar.org/otros/mapasc/JCR_EL_AVANCE_TECNOLoGICO.pdf

[9] Telléz V., J. "*Derecho Informático"*, Mc Graw Hill, 4° edición, México, 1987, pág. 6.

[10] Andreu, R.; Ricart, J. y Valor, J. "*Estrategia y Sistemas de Información"*, Editorial McGraw-Hill, Barcelona, 1991.

En lo particular, el Dr. Figari analizó estas cuestiones respecto a las defraudaciones informáticas y la inconstitucionalidad en su obra denominada "*Reflexiones sobre la defraudación informática ley 26.388*". Donna lo analizó a través de su libro *"Derecho Penal. Parte Especial. Tomo II-B"*. Pablo Palazzi también se dedicó a ello en su trabajo *"Los delitos informáticos en el Código Penal. Análisis de la ley 26.388".*

[11] Laudon, K. C.; Laudon, J. P. "*Sistemas de Información Gerencial"*, Editorial Pearson, ISBN: 978-607-32-0949-6, México, 1996, pág. 15.

Capítulo I

SISTEMAS INFORMÁTICOS Y LA TRANSMISIÓN DE DATOS

Sumario: definición, historia y evolución, el internet y el ciberespacio, avance de la ciberdelincuencia.

I. Sistemas informáticos

El prodigioso avance de la informática y la masiva implantación de los sistemas informáticos en todos los sectores de la sociedad abrió paso a una nueva etapa histórica con unas consecuencias todavía imprevisibles.[12]

Durante los últimos años los sistemas de información constituyeron uno de los principales medios para cometer el delito de ciber defraudación. Más aún a partir de la pandemia que se decretó en marzo del año 2020, ya que las sociedades debieron adaptarse a una nueva realidad que exigía que permaneciéramos en nuestros hogares y realicemos nuestras actividades diarias mediante la virtualidad.

El advenimiento de Internet y los sistemas informáticos significó un "antes" y un "después" del acceso al sistema de información, donde cada acción se reflejaba, siendo la web el nuevo espacio en el que se construyen, desarrollan y modifican los roles de diferentes agentes.

Un sistema de información, en sentido estricto, es *"un conjunto integrado de procesos, principalmente formales, desarrollados en un entorno usuario-computador que […] recopilan, procesan y distribuyen selectivamente la información necesaria para la operatividad habitual."*[13]

También puede entenderse como *"un conjunto de componentes interrelacionados que recuperan, procesan, almacenan y distribuyen información para soportar la toma de decisiones, la coordinación y el control de una organización."* [14]

El Convenio de Budapest en su artículo 1 define al sistema informático como *"todo dispositivo aislado o conjunto de dispositivos interconectados o relacionados entre sí, cuya función, o la de alguno de sus elementos, sea el tratamiento automatizado de datos en ejecución de un programa".*[15]

Según Arocena, es todo dispositivo o grupo de elementos relacionados que, conforme o no a un programa, realiza el tratamiento automatizado de datos, que

---

[12] Sanz L., F. J. "*El Derecho Ante las Nuevas Tecnologías de la Información",* 1997, pág. 501. Disponible en: https://ruc.udc.es/dspace/bitstream/handle/2183/1934/AD-1-26.pdf

[13] Andreu, R.; Ricart, J. y Valor, J. "*Estrategia y Sistemas de Información"*, Editorial McGraw-Hill, Barcelona, 1991.

[14] Laudon, K. C.; Laudon, J. P. "*Sistemas de Información Gerencial"*, Editorial Pearson, ISBN: 978-607-32-0949-6, México, 1996, pág. 15.

[15] Convenio de Budapest. Capítulo I, "Terminología", art. 1 inc. A.

implica generar, enviar, recibir, procesar o almacenar información de cualquier forma y por cualquier medio.[16]

Todo sistema de información utiliza como materia prima los datos, los cuales almacena, procesa y transforma para obtener como resultado final información, la cual será suministrada a los diferentes usuarios del sistema.[17]

Estos datos informáticos, según el Convenio, será *"toda representación de hechos, información o conceptos expresados de cualquier forma que se preste a tratamiento informático, incluidos los programas diseñados para que un sistema informático ejecute una función".*[18]

La resolución 476/01 de la Secretaría de Comunicación de la Nación los entiende al sistema informático como *"todo dispositivo o grupo de elementos relacionados que, conforme o no a un programa, realiza el tratamiento automatizado de datos, que implica generar, enviar, recibir, procesar o almacenar información de cualquier forma y por cualquier medio."* Por su parte, la transmisión de datos -informáticos- *"son toda representación de hechos, manifestaciones o concepto en un formato que puede ser tratado por un sistema informático.*[19]

Este dispositivo o grupo de dispositivos ha de servir para el tratamiento automatizado de datos.

El tratamiento de la información es "automatizada" cuando se emplean para ello, no ya personas físicas, sino dispositivos mecánicos o electrónicos. Es claro que la computadora es operada por un ser humano, pero el tratamiento de los datos, en sí mismo, es llevado a cabo por tales dispositivos tecnológicos.[20]

---

[16] Arocena, G. A. *"La Regulación de los Delitos Informáticos en el Código Penal Argentino. Introducción a la Ley Nacional N° 26.388",* Boletín mexicano de derecho comparado, 45(135), 2011, 945-988. Disponible en: http://www.scielo.org.mx/scielo.php?script=sci_arttext&pid=S0041-86332012000300002&lng=es&tlng=es

[17] Hernández T., A. "*Los Sistemas de Información: Evolución y Desarrollo",* Proyecto social: Revista de Relaciones Laborales, ISSN 1133-3189, N.º 10-11, 2003, págs. 149-165. Disponible en: https://dialnet.unirioja.es/servlet/articulo?codigo=793097

[18] Convenio de Budapest. Capítulo I, "Terminología", art. 1 inc. B.

[19] Migliorisi, D. "*Crímenes en la Web: los delitos del siglo XXI"*, Editorial: Del Nuevo Extremo, ISBN 978-987-609-611-9, Ciudad Autónoma de Buenos Aires, 2014, pág. 119.

[20] Arocena, G. A. *"La Regulación de los Delitos Informáticos en el Código Penal Argentino. Introducción a la Ley Nacional N° 26.388",* Boletín mexicano de derecho comparado, 45(135), 2011, 945-988. Disponible en: http://www.scielo.org.mx/scielo.php?script=sci_arttext&pid=S0041-86332012000300002&lng=es&tlng=es

Para que estos sistemas puedan cumplir con su finalidad se requiere que exista una serie de elementos que estar interrelacionados entre sí: el componente físico (*hardware)*, el componente lógico (*software)* y el componente humano (usuario).

El *hardware* es el conjunto de elementos físicos o materiales que constituyen una computadora o un sistema informático, por ejemplo, pantallas, teclados, microprocesador, entre otros. Por otro lado, el *software* es el conjunto de programas y algoritmos que se utiliza para realizar determinadas tareas, como lo es Windows, IOS o Android. Y, por último, el factor humano son aquellos usuarios de diversa índole que intervienen en una red informática, que usan un sistema informático o que lo programan[21].

Además, existe otro elemento completamente necesario para que los sistemas informáticos puedan alcanzar su propósito: *internet*.

Las características intrínsecas de Internet posibilita múltiples consecuencias positivas (interconexión virtual, eliminación de barreras de espacio y tiempo, económicamente accesible, la posibilidad del anonimato, acceso a contenidos ilimitados de cualquier lugar en el mundo, etc.) pero también acarrea como contracara aspectos negativos entre los que se encuentran los delitos informáticos y los inconvenientes para la persecución de dichas actividades apoyados en algunas de las mencionadas ventajas.[22]

II. Historia y evolución de los ordenadores

En primer lugar, es importante aclarar que se realizará un desarrollo escueto con respecto a los ordenadores, ya que ellos son el primer instrumento mediante el cual se procesa automáticamente la información, por lo tanto, son un sistema informático.

Ahora bien, el ser humano siempre necesitó de medios para procesar información. Evidentemente, la sociedad fue avanzando y provocó que la complejidad de los sistemas informáticos incrementara con el tiempo, ya que debían ajustarse a las nuevas necesidades y al progreso de la tecnología. [23]

[21]Uriarte, J. M. "*Sistema Informático"*. Para Características.co, 2020. Disponible en: https://www.caracteristicas.co/sistema-informatico/

[22] Vaninetti, H. A. "*Estafa en internet. Transferencia electrónica de fondos. Operatoria de home banking. La competencia en los delitos informáticos*", revista jurídica La Ley N.º 2017 a, 2017.

[23] Barzanallana, R. *"Historia de la informática. Introducción a la informática"*, Universidad de Murcia, Murcia, 2013. Disponible en: https://www.um.es/docencia/barzana/II/Ii04.html

El nacimiento del procesamiento automático de la información fue en el año 1896 con la fundación de la empresa de Herman Hollerith, "*Tabuling Machine co.*", la cual, posteriormente, Thomas Watson la convertiría en *"International Bussines Machines"* (IBM).

Hollerith fue la primera persona en construir una máquina con el objetivo de tratar de manera automatizada la información. Él trabajaba en una oficina de censo en Estados Unidos y que el procesamiento de los datos del año 1880 no había terminado al momento de hacer el del año 1890.

Para ello, Herman diseñó una tarjeta que debía perforar con los datos de cada uno de los encuestados y, luego, debían introducirse en una lectura que detectaba aquellas perforaciones mediante un baño de mercurio que, al introducirse por los agujeros, provocaba contactos eléctricos. Finalmente, los datos se registraban en una tabuladora. Con este invento, Hollerith provocó que la velocidad de proceso se multiplique por 100, es decir, 200 fichas por minuto.[24]

Los tabuladores de Hollerith fueron una de tantas respuestas, pero hubo otras, como las máquinas eléctricas de contabilidad, las cajas registradoras, las máquinas de sumar mecánicas, la conmutación automática y los mecanismos de control para los ferrocarriles, las centrales telefónicas y telegráficas junto con los sistemas de información para los mercados internacionales de valores y materias primas.[25]

Los primeros ordenadores datan a partir de los años 1900, los denominados "Ordenadores de Primera Generación". Éstos utilizaban tubos al vacío y se caracterizaban por su enorme tamaño y no contar con un sistema operativo, sino que tenían una tarjeta perforada -como la de la *Tabuling Machine co*. - que almacenaban toda la información.[26]

La primera generación de ordenadores era utilizada exclusivamente por las fuerzas militares y la industria científica. Dentro de ellas podemos nombrar a la *"UNIVAC"*, *"ENICAC"* o la *"EDSAC"*.

---

[24] Barzanallana, R. *"Historia de la informática. Introducción a la informática"*, Universidad de Murcia, Murcia, 2013. Disponible en: https://www.um.es/docencia/barzana/II/Ii04.html

[25] Ceruzzi, P. E. *"Historia de la informática",* Fronteras del conocimiento, Madrid, 2010, pág. 110 Disponible en: https://www.bbvaopenmind.com/wp-content/uploads/2009/01/BBVA-OpenMind-Fronteras_del_conocimiento.pdf

[26] Next U, Tecnología de la Información, Disponible en: https://www.nextu.com/blog/generaciones-de-las-computadoras/

Durante la segunda generación de ordenadores se sustituyeron las válvulas de vacío por transistores, se implementó el uso de memorias de núcleo de ferritas y tambores magnéticos para el almacenamiento de información. Estas computadoras eran de menor tamaño, pero tenían mayor potencia, rapidez y fiabilidad. La "*IBM 1401"* y la *"IBM 1620"* fueron computadoras de segunda generación.

También aparecieron lenguajes de programación: *"COBOL", "ALGOL", "FORTRAN"*, entre otros.

En el año 1964 se inventó el circuito cerrado o chip, lo que generó una revolución en el diseño de las computadoras y dio lugar a la tercera generación de las mismas. En esta época aparecieron los primeros discos magnéticos y los componentes electrónicos se integraban en una sola pieza o chip que albergaban en su interior condensadores, transistores y diodos, lo que hacía que se aumente la velocidad de carga y reducir el consumo de energía eléctrica.[27] La *"CDC 6600"*, la *"IBM 360"* y la *"IBM 370"* son ejemplos de éstas.

A su vez, surgieron la multiprogramación y el tiempo compartido, y se dio la crisis del software[28].

Como se puede deducir, todos los sistemas informáticos desarrollados hasta ahora, se utilizaban solamente para realizar, principalmente, cálculos. Por lo que, la profundización de los ordenadores y sistemas informáticos anteriormente desarrollados, no es lo que en realidad concierne, empero es importante realizar una pequeña reseña sobre ellos para poder entender de dónde surgen los sistemas informáticos actuales.

A partir del 1971, los elementos que conformaban a la CPU se almacenarán en un circuito integrado: el microprocesador. Además, la compañía Intel comenzó a fabricar microprocesadores de una gran gama, siendo el primero de éstos el denominado "4004".

La empresa Microsoft creó el sistema operativo *"MS-DOS"* para la computadora. Esta serie de sucesos provocó la aparición de la cuarta generación de ordenadores.

[27] Next U, Tecnología de la Información. Disponible en: https://www.nextu.com/blog/generaciones-de-las-computadoras/

[28] La crisis del software son los problemas que se presentaron durante el desarrollo del software especialmente fue marcada por los excesos de costos, la escasa fiabilidad, la insatisfacción de los usuarios y los horarios de tiempos.

En 1977 Steve Jobs y Steve Wozniak se unieron para crear un ordenador llamado "*Apple II"*, la cual permitió que la informática no sea exclusivamente de las empresas y que las personas del mundo puedan acceder a ella. Ante esto, IBM sacó al mercado su propia computadora años después. Ésta hacía posible a otras empresas suministrar software, equipo periférico, tarjetas de circuitos conectables. Tenía un procesador avanzado de 8 bits suministrado por Intel, el "8088", que le permitía tener acceso a mucha más memoria que la *"Apple II"* y utilizaba el sistema operativo de Microsoft.[29]

A fines del año 1981, en Japón se anunció que se iniciará una investigación y desarrollo para lograr la producción de una nueva generación de ordenadores -la quinta-. Estos ordenadores tenían que ser capaces de resolver problemas muy complicados, de trabajar con grandes subconjuntos de los lenguajes de programación y debían permitir el manejo de personas no expertas en el área informática. Evidentemente, esto significaba una tecnología mucho más avanzada, los lenguajes eran más complejos para las computadoras, pero sencillos para las personas.

Esta generación empezó a cumplir con tareas que todavía existen, por ejemplo, la traducción de un idioma a otro o almacenar información digital en gigabytes. Para alcanzar estos objetivos -y otros-, estos equipos contaban con tres subsistemas fundamentales: un sistema inteligente, un mecanismo de interferencia y una interfaz de usuario inteligente.[30]

La última generación de computadoras, la sexta, es la que hoy todavía tenemos. Cabe aclarar que, hay quienes creen que no existe una sexta generación, pero en este trabajo consideramos que sí la hay, ya que la informática ha avanzado de manera muy abrupta y veloz, por lo que los ordenadores de la quinta y sexta generación son muy diferentes entre sí.

La inteligencia artificial, la arquitectura vectorial y paralela de los ordenadores, la incorporación de chips de procesadores especializados para llevar a cabo ciertas tareas, los dispositivos móviles predominan en la actualidad.[31]

---

[29] Ceruzzi, P. E. *"Historia de la informática",* Fronteras del conocimiento, Madrid, 2010, pág. 110 Disponible en: https://www.bbvaopenmind.com/wp-content/uploads/2009/01/BBVA-OpenMind-Fronteras_del_conocimiento.pdf

[30] Barzanallana, R. *"Historia de la informática. Introducción a la informática"*, Universidad de Murcia, Murcia, 2013. Disponible en: https://www.um.es/docencia/barzana/II/Ii04.html

[31] Next U, Tecnología de la Información. Disponible en: https://www.nextu.com/blog/generaciones-de-las-computadoras/

III. El Internet y el ciberespacio

La Real Academia Española (R.A.E.) define al internet como:

"Red informática mundial, descentralizada, formada por la conexión directa entre computadoras mediante un protocolo especial de comunicación."[32]

Podría explicarse como *"**una red global de redes de ordenadores cuya finalidad es permitir el intercambio libre de información entre todos los usuarios**".*[33] Cuando decimos "red" queremos decir que, entre sus componentes existe una interconexión, esto significaría que desde cualquier punto de la red se podría llegar a otro.[34] Básicamente es un conjunto de dos o más equipos conectados entre sí.

Para que esa interconexión sea global, todas las redes que se conectan a internet deben hacerlo a través de un mismo protocolo de comunicación, lo que permitirá que la conexión sea desde cualquier origen hasta cualquier destino.

Pero esto no es tan sencillo, podría ser un error considerar que el internet únicamente es como una red de ordenadores, ya que es mucho más amplio que eso. Hoy en día existen otros dispositivos, además de las computadoras, que operan a través de internet: los teléfonos inteligentes y las tabletas, por ejemplo.

Hay personas que creen que el internet ha incentivado la democratización, ya que permite el acceso a una gran cantidad de datos a un costo bajo.[35]

El origen del internet data en el año 1973, donde se creó un método de conexión de redes que se llamó *"Ethernet"*, el que permitió conectar ordenadores que se encontraban en un mismo lugar físico entre sí y con ello compartir la memoria de masa e intercambiar mensajes por el correo electrónico.[36]

La Agencia de Proyectos de Investigación Avanzada en Defensa intentaba conectar ordenadores que no se encontraban en el mismo espacio, sino que estaban

---

[32] Real Academia Española. https://dle.rae.es/internet?m=form
[33] Pacheco J., Universidad Jaume I. Disponible en: https://www3.uji.es/~pacheco/INTERN~1.html
[34] NIC Argentina. Disponible en: https://nic.ar/es/enterate/novedades/que-es-internet
[35] Glosario digital de Arimetrics. Disponible en: https://www.arimetrics.com/glosario-digital/internet
[36] Ceruzzi, P. E. *"Historia de la informática",* Fronteras del conocimiento, Madrid, 2010, pág. 110 Disponible en: https://www.bbvaopenmind.com/wp-content/uploads/2009/01/BBVA-OpenMind-Fronteras_del_conocimiento.pdf

dispersos geográficamente. Puesto que, pretendían que las comunicaciones militares se mantuvieran seguras en caso de guerra.[37]

Sin dudas, el Internet es la invención más importante del último tiempo. Su creación permitió desarrollos tecnológicos que transforman la forma en que las personas viven y se relacionan. Y, aunque esto parezca positivo en su totalidad, también generó que ciertas personas lo utilicen para causar daños a otros, ocasionando consecuencias extremadamente lesivas al patrimonio, a la dignidad, el honor -entre otros- de las víctimas.

Hoy en día, todas las sociedades y los ciudadanos que la componen dependen casi por completo del internet y los sistemas informáticos para la ejecución de todos los procesos económicos y sociales que, además, están estrechamente interconectados. El rápido y vertiginoso desarrollo de la tecnología de la información ha allanado el camino para la delincuencia, poniendo "armas pesadas" en manos de delincuentes y terroristas.

El *Ciberespacio* es, según Curtis[38], un dominio artificial construido por el hombre, diferenciado de los otros cuatros dominios de guerra (tierra, aire, mar y espacio). Aunque se haya formalizado recientemente, el ciberespacio puede afectar a las actividades en los otros dominios y viceversa. Además, el ciberespacio no está aislado sino profundamente vinculado y apoyado por medios físicos, por ejemplo, las redes eléctricas.[39]

La página del Gobierno argentino lo entiende como *"un área intangible a la que cualquier persona puede acceder con un ordenador desde su hogar, su lugar de trabajo o dispositivos móviles"*[40].

El ciberespacio es el espacio virtual creado por las redes informáticas. Algo que es inmaterial, podría decirse que un concepto para ubicar cosas almacenadas en objetos intangibles. De acá es donde surge el primer vínculo entre el ciberespacio e

---

[37] Ceruzzi, P. E. *"Historia de la informática",* Fronteras del conocimiento, Madrid, 2010, pág. 110 Disponible en: https://www.bbvaopenmind.com/wp-content/uploads/2009/01/BBVA-OpenMind-Fronteras_del_conocimiento.pdf

[38] Curtis E., L. "*Introduction to cyberspaceoperations",* 2011.

[39] Pons G., V. "*Internet, la nueva era del delito: ciberdelito, ciberterrorismo, legislación y ciberseguridad"*. URVIO, Revista Latinoamericana de Estudios de Seguridad, Vol. núm.20, ISSN: 1390-3691, 2017, págs. 80-93. Disponible en: https://www.redalyc.org/articulo.oa?id=552656641007

[40] Página Oficial del Gobierno argentino. Disponible en: https://www.argentina.gob.ar/justicia/convosenlaweb/situaciones/que-es-el-ciberdelito#:~:text=Los%20ciberdelitos%20que%20se%20cometen,fines%20econ%C3%B3micos%20y%20de%20da%C3%B1o.

Internet. A pesar de que exista una fuerte relación entre estos dos, son términos totalmente diferentes.

El internet es un conjunto descentralizado de redes de comunicación a través de protocolos, mientras que el ciberespacio es el lugar en el que se producen las comunicaciones de internet.[41] Por ejemplo, cuando hablamos de *hacking*, este ataque no tiene lugar en un espacio físico en particular, sino en el ciberespacio. No obstante, las decisiones que se toman en el internet tienen un impacto directo en la vida real.

Todo lo anteriormente expuesto, le concede al ciberdelincuente varios beneficios: le permite estar seguro porque no se expone físicamente a su víctima ni a la posible intervención de las fuerzas de seguridad, dado que su acción se realiza desde cualquier parte del mundo; le proporciona al ciberatacante una sensación de cómoda impunidad porque existen vacíos legales a nivel internacional y, por lo tanto, hay muchos delitos que todavía no se castigan; le da la posibilidad de aprovechar el anonimato y, por ello, se torna dificultoso poder identificarlo.[42]

El flujo instantáneo de información y la multitud de interacciones sociales en Internet presentan complejidad y amenaza para los usuarios debido al aumento de los delitos cibernéticos a nivel mundial.

IV. Avance de la ciberdelincuencia

El delito cibernético se está convirtiendo cada vez más en un fenómeno recurrente y en un método delictivo basado en tecnología altamente sofisticado.

Es una de las formas de delincuencia más activas e importantes del mundo. Después de todo, internet es accesible y visible para todos, y esto, por supuesto, conlleva riesgos. Cometer un delito utilizando una computadora u otro dispositivo conectado a internet es muy peligroso porque la identidad del perpetrador es difícil de establecer.

El desarrollo de las nuevas tecnologías ha fomentado y posibilitado delitos que existían en el pasado, como la estafa o el fraude, pero que ahora se realizan de otra forma: utilizando o explotando la existencia de sistemas informáticos. El hecho es que internet se ha convertido en un avance asombroso en el complejo mundo de la

[41] Blog de LINUBE. Disponible en: https://linube.com/blog/ciberespacio-no-es-internet/
[42] Pons G., V. "*Internet, la nueva era del delito: ciberdelito, ciberterrorismo, legislación y ciberseguridad"*. URVIO, Revista Latinoamericana de Estudios de Seguridad, Vol. núm.20, ISSN: 1390-3691, 2017, págs. 80-93. Disponible en: https://www.redalyc.org/articulo.oa?id=552656641007

tecnología, al mismo tiempo que se ha convertido en una nueva herramienta para el crimen.

Los primeros casos de la delincuencia cibernética se cometieron antes de que internet llegara a existir. En 1834 un grupo de jóvenes hackearon el sistema de telégrafos francés para robar información del mercado financiero. Este fue el primer ciberataque que se llevó a cabo de manera efectiva en el mundo.

Sin embargo, éste no es considerado el origen de la ciberdelincuencia. El gran ataque a una red telefónica es el que se toma como punto de referencia en la evolución de los ciberdelitos, aunque precedentemente se hubiesen cometidos otros.

A inicios de la década del ’70, los delitos se cometían, usualmente, a través de líneas telefónicas y los delincuentes se asignaron el nombre de *“phreakers”*. John Draper era uno de ellos y descubrió que un silbido -que fue premio de las cajas de Cap’n Crunch- producía los mismos tonos que el sistema telefónico en Estados Unidos. Consecuentemente, creó una “caja azul” para imitar esos tonos que le permitían hacer llamadas de larga distancia gratuitas y luego publicó instrucciones sobre cómo hacerlo. Los casos de frade telefónico aumentaron significativamente.[43] [44]

En el año 1981 se condenó por primera vez a una persona por la comisión de un delito informático: Ian Murphy, quien hackeó la red de AT&T, una compañía telefónica estadounidense, para manipular el reloj interno y que sus clientes pudiesen llamar de manera gratuita en horas pico. Su condena fue realizar el servicio comunitario durante mil horas y 2 años y medio de libertad condicional.

Años después, en 1988, Robert Morris desarrolló al primer gusano auto replicante de internet. Este ataque provocó que más de 600.000 computadoras se infecten y reinfecten a un ritmo muchísimo más rápido de lo esperado. El creador del gusano fue sentenciado a pagar una multa de $10.000 y a tres años de libertad condicional.

A finales de la década del 90, se registró el primer caso de *ransomware* a gran escala. Este es un tipo de malware que impide a los usuarios acceder a su sistema o a sus archivos personales y que exige el pago de un rescate para poder acceder de nuevo a ellos. Lo que sucedió en 1989 fue que se presentó un cuestionario sobre el sida que,

[43] Observatorio Guatemalteco de Delitos Informáticos. Disponible en: https://ogdi.org/historia-del-cibercrimen

[44] Rinaldi, P. *“¿De dónde viene el delito cibernético? Origen y evolución del delito cibernético”,* Le VPN, 2017. Disponible en: https://www.le-vpn.com/es/delito-cibernetico-origen-evolucion/

una vez que era descargado por los usuarios, mantenía los datos informáticos como rehenes por $500.

Con posterioridad, hubo más ciberdelitos pero que no eran tan relevantes, hasta que en el año 1999 se produjo el lanzamiento del virus "Melissa", el cual se convirtió en la infección informática más agresiva hasta la actualidad. Melissa era un *macrovirus* que infectó los documentos de Microsoft Word y se diseminó automáticamente como un archivo adjunto por correo electrónico, básicamente se apoderaba de cuentas de correos y enviaba mails masivos. Este virus causó más de 80 millones de dólares de daños a las redes informáticas.

A partir de aquí, los ataques en el internet aumentaron bruscamente. Los ciberdelincuentes se adaptaban a las nuevas tecnologías para consumar sus crímenes; denegaron los servicios de Yahoo!, EBay; se emitieron noticias falsas; se propagó el virus *"I love you"*; el correo electrónico tenía una seguridad precaria; se creó el gusano de proliferación más rápido de la historia: el *SQL SLAMMER;* los casos de hackeo, robo de datos e infecciones de malware se dispararon; phishing, piratería informática, spam y otros fraudes, entre otros.[45]

La ciberdelincuencia crece a un ritmo muy acelerado, con nuevas tendencias emergiendo continuamente. Los ciberdelincuentes se están volviendo más ágiles, explotan las nuevas tecnologías a una velocidad de vértigo, adaptan sus ataques utilizando nuevos métodos y cooperan entre sí de manera nunca vista hasta ahora. Las redes delictivas operan a escala planetaria, coordinando ataques complejos contra sus objetivos en cuestión de minutos.[46]

Pese a que varios de estos ataques -que ya se encuentran tipificados por nuestro Código Penal- siguen llevándose a cabo al día de hoy, durante la pandemia decretada en el 2020 se incrementaron exponencialmente, sobre todo, las estafas y defraudaciones informáticas.

[45] Rinaldi, P. *"¿De dónde viene el delito cibernético? Origen y evolución del delito cibernético",* Le VPN, 2017. Disponible en: https://www.le-vpn.com/es/delito-cibernetico-origen-evolucion/
[46] INTERPOL. Disponible en: https://www.interpol.int/es/Delitos/Ciberdelincuencia

Capítulo II

DELITOS INFORMÁTICOS Y LAS NORMAS CONVENCIONALES

Sumario: delitos informáticos, características, clasificación, Convenio de Budapest, Ley Nacional de Delitos Informáticos N° 26.388.

I. Delitos informáticos

El delito informático cobra vida a partir del avance creciente de las Tecnologías de la Informática y las Comunicaciones (TIC) y el acceso e incorrecto uso de las mismas. Inicialmente, los países pretendieron encuadrar estas actividades criminales dentro de figuras tradicionales reguladas convencionalmente en los ordenamientos penales, respectivo a cada uno de ellos. Sin embargo, la utilización de las TIC ha creado nuevas posibilidades de manejo indebido de las mismas, dando lugar a conductas delictivas que por sus particularidades no encuentran precedente dentro las regulaciones preexistentes y cuyas consecuencias llegan alcanzar altos niveles de nocividad que requieren una urgente regulación por parte del Derecho Penal.[47]

En la actualidad, la relación entre las redes de comunicación y los sistemas informático con las sociedades es cada vez mayor, esto genera que ciudadanos de distintas partes del mundo se encuentren conectados sin importar la distancia que los separe. Si bien esto significa la existencia de una enorme cantidad de beneficios, es cierto que también existe el aspecto negativo.

Las redes de comunicación y los sistemas informáticos también pueden ser utilizados para realizar actos delictivos. Estos actos delictivos son los **delitos informáticos** y pueden ser cometidos de diferentes maneras y de distintas partes del mundo.

I. a) Definición

La doctrina todavía no ha encontrado un concepto unívoco respecto a los delitos informáticos, ni existe una norma en Argentina que establezca algún punto de partida para aceptar o criticar jurídicamente su significado, pero internacionalmente se han propuesto diferentes definiciones de los mismos

En un principio, se puede definir al delito informático como aquella actividad ilegal encuadrada en las figuras tradicionales y que se configura al utilizar ilegalmente un medio electrónico o digital. Esto quiere decir que, es un requisito esencial que el medio para cometer la ilegalidad sea la informática.[48] Éstos ilícitos

[47] Garzón T., P. N. y Gallardo V., M. F. *"Fraude informático: valoraciones técnico-jurídicas"*. Tesis de Grado, Universidad Técnica de Cotopaxi, 2009. Disponible en: http://repositorio.utc.edu.ec/bitstream/27000/139/1/T-UTC-0066.pdf

[48] Sorbo, H. D. "*Delitos Informáticos - Aspectos a tener en cuenta de la Ley 26.388"*, 2013. Disponible en: http://server1.utsupra.com/doctrina1?ID=articulos_utsupra_02A00376672921

deben ser relativos a la propiedad, intimidad, la libertad, la integridad sexual, entre otros.

Afirmando esto, Téllez Valdés sostiene que *"dar un concepto acerca de delitos informáticos no es labor fácil, ya que su denominación alude a una situación muy especial porque para hablar de "delitos" en el sentido de acciones típicas (o tipificadas), es decir, contempladas en textos jurídico-penales, se requiere que la expresión delitos informáticos esté consignada en los códigos penales, lo cual en algunos países no ha sido objeto de tipificación*." [49]

Por su lado, el autor considera que se debe establecer la diferencia entre lo típico y lo atípico. Para él, el concepto atípico es *"actitudes ilícitas que tienen a las computadoras como instrumento o fin"* y el concepto típico son *"conductas típicas, antijurídicas y culpables que tienen a las computadoras como instrumento o fin."*[50]

Según Alexander Díaz García los delitos informáticos deben ser observados desde **un punto de vista triple**, esto es, *"**como fin en sí mismo**, pues el computador puede ser objeto de la ofensa, al manipular o dañar la información que éste pudiera contener; **como medio**, es decir, como herramienta del delito, cuando el sujeto activo utiliza el ordenador para facilitar la comisión de un delito tradicional, y **como objeto de prueba**, ya que las computadores guardan pruebas incidentales de la comisión de ciertos actos delictivos a través de ellos."*

La **Organización de Naciones Unidas** (ONU) establece que los delitos informáticos se configuran con la utilización de una computadora, pero este criterio ha quedado desactualizado ya que, la tecnología ha avanzado y se han creado otras herramientas informáticas que pueden llegar a ser más idóneas que una computadora.

En el año 1983 la **Organización de Cooperación y Desarrollo Económico** definió a los delitos informático como *"cualquier comportamiento antijurídico, no ético o no autorizado, relacionado con el procesado automático de datos y/o transmisiones de datos."*

Miguel Á. Davara Rodríguez determina que el crimen cibernético es *"la realización de una acción que, reuniendo las características que delimitan el concepto de delito, sea llevada a cabo utilizando un elemento informático y/o telemático, o vulnerando los derechos del titular de un elemento informático, ya sea hardware o*

[49] Telléz V., J. "*Derecho Informático"*, Mc Graw Hill, 4° edición, México, 1987, págs. 188, 189
[50] Telléz V., J. "*Derecho Informático"*, Mc Graw Hill, 4° edición, México, 1987, pág. 189

software", "nos estamos refiriendo solamente, a la comisión de un delito por medios informáticos o telemáticos, ya que la comisión de otros delitos en los que alguna forma interviene un elemento informático, se encontrará sin duda dentro del Derecho Penal General".

El delito informático es "*el injusto determinado en sus elementos por el tipo de la ley penal, conminado con pena y por el que el autor merece un reproche de culpabilidad, que, utilizando a los sistemas informáticos como medio comisivo o teniendo a aquéllos, en parte o en todo, como su objeto, se vinculan con el tratamiento automático de datos*."[51]

De esta concepción podemos deducir que el concepto de ciberdelito se construye en derredor de la noción de **"sistema informático"**, es éste el que se constituye en el **instrumento del delito o su objeto de ataque**, o sea, el medio a través del cual el ilícito se comete, o en el objeto material sobre el cual recae la conducta típica.[52]

Según Callegari el delito informático es *"aquel que se da con la ayuda de la informática o de técnicas anexas"*.[53] Por su parte, Sain y Azzolin los entienden como dichas *"conductas indebidas e ilegales donde interviene un dispositivo informático como medio para cometer un delito o como fin u objeto del mismo"*[54]

De esta última se aprecia que las tecnologías son utilizadas o como medio para cometer el delito o como fin. En la primera situación, una persona- por ejemplo- utiliza un dispositivo informático como medio para ejecutar la acción ilegal: una estafa. En el segundo caso, el dispositivo informático es afectado por un programa maligno con el fin de aprovechar o modificar su funcionamiento.[55]

---

[51] Arocena, G. A. *"La Regulación de los Delitos Informáticos en el Código Penal Argentino. Introducción a la Ley Nacional N° 26.388",* Boletín mexicano de derecho comparado, 45(135), 2011, 945-988. Disponible en: http://www.scielo.org.mx/scielo.php?script=sci_arttext&pid=S0041-86332012000300002&lng=es&tlng=es

[52] Arocena, G. A. *"La Regulación de los Delitos Informáticos en el Código Penal Argentino. Introducción a la Ley Nacional N° 26.388",* Boletín mexicano de derecho comparado, 45(135), 2011, 945-988. Disponible en: http://www.scielo.org.mx/scielo.php?script=sci_arttext&pid=S0041-86332012000300002&lng=es&tlng=es

[53] Callegari, N. "*Delitos informáticos y legislación".* Revista de la Facultad de Derecho y Ciencias Políticas de la Universidad Pontificia Bolivariana, N° 70, Colombia, 1985, pág. 115. Disponible en: https://egov.ufsc.br/portal/sites/default/files/6054-12231-1-sm.pdf

[54] Sain, G. y Azzolin H. "*Delitos informáticos. Investigación criminal, marco legal y peritaje",* Editorial BdeF, ISBN 978-9974-745-27-8, Montevideo-Buenos Aires, 2017

[55] Celli T., S. "*Las nuevas tecnologías y los delitos informáticos. Análisis de la ley 26.388. Modificación del Código Penal Argentino",* Tesis de Grado, Universidad Siglo 21, 2019.

En concordancia a los conceptos enumerados previamente, se puede deducir que la comisión de este tipo de delitos es, imprescindiblemente, a través de medios informáticos, tales como una computadora, un teléfono fijo o celular, *tablets*, etc., los cuales permiten la transmisión de datos.

Es importante destacar que, generalmente, la gran mayoría de delitos que se cometen mediante sistemas informáticos son de acción (positiva), o sea, que se cometen a través de un hacer. Siempre se perpetran mediante conductas (acciones positivas) con la voluntad de causar o generar resultados negativos sobre los bienes jurídicos.[56] Sin embargo, existe una minoridad de delitos informáticos que sí pueden cometerse a través de la **omisión**.

Recordemos que la omisión se da cuando hay un deber incumplido. Diego Migliorisi da un ejemplo interesante: un operador de una organización tiene la obligación de actualizar el antivirus ante un inminente ataque a su ordenador, pero no cumple con ella por lo que equivale a la intromisión de dicho virus por su parte.[57]

En conclusión, los delitos informáticos pueden configurarse por acción (conductas positivas) y también por omisión (conductas pasivas), aunque en el primer caso es lo más convencional.

En términos generales estas nuevas conductas delictivas, se enmarcan en la criminología de naturaleza cibernética, que se desarrolla a través de internet o mediante el uso de computadoras o dispositivos informáticos, siendo el objeto material del acto ilícito. *"Delitos que apuntan a los sistemas informáticos como objeto de la infracción, pero también a los que usan a la informática como medio para atentar contra bienes jurídicamente protegidos e incluso contra la privacidad y la dignidad de las personas."*.[58]

I. b) Características

El autor Telles Valdés en su obra *"derecho informático"*[59] procede a enumerar una serie de características de este tipo de delitos:

[56] Migliorisi, D. "*Crímenes en la Web: los delitos del siglo XXI"*, Editorial: Del Nuevo Extremo, ISBN 978-987-609-611-9, Ciudad Autónoma de Buenos Aires, 2014, pág. 36.
[57] Migliorisi, D. "*Crímenes en la Web: los delitos del siglo XXI"*, Editorial: Del Nuevo Extremo, ISBN 978-987-609-611-9, Ciudad Autónoma de Buenos Aires, 2014, pág. 37.
[58] Tribunal Superior de Justicia de la Provincia de La Rioja. Disponible en: https://justicialarioja.gob.ar/index.php/typography/noticias-e-informacion-general/558-peligros-en-la-web-el-avance-de-los-ciberdelitos
[59] Telléz V., J. "*Derecho Informático"*, Mc Graw Hill, 4° edición, México, 1987, pág. 188.

1. *Son conductas criminales de cuello blanco, en tanto que sólo determinado número de personas con ciertos conocimientos (en este caso técnicos) pueden cometerlas;*
2. *Son acciones ocupacionales en cuanto que muchas veces se realizan cuando el sujeto está trabajando;*
3. *Son acciones de oportunidad porque se aprovecha una ocasión creada o altamente intensificada en el campo de las funciones y organizaciones del sistema tecnológico y económico;*
4. *Provocan serias pérdidas económicas, ya que casi siempre producen "beneficios" de más de cinco cifras a aquellos que los realizan;*
5. *Ofrecen facilidades de tiempo y espacio, ya que pueden cometerse en milésimas de segundo y sin una necesaria presencia física;*
6. *Son muchos los casos y pocas las denuncias, debido a la falta de regulación jurídica a nivel internacional;*
7. *Son muy sofisticados y relativamente frecuentes en el ámbito militar;*
8. *Presentan grandes dificultades para su comprobación, por su carácter técnico;*
9. *En su mayoría son dolosos o intencionales, aunque también hay muchos de carácter culposo o imprudenciales;*
10. *Ofrecen a los menores de edad facilidades para su comisión;*
11. *Tienden a proliferar cada vez más, por lo que requieren una urgente regulación jurídica en el ámbito internacional.*

Además de estas características, consideramos importante e interesante hacer mención a la Teoría General del Proceso que entiende que este tipo de delitos presentan los mismos aspectos característicos en cuanto a su composición que los demás delitos.

En este sentido, se afirma que debe existir una acción u omisión por parte de un sujeto, que sea típica, es decir, prevista en nuestro sistema jurídico penal; que sea antijurídica y no se encuentre amparada por alguna causa de justificación; que exista la culpabilidad en el sujeto y debe ser pasible de una determinada sanción. Por supuesto a

esto se suma las particularidades que deben tener este tipo de delitos: que sea cometido con la utilización de medios informáticos.[60]

I. c) Clasificación

La Organización de Naciones Unidas (**ONU**) reconoció una serie de ciberdelitos y, en consecuencia, realizó una clasificación de los mismos que, generalmente, ha sido aceptada por los países ratificantes.[61]

En primer lugar, tenemos los **fraudes cometidos mediante la manipulación de computadoras.** Estos son aquellas conductas que consisten en la manipulación ilícita de datos tanto de entrada como de salida, de programas o el aprovechamiento de procesos de cómputo a través de computadoras.

Luego están las **falsificaciones informáticas** que pueden darse como *objeto* o como *instrumento*. En el primer supuesto se alteran datos de los documentos almacenados en forma computarizada, en el segundo se efectúan falsificaciones de documentos con fines comerciales.

Los **daños a los datos** son conductas consistentes en generar daños por medio de sabotajes, virus, gusanos, accesos no autorizados por hacker o cracker. Y, por último, está el **acceso no autorizado a servicios y sistemas informáticos**, que se puede dar por múltiples motivos que van desde la simple curiosidad, como en el caso de muchos piratas informáticos (hackers) hasta el sabotaje o espionaje informático.

Del mismo modo, Diego Migliorisi[62] considera que los delitos informáticos se dividen en dos grandes grupos: los **ciberdelitos tipificados o delitos tradicionales del Código Pernal que se configuran a través de Internet** y los **ciberdelitos propiamente informáticos.**

Los primeros *son los delitos históricamente tipificados en el Código Penal Argentino, cuya configuración se realiza utilizando medios informáticos y, por supuesto, Internet. Es decir, su existencia data de tiempos anteriores a la creación de Internet y la informática, y solamente se incorpora un nuevo medio para configurarlos.*

---

[60] Celli T., S. "*Las nuevas tecnologías y los delitos informáticos. Análisis de la ley 26.388. Modificación del Código Penal Argentino",* Tesis de Grado, Universidad Siglo 21, 2019.

[61] X° Congreso de las Naciones Unidas sobre Prevención del Delito y Justicia Penal, Salvador, Brasil, 2010.

[62] Migliorisi, D. "*Crímenes en la Web: los delitos del siglo XXI"*, Editorial: Del Nuevo Extremo, ISBN 978-987-609-611-9, Ciudad Autónoma de Buenos Aires, 2014, pág. 44

Mientras que los segundos son *aquellos que surgieron con la tecnología, es decir, con el nacimiento de la informática e Internet. También este grupo está integrado por delitos que están tipificados en el Código Penal, pero que han mutado sus efectos al ciberespacio, como el fraude informático y el daño informático.*

No obstante, existen otras clasificaciones, pero nos limitaremos a desarrollar éstas, ya que consideramos que ahondar en el tema excede al objeto de estudio.

II. Normas convencionales

II. a) Convenio de Budapest

El Convenio de Budapest es el primer tratado internacional vinculante en materia penal, creado para proteger a la sociedad de la ciberdelincuencia mediante el desarrollo de una legislación adecuada, la mejora de los métodos de investigación y el fortalecimiento de la cooperación internacional. Establece las herramientas jurídicas para la persecución de los delitos contra o utilizando los sistemas informáticos.

Lo mencionado *supra* se encuentra dentro del preámbulo del tratado, cuando éste establece que:

"Convencidos de la necesidad de aplicar, con carácter prioritario, una política penal común con objeto de proteger a la sociedad frente a la ciberdelincuencia, en particular mediante la adopción de una legislación adecuada y la mejora de la cooperación internacional."

En lo que se refiere a la "política penal general", la norma tiene por objeto otorgar a los Estados miembros la facultad de detectar, perseguir y sancionar conductas que, por la definición establecida en la primera parte del texto legal internacional, constituyan actos de riesgo para los sistemas, redes y datos informáticos, con el propósito de proteger los intereses legítimos relacionados con el uso y desarrollo de la tecnología de la información.

Este tratado es considerado la norma internacional más completa, ya que proporciona un marco integral y coherente contra el ciberdelito y la evidencia electrónica.

El contexto en el que surge esta norma internacional es que el mundo estaba sufriendo cambios profundos acaecidos por la digitalización. Se creó como resultado del reconocimiento de dos aspectos: en primer lugar, la necesidad de cooperación entre los

estados y el sector privado en la lucha contra el ciberdelito, y, por otro lado, la necesidad de proteger los intereses de uso lícito y desarrollo de los sistemas informáticos.

La idea del mismo es que los Estados ratificantes ajusten su normativa interna a las disposiciones del Convenio. Para ello, el Estado interesado deberá incluir los tipos penales enumerados y definidos en él, y proporcionar de facultades y herramientas procedimentales a las autoridades para investigar la comisión de estos delitos, incluyendo la expansión de capacidades de inteligencia, vigilancia y herramientas.[63]

Como mencionamos anteriormente, este convenio incluye tipos penales y los divide en: 1) delitos contra la confidencialidad, la integridad y la disponibilidad de los datos y sistemas informáticos; 2) delitos informáticos; 3) delitos relacionados con el contenido, y 4) delitos relacionados con infracciones a la propiedad intelectual y los derechos afines.

El Convenio se firmó el 23 de noviembre del 2001 y entró en vigencia el 1° de julio del 2004 en Budapest, Hungría. Argentina adhirió al mismo el 22 de noviembre del año 2017 a través de la ley N° 27.411.

Para que el Estado argentino se adhiera al Convenio tuvo que atravesar un largo proceso legislativo. Primero, en 1996 se dictó la ley de secretos comerciales N° 24.766, la que tipificó la sustracción de secretos comerciales que se encontraban dentro de soportes informáticos, posteriormente se promulgó la ley N° 11.703 de propiedad intelectual que, en 1998, se refirió a la copia ilegítima de cualquier programa de software y base de datos informáticos, y, por último, el Congreso en el año 2000 sancionó la ley N° 25.326 de protección de los datos personales.

Si bien ya existían leyes con contenido informático, todavía había un vacío legal con respecto a la ciberdelincuencia que perduró varios años, hasta que en 2008 se sancionó la ley N° 26.388, mejor conocida como la **ley de los delitos informáticos**, la cual modifica, sustituye e incorpora figuras típicas en el Código Penal de la Nación; y en el año 2013 se dictó la ley N° 26.904 la que penó el delito de ***grooming***. Todo ello, dio lugar a que la Argentina ratificara el Convenio de Budapest en el año 2017.

[63] Novoa T., I., Venegas C., L. *"Herramientas del Convenio de Budapest sobre ciberdelincuencia, y su adecuación a la legislación nacional"*, Tesis de Grado, Universidad de Chile, 2020. Disponible en: https://repositorio.uchile.cl/handle/2250/176344

A pesar de haberse adherido, el Estado argentino hizo sus reservas con respecto al Convenio:

"a) La República Argentina hace reserva del artículo 6.1.b. del Convenio sobre Ciberdelito y manifiesta que no regirá en su jurisdicción por entender que prevé un supuesto de anticipación de la pena mediante la tipificación de actos preparatorios, ajeno a su tradición legislativa en materia jurídico penal.

b) La República Argentina hace reserva de los artículos 9.1.d., 9.2.b. Y 9.2.c. del Convenio sobre Ciberdelito y manifiesta que estos no regirán en su jurisdicción por entender que son supuestos que resultan incompatibles con el CÓDIGO PENAL vigente, conforme a la reforma introducida por la ley 26.388.

c) La República Argentina hace reserva parcial del artículo 9.1.e. del Convenio sobre Ciberdelito y manifiesta que no regirá en su jurisdicción por entender que el mismo sólo es aplicable de acuerdo a legislación penal vigente hasta la fecha, cuando la posesión allí referida fuera cometida con inequívocos fines de distribución o comercialización (artículo 128, segundo párrafo, del Código Penal).

d) La República Argentina hace reserva del artículo 22.1.d. del Convenio sobre Ciberdelito y manifiesta que no regirá en su jurisdicción por entender que su contenido difiere de las reglas que rigen la definición de la competencia penal nacional.

e) La República Argentina hace reserva del artículo 29.4 del Convenio sobre Ciberdelito y manifiesta que no regirá en su jurisdicción por entender que el requisito de la doble incriminación es una de las bases fundamentales de la Ley de Cooperación Internacional en Materia Penal N° 24.767 para el tipo de medidas de cooperación previstas en artículo y numeral citados."[64]

II. b) Ley Nacional de Delitos Informáticos (N° 26.388)

La ley 26.388 se sancionó por el Congreso Nacional el 4 de junio del 2008. Es una ley especial que modifica, sustituye e incorpora figuras típicas en el Código Penal de la Nación. Podría decirse que, gracias a ella, nuestro Código Penal sufrió la principal reforma respecto a los delitos informáticos y pudo corregir ese vacío legal que existía en materia de ciberdelincuencia.

[64] Artículo 2, Ley N° 27.411. Disponible en: http://servicios.infoleg.gob.ar/infolegInternet/anexos/300000-304999/304798/norma.htm

La doctrina entiende que la ley de delitos informáticos no solo actualiza el Código Penal en relación a las lagunas legislativas que la jurisprudencia habría señalado, sino que implica asimismo un cambio de concepción en muchos conceptos legales que el avance tecnológico había dejado obsoletos.[65]

El debate tendiente a minimizar las lagunas jurídicas que existían en el ordenamiento nacional respecto a los delitos producidos a través de las nuevas tecnologías de la información comenzó en el 2000 con la promulgación parcial de la ley de Habeas Data (N° 25.326), de Protección de Datos Personales, donde también se protegen las bases de datos informáticas. Con las modificaciones al Código Penal del 2008 se reconoció la validez de los documentos y las firmas digitales como equivalentes a los documentos en cualquier otro soporte, a la vez que se reconoció la privacidad e inviolabilidad del correo electrónico, colocándolo a la misma altura que el correo epistolar.[66]

Pese a que, al momento de sancionar la ley 26.388, Argentina todavía no había adherido al Convenio de Budapest, a través de ella se tipificaron delitos informáticos en conformidad a este tratado.

La ley penaliza la divulgación por la red de pornografía infantil, la violación de la correspondencia electrónica, equiparándola a la correspondencia postal, la afectación de bases de datos y la comisión de delitos a través de la manipulación de comunicaciones informáticas, espionaje informático, entre otros. Además, incorpora a las nuevas tecnologías como medios de comisión de distintos tipos previstos en el Código Penal.[67]

Además de tipificar delitos, establece las condenas respectivas: prisión, inhabilitación -en el caso de que el delito lo cometa un funcionario público o el depositario de objetos destinados a servir de prueba- y multas. No sólo eso, Palazzi sostiene que la ley prohíbe el daño a bienes intangibles como, por ejemplo, el borrado de software o de datos contenidos en un ordenador.[68]

---

[65] Palazzi, P. A. *"Los Delitos Informáticos en el Código Penal. Análisis de la ley 26.388"*, 3º Ed. actualizada y ampliada, AbeledoPerrot, Argentina, 2016.

[66] López N. *"Sanciones para los Ciberdelincuentes"*, Revista Ciudad Segura, N.º Ecuador, 2011. Disponible en: https://repositorio.flacsoandes.edu.ec/bitstream/10469/6501/1/BFLACSO-CS44-03-Lopez.pdf

[67] Sorbo, H. D. "*Delitos Informáticos - Aspectos a tener en cuenta de la Ley 26.388"*, 2013. Disponible en: http://server1.utsupra.com/doctrina1?ID=articulos_utsupra_02A00376672921

[68] Palazzi, P. A. *"Los Delitos Informáticos en el Código Penal. Análisis de la ley 26.388"*, 3º Ed. actualizada y ampliada, AbeledoPerrot, Argentina, 2016.

También amplía el término **correspondencia**, ya que la ley se refiere a "comunicación electrónica". Ésta debe entenderse como todo mensaje enviado por un remitente a un destinatario a través de un sistema electrónico y así quedarían incluidos los correos electrónicos, chats, fax, llamadas o mensajes de textos. El contenido de ellos puede consistir en la voz, caracteres alfanuméricos o signos y gráficos de diversa índole que permiten algunos sistemas informáticos.[69]

[69] Arocena, G. A. *"La Regulación de los Delitos Informáticos en el Código Penal Argentino. Introducción a la Ley Nacional N° 26.388"*, Boletín mexicano de derecho comparado, 45(135), 945-988, 2011. Disponible en: http://www.scielo.org.mx/scielo.php?script=sci_arttext&pid=S0041-86332012000300002&lng=es&tlng=es

Capítulo III

ESTAFAS Y DEFRAUDACIÓN INFORMÁTICA

Sumario: estafas y otras defraudaciones, estafa informática, análisis del tipo penal, estafas informáticas en el período pandémico.

I. Estafas y defraudaciones informáticas

El artículo 172 del Código Penal de la Nación establece que *"será reprimido con prisión de un mes a seis años, el que defraudare a otro con nombre supuesto, calidad simulada, falsos títulos, influencia mentida, abuso de confianza o aparentando bienes, crédito, comisión, empresa o negociación o valiéndose de cualquier otro ardid o engaño."*[70]

En este caso, el legislador optó por no definir a la estafa, sino que utilizó un sistema ejemplificativo-casuístico, señalando las diferentes formas que resultan punibles. No obstante, el texto legal nos brinda una primera aproximación al concepto de **estafa**, en el sentido de que el delito consiste en una *defraudación causada mediante ardid o engaño.*[71]

Fontán Balestra la define como *"un ataque a la propiedad, consistente en una disposición de carácter patrimonial perjudicial, viciada en su motivación por el error que provoca el ardid o el engaño del sujeto activo, que persigue el logro de un beneficio indebido para sí o para un tercero*."[72]

La **defraudación** es *"toda lesión patrimonial producida con fraude"*.[73] Ésta no es un tipo delictivo sino una expresión genérica que abarca distintas clases de estructuras típicas: la estafa y el abuso de confianza.[74]

Según Soler[75], el **fraude** actúa como determinante del acto que ocasiona el perjuicio patrimonial, mientras que el **abuso de confianza** existe en una situación jurídica legítima preexistente, a partir de la cual se concreta posteriormente la defraudación.

El fraude es el medio propio de la estafa, el que consiste en la inducción mantenimiento o reforzamiento de otro en un error sobre un hecho o circunstancia, que

---

[70] Código Penal de la Nación, Artículo 172. Disponible en: http://servicios.infoleg.gob.ar/infolegInternet/anexos/15000-19999/16546/texact.htm#20

[71] Donna, E. A. "*Derecho penal: parte especial"*, T° II-B, Editorial: Rubinzal-Culzoni, Santa Fe, 2007, pág. 334

[72] Fontán B., C. "*Tratado de Derecho Penal"*, T° VI, Editorial Abeledo Perrot, Buenos Aires, 1980, pág. 35.

[73] Donna, E. A. "*Derecho penal: parte especial"*, T° II-B, Editorial: Rubinzal-Culzoni, Santa Fe, 2007.

[74] Buompadre, J.E. "*Derecho Penal: parte especial"*, 1° edición, ConTexto Libros Editorial, 2018, pág. 342

[75] Soler, S. "*Derecho Penal argentino"*, T° IV, Editorial: TEA, Buenos Aires, 1996, pág. 346.

lo determina a hacer la disposición patrimonial perjudicial para él o para un tercero respecto de cuyo patrimonio tiene poder legal para disponer.[76]

En las estafas la acción del delincuente comienza por un engaño de la realidad y obra de manera tal que la víctima causa o acepta la producción de un hecho que perjudica su patrimonio.[77] En otras palabras, es un delito de autolesión patrimonial causado por el ardid o engaño.

Es importante mencionar que, el dolo del autor en el presente delito, siempre es anterior -*ex ante*- a la prestación patrimonial y que la relación jurídica entre el sujeto activo y la víctima es ilegítima, ya que la confianza es lograda mediante fraude, lo cual determina la entrega de la cosa.[78]

De todo lo anteriormente expuesto, se entiende que los elementos exigidos por el tipo de estafa son el **engaño, error, acto de disposición patrimonial, perjuicio y ánimo de lucro.** Dichos elementos no pueden aparecer en forma aislada, sino que deben estar relacionados de una forma especial.[79]

Cuando nuestro Código Penal utiliza la frase *"o valiéndose de cualquier otro ardid o engaño"* en su artículo 172 convierte al precepto en un tipo penal abierto, puesto que utiliza una fórmula ejemplificativa de formas posibles de comisión.[80]

La ley 26.388[81], sancionada en el año 2008, con su artículo 9 incorporó al Código Penal de la Nación el inciso 16 estableciendo que *"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."*, incluyendo así a la estafa informática dentro del cuerpo normativo.

La **estafa informática** se la puede definir como *"la producción de un daño patrimonial cuantificable mediante un comportamiento externo, impropio de un*

---

[76] Tobares C., G. H. y Castro A., M. J. "*Delitos informáticos"*, 1° Edición, Editorial Advocatus, ISBN: 978-987-551-151-4, Córdoba, 2010.
[77] Molinario, A. J. "*Los delitos"*, T° II, Editorial: TEA Buenos Aires, 1999.
[78]Buompadre, J.E. "*Derecho Penal: parte especial",* 1° edición, ConTexto Libros Editorial, 2018, pág. 343
[79] Donna, E. A. "*Derecho penal: parte especial"*, T° II-B, Editorial: Rubinzal-Culzoni, Santa Fe, 2007, pág. 344.
[80] Buompadre, J.E. "*Derecho Penal: parte especial",* 1° edición, ConTexto Libros Editorial, 2018, pág. 342
[81] Ley N° 26.388, Artículo 9. Disponible en: http://servicios.infoleg.gob.ar/infolegInternet/anexos/140000-144999/141790/norma.htm

proceso automatizado informático, que altera los datos gestionados por éste, con ánimo lucro y en perjuicio de un tercero".[82]

Esta nueva modalidad constituye una figura especializada con relación a la estafa prevista en el artículo 172 del Código Penal, por el medio empleado (un sistema informático), aunque con anterioridad ya se había contemplado la posibilidad de defraudar con tarjetas de compra, débito o crédito sustraídas o extraviadas incluso si se lo hacía mediante operaciones automatizadas.[83]

De hecho, con esta inclusión al código de fondo desaparecerán las hipótesis de atipicidad que se daban por no concurrir en el caso concreto la secuencia tradicional de la estafa (ardid o engaño, error, disposición patrimonial perjudicial), en especial el engaño a otro a que hace referencia el art. 172 del Código que requiere para su determinación el engaño a otra persona física.[84]

Dicho artículo buscar incorporar ciertas situaciones patrimoniales abusivas relacionadas con la informática como una modalidad de defraudación, para superar el problema que presentaba en nuestro derecho y en el comparado respecto de la imposibilidad de estafar o engañar a una máquina u ordenador.[85]

Con respecto al **fraude informático**, es el *modus operandi*, a la dinámica intelectiva ideal, que caracteriza un determinado comportamiento. Implica la presencia dominante de un montaje o artimaña ideal que desencadena determinada modalidad de acción.[86] Lo informático del fraude está en el aprovechamiento, utilización o abuso de las características funcionales de los sistemas informáticos como instrumento para realizar una conducta astuta, engañosa, artera; o sea, el carácter informático del fraude alude al instrumento con cuyo auxilio se efectúa la defraudación.[87]

---

[82] Abogados Portaley, 2013. Disponible en: https://delitosinformaticos.com/04/2013/fraudes/estafas-en-internet

[83] Buompadre, J.E. "*Derecho Penal: parte especial",* 1° edición, ConTexto Libros Editorial, 2018, pág. 476

[84] Buompadre, J.E. "*Derecho Penal: parte especial",* 1° edición, ConTexto Libros Editorial, 2018, pág. 476

[85] Palazzi, P. A. *"Los Delitos Informáticos en el Código Penal. Análisis de la ley 26.388"*, 3º Ed. actualizada y ampliada, AbeledoPerrot, Argentina, 2016, pág. 169

[86] Gutiérrez F., M. L. "*Fraude informático y estafa",* Ministerio de Justicia, 1991.

[87] Garzón T., P. N. y Gallardo V., M. F. "*Fraude informático: valoraciones técnico-jurídicas*", Tesis de Grado, Universidad Técnica de Cotopaxi, 2009. Disponible en: http://repositorio.utc.edu.ec/bitstream/27000/139/1/T-UTC-0066.pdf

En definitiva, el fraude informático es el medio por el cual se logra el menoscabo patrimonial de una persona generando así el beneficio e incremento económico de otra.

Cabe aclarar que, los modos en que se lleva a cabo el fraude son diversos y serán desarrollados en el capítulo IV.

II. Estructura típica del tipo penal

El **bien jurídico** protegido en esta figura es el **patrimonio**[88] de la víctima. A pesar de ello, Gutiérrez Francés considera que las defraudaciones por medios informáticos lesionan algo más que el patrimonio en cuanto hay un interés social valioso y digno de protección, de carácter macrosocial, cuál sería la confianza en el funcionamiento de los sistemas informatizados.[89]

Existe otra opinión con respecto a esto y es que en realidad el bien jurídico protegido es la **libertad** de administrar los bienes ante transferencias patrimoniales.[90] Esto es así porque la víctima actúa con error generado por la manipulación y alteración de un sistema informático o transmisión de datos.

Incluso, hay quienes consideran que la estafa no afecta solamente al patrimonio, sino que excede de ello. Donna piensa que basta con analizar el contenido de los diferentes tipos de estafa para reconocer que en realidad la protección legal va mucho más allá.[91]

Aun así, es indudable que el bien jurídico protegido es el patrimonio, ya que el delito se encuentra ubicado en el Título VI del Libro II, ***"delitos contra la propiedad".*** Además, en este caso, no se castiga el engaño, sino que el daño patrimonial que ocasiona.

De todos modos, la doctrina mayoritaria, para establecer si hubo consumación de la estafa o no, es suficiente con establecer la existencia de una lesión de

[88] Conjunto de relaciones jurídicas de una persona valorables económicamente. (Teoría Alemana mixta jurídica-económica)
[89] Gutiérrez F., M. L. "*Fraude informático y estafa",* Ministerio de Justicia, 1991, págs. 266 y 267.
[90] Bottke, W. "*¿Qué es o a qué se llama estafa?",* Revista de Derecho Penal, ISBN 9789507273049, 2001, pág. 38.
[91] Donna, E. A. "*Derecho penal: parte especial"*, T° II-B, Editorial: Rubinzal-Culzoni, Santa Fe, 2007, pág. 262.

un elemento concreto del patrimonio, sin necesidad de efectuar un análisis global de la totalidad del patrimonio del sujeto pasivo antes y después del hecho.[92]

II. a) Aspecto objetivo

El tipo objetivo de estafa informática exige la presencia de tres elementos fundamentales: **la manipulación informática**, **error y disposición patrimonial perjudicial**. Estos elementos deben darse en tal orden y vincularse por una relación de causalidad. Esto es, que el sujeto activo manipule y altere un sistema informático o de transmisión de datos lo que generará error en la víctima y, posteriormente, ésta realice una disposición patrimonial perjudicial.

La **acción típica** es, además de las exigencias propias de cualquier otra defraudación[93], **defraudar** a otro *"mediante cualquier técnica de manipulación informática"*. La manipulación debe alterar el funcionamiento del sistema informático o de telecomunicaciones. Si bien esto es así, no cualquier manipulación informática es la que encuadra en la acción típica, sino que solamente aquella que es apta para producir dicho efecto.[94]

En este tipo de estafa no existe un ardid ni engaño sobre la víctima, sino que el autor altera el normal funcionamiento de sistemas informáticos o la transmisión de datos para obtener así una transferencia de patrimonio a favor de él o de otros.

Cabe aclarar que, este delito no puede ser cometido mediante una omisión, ya que ésta existe solamente cuando hay un deber incumplido y, en este caso, el sujeto activo realiza una acción para provocar un menoscabo.

De todo ello, se deduce que para que se configure la estafa informática tiene que haber la manipulación y alteración del normal funcionamiento del sistema informático o la transmisión de datos.

Buompadre define a la manipulación informática como *"cualquier modificación del resultado de un proceso automatizado de datos que se produzca a través de la introducción de nuevos datos, de la alteración de los existentes en el*

[92] Buompadre, J. E. *Código Penal*, T° VII, Editorial: Hammurabi, pág. 66.
[93] Engaño al sujeto pasivo, acto de disposición perjudicial para sí o para un tercero, ánimo de lucro.
[94] Migliorisi, D. "*Crímenes en la Web: los delitos del siglo XXI"*, Editorial: Del Nuevo Extremo, ISBN 978-987-609-611-9, Ciudad Autónoma de Buenos Aires, 2014, pág. 119

computador, en cualquier de las fases de su procesamiento o tratamiento informático"[95]

El delito quedará configurado solamente cuando la transferencia del patrimonio sea a partir de la alteración y manipulación de un sistema informático o transmisión de datos. En el caso que exista una disminución en el patrimonio de la víctima posteriormente a ser engañada por el autor a través de medios informáticos, será una estafa del artículo 172 del Código Penal.

Esto es importante aclararlo, porque popularmente se cree que, si te engañan por medio de redes sociales, llamadas telefónicas, aplicaciones de mensajería instantánea, etc., y luego se ocasiona un perjuicio económico, estamos frente la figura de **estafa informática.**

En cuanto el **error**, es el estado psicológico provocado por el autor del delito, quien induce a la víctima a la realización de una disposición patrimonial perjudicial**.**[96] El error, en este caso, debe ser causado por la manipulación de los sistemas informáticos.

El mismo es un requisito autónomo que se encuentra de manera tácita dentro del tipo penal, pero que deriva necesariamente del resto de los elementos del tipo objetivo.[97]

La **disposición patrimonial** debe ser, como hemos mencionado anteriormente, perjudicial. Ésta es aquel comportamiento, activo u omisivo, del sujeto inducido a error, que conllevará de manera directa la producción de un daño patrimonial en sí mismo o en un tercero[98]. Por ello, este delito se tiene como de autolesión, ya que es la víctima quien perjudica su patrimonio o el de un tercero.

En relación a los **sujetos**, este delito es considerado un delito común, ya que cualquier persona puede ser **sujeto activo** sin importar las características que éste tenga. Esto lo establece el inicio del artículo cuando dispone que *"el que defraudare […]"*, ello indica que el autor no requiere de ninguna calidad especial.

---

[95] Boumpadre, J. E. En *Derecho Penal*, Baigún-Zaffaroni y otros, T° VII, pág. 277, cita a Hendler.
[96] Donna, E. A. "*Derecho penal: parte especial"*, T° II-B, Editorial: Rubinzal-Culzoni, Santa Fe, 2007, pág. 361.
[97] Rodríguez, P. *"Estafas y otras defraudaciones"*, Revista Pensamiento Penal, 2013. Disponible en: https://web.archive.org/web/20200327152749/http://www.pensamientopenal.com.ar/system/files/cpcomentado/cpc37767.pdf
[98] Donna, E. A. "*Derecho penal: parte especial"*, T° II-B, Editorial: Rubinzal-Culzoni, Santa Fe, 2007, pág. 377.

En este sentido, el criminólogo Sutherland[99] entiende que el autor de este delito es una persona de cierto estatus socio-económico y que la comisión del delito no puede justificarse por pobreza, ni por mala habitación, ni por carencia de recreación, ni por baja educación, ni por poca inteligencia, ni por inestabilidad emocional.

Para Vaninetti[100] existen dos tipos de estafadores virtuales:

1. Quienes realizan maniobras delictivas más tradicionales y no requieren de conocimientos informáticos. Este tipo de sujeto activo solo necesita de conocimientos básicos como navegar en internet o utilizar el mail, por ejemplo.
2. Quienes sí tienen un gran conocimiento de utilización de la red. Estas personas manipulan sistemas de procesamiento de datos a la distancia, despliegan técnicas y procedimientos de distinta complejidad.

Por lo general, los primeros quedarían encuadrados en el artículo 172 del Código Penal, mientras que los segundos están comprendidos en el artículo 173, inciso 16 del mismo cuerpo normativo.

Comúnmente, se relaciona al *hacker* como el sujeto activo de este tipo de delito, pero como hemos mencionado *supra*, el legislador no exige ninguna calidad especial.

Para finalizar con lo que respecta al sujeto activo, es importante aclarar que éste puede o no tener autorización para el ingreso al sistema, ya que el tipo subjetivo requiere de **dolo directo**.

Todo aquél que sea perjudicado económicamente a través de la manipulación y alteración de un sistema informático o transmisión de datos, tanto persona física como jurídica puede ser **sujeto pasivo** de este tipo de delito.

II. b) Aspecto subjetivo

El delito es **doloso**, de dolo directo, ya que el autor debe conocer y querer manipular y alterar sistemas informáticos o la transmisión de datos para así generar un detrimento en el patrimonio de la víctima.

[99] Sutherland, E. "*Delitos de cuello blanco",* Editorial La Piqueta, Madrid, 1999.
[100] Vaninetti, H. A. "*Estafa en internet. Transferencia electrónica de fondos. Operatoria de home banking. La competencia en los delitos informáticos"*, Suplemento Penal y Procesal Penal, Revista Jurídica LA LEY, 2017.

Un delito doloso es aquél en el que un sujeto realiza una acción antijurídica conociendo su ilicitud y teniendo voluntad a tal fin.

La consumación de este tipo de delito se produce con el perjuicio patrimonial que generó el sujeto activo a través del uso de cualquier técnica de manipulación informática que altere el normal funcionamiento de un sistema informático o la transmisión de datos del sujeto pasivo.[101]

La tentativa es admisible, ya que el ciberdelincuente puede tener la intención de generar un perjuicio patrimonial a una persona y para ello, utilizar técnicas de manipulación informáticas, pero la posible víctima no caer en ellas, por lo tanto, la acción no quedaría configurada de modo consumado.

III. Defraudaciones informáticas en pandemia

Durante los dos primeros años de la pandemia de *Covid-19* en Argentina hubo un aumento en el número de denuncias sobre diversas actividades delictivas que se han producido mediante Internet. El aumento en el número de casos se puede atribuir al mayor uso de la tecnología de la información y comunicación, servicios de internet y aplicaciones por: referencias de trabajo remoto, capacitación a distancia y pago por servicios prestados por desarrollo de comercio electrónico. [102]

Por esta razón, en lo que respecta a la ciberseguridad, los últimos 24 meses ha habido un número récord de robos de tarjetas de crédito e información personal. Y no solo a los individuos, sino también las grandes empresas y negocios fueron extorsionados con una gran cantidad de dinero.

Con respecto a ello, algo interesante de mencionar es lo que advierte el Dr. Migliorisi: *"[…] lamentablemente, la adaptación al homeworking de forma tan repentina expuso a muchos usuarios y empresas a riesgos que en cierta forma se encontraban contenidos en los puestos de trabajo físico. En las empresas existen barreras de seguridad informática para prevenir ataques, filtraciones y robo de*

[101] Migliorisi, D. "*Crímenes en la Web: los delitos del siglo XXI"*, Editorial: Del Nuevo Extremo, ISBN 978-987-609-611-9, Ciudad Autónoma de Buenos Aires, 2014, pág. 134

[102] Jefatura de Gabinete de ministros, Secretaría de Innovación Tecnológica del Sector Público. *"Delitos Informáticos en Argentina: modalidades detectadas durante la pandemia del Covid-19"*. Disponible en: https://www.argentina.gob.ar/sites/default/files/2022/04/ciberdelitos_en_pandemia.pdf

información. En los dispositivos domésticos, las barreras de seguridad, en muchos casos, no son tan rigurosas y es ahí de donde los ciberatacantes sacan provecho." [103]

Esto es importante de aclarar, ya que no sólo el aumento del uso de las tecnologías en este periodo influyó a que los delitos informáticos se dispararan de manera tan drástica, sino que los particulares no cuenten con un sistema de ciberseguridad como el de las grandes empresas también contribuyó con ello.

La Unidad Fiscal Especializada en Ciberdelincuencia (UFECI) puso en conocimiento que los fraudes, usurpaciones de identidad y maniobras de *phishing* registraron un aumento entre abril de 2020 y marzo del 2021, recibiendo 14.583 denuncias e iniciando 289 investigaciones preliminares en Argentina.[104]

La misma entidad presentó el informe correspondiente al año 2020 en el cual, además de hacer foco en el aumento en la comisión de estos tipos de delitos, se detallaron los nuevos *modus operandi* que surgieron a partir de la pandemia, cuyo desarrollo será en el capítulo IV del presente trabajo de investigación.

En el informe se plasma que "*en el transcurso del año 2019 se recibieron un total de 2.369, lo que equivale a aproximadamente 6,5 reportes diarios -sin distinción de días hábiles y no hábiles-, mientras que, para el año 2020, el número ascendió a 11.396, un 381% más, lo que equivale a alrededor de 31 reportes por día."*[105]

Según la Asociación Argentina de Lucha Contra el Cibercrimen (en adelante A.A.L.C.C.), los delitos informáticos en Argentina desde la llegada de la pandemia incrementaron en un 60%.[106] Conforme a ésta, el 60,28% de los delitos informáticos de los últimos 5 años se reportaron en el 2020, principalmente bajo las modalidades de comercio digital o fraude bancario, además del robo de datos e

---

[103] Migliorisi, D. *"Delitos informáticos en cuarentena: riesgo y soluciones del trabajo online"*, Revista Consejo (Digital) N.° 60, ISSN 1851-6610, Ciudad Autónoma de Buenos Aires, 2020. Disponible en: https://archivo.consejo.org.ar/consejodigital/RC60/migliorisi.html

[104] Unidad Fiscal Especializada en Ciberdelincuencia. Disponible en: https://www.fiscales.gob.ar/ciberdelincuencia/la-unidad-fiscal-especializada-en-ciberdelincuencia-dimensiono-el-crecimiento-de-los-delitos-informaticos-en-su-informe-de-gestion-2020/#:~:text=Modalidades%20delictivas%20como%20fraudes%2C%20usurpaciones,e%20inici%C3%B3%20289%20investigaciones%20preliminares.

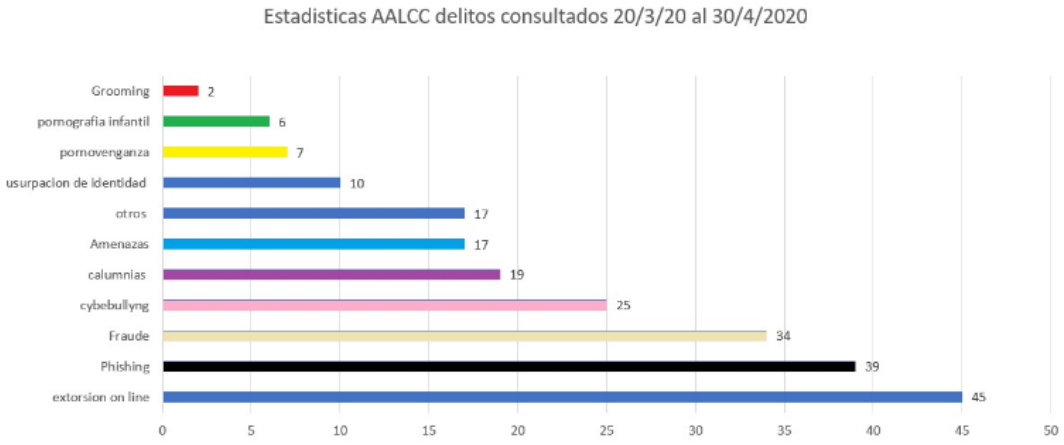
[105] Informe de Gestión de la UFECI 2020. Disponible en: https://www.mpf.gob.ar/ufeci/files/2021/09/UFECI_informe-pandemia.pdf

[106] Asociación Argentina de Lucha contra el Cibercrimen. *"Los delitos informáticos se dispararon en el país desde la pandemia"*, 2021. Disponible en: https://www.cibercrimen.org.ar/2021/04/20/los-delitos-informaticos-se-dispararon-en-el-pais-desde-la-pandemia/

información mediante el uso de logotipos de entidades y empresas, llamadas telefónicas o diversos métodos de captación.

Uno de los fraudes más cometidos durante el confinamiento, fue en relación al cobro del Ingreso Familiar de Emergencia (IFE)[107]. Los ciberdelincuentes aprovechaban la expectativa del cobro y creaban páginas falsas en la cual se solicitaba a los interesados que se inscriban exigiéndoles que aporten información de las tarjetas de créditos.

Otra manera de defraudar a aquellas personas que requerían del IFE era a través de llamadas telefónicas. Los estafadores se comunicaban por esta vía haciéndose pasar por gestores del ANSES y les pedían a sus víctimas datos personales como el nombre, apellido, fecha de nacimiento, etc., para otorgarle la ayuda. Posteriormente, el falso gestor le indicaba al interesado que se debía acercar a un cajero para generar una clave de seguridad, esta clave le permitía al delincuente acceder a la cuenta bancaria de la víctima.



Fuente: https://www.cibercrimen.org.ar/2020/05/03/importante-incremento-de-delitos-informaticos-en-cuarentena/

[107] Un seguro social de Argentina que se entregó a trabajadores informales y monotributistas de las primeras categorías durante la emergencia debido a la pandemia de enfermedad por coronavirus. Consistió en un bono de 10 mil pesos argentinos.

Estas estadísticas fueron realizadas por A.A.L.C.C. En ella se puede observar que durante el período pandémico correspondiente a los meses de marzo-abril 2020, los delitos informáticos fueron los más consultados por los argentinos a la A.A.L.C.C., sobre todo aquellos que producen un menoscabo en el patrimonio de la víctima. La misma asociación hace el análisis de que en el año 2019 el delito más consultado han sido las calumnias, seguida por la extorsión *online*.



Fuente: https://www.cibercrimen.org.ar/2020/12/24/estadisticas-ano-2020-completo/

En este gráfico, la A.A.L.C.C., comparó las consultas recibidas en el año 2019 y 2020. El 51,62% de los delitos consultados pertenecen a los configurables a través de internet con finalidades económicas, correspondiéndole al fraude un 18,10% y al *phishing* un 16,82%.

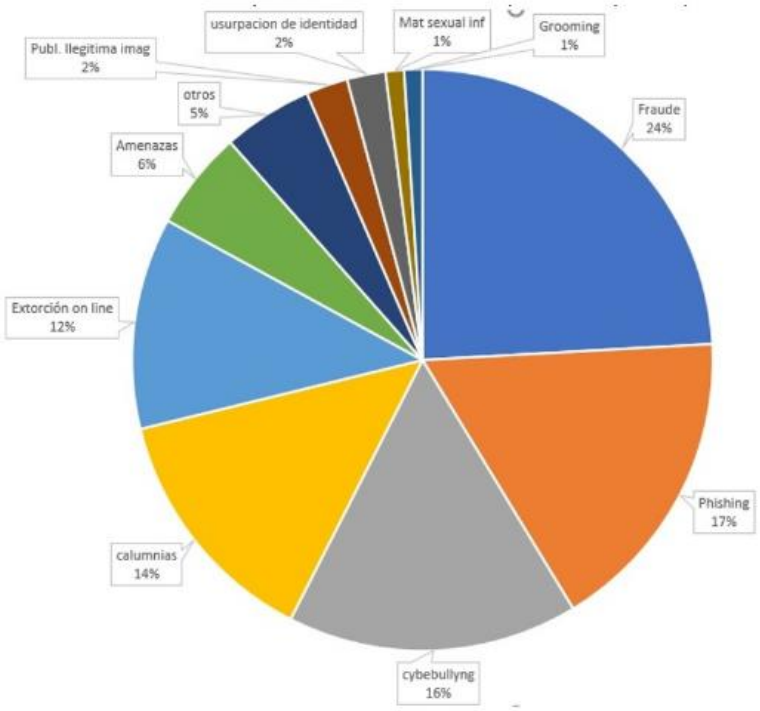
Del mismo estudio surgió que el 60,28% del total de los delitos informáticos consultados de los últimos 5 años se reportaron en el año 2020. A su vez, en el año 2020 aumentaron un 61,12% las denuncias respecto de mismo periodo en análisis en el año 2019.

Según datos registrados por el Equipo de Respuesta a Emergencias Informáticas (Cert.ar) dependiente de la Dirección Nacional de Ciberseguridad, se duplicó el número de incidentes de inseguridad informática en 2021 respecto al año anterior.[108]

[108] L.M. *"Los ciberataques en Argentina se duplicaron durante 2021",* Portal de Noticias "*Perfil"*, 2022. Disponible en: https://www.perfil.com/noticias/economia/los-ciberataques-en-argentina-se-duplicaron-durante-2021.phtml

En base a este informe, el 39,7% de los incidentes reportados correspondían a sitios del Estado; seguido por el sector finanzas (26,13%) y el de Tecnologías de la información y las comunicaciones (Tics) con 21,11%.

Pablo Rodríguez realizó un análisis para Télam en cuanto a los ciberdelitos e identificó que el 2021 ha sido un año marcado por las estafas virtuales, sobre todo bancarias. Los engaños a través de WhatsApp, correos electrónicos, mensajes de texto y llamados telefónicos se han convertido en los fraudes a usuarios más comunes y por los que se han tenido la mayor cantidad de denuncias y consultas.[109]



Fuente: https://www.cibercrimen.org.ar/2021/12/28/estadisticas-2021/

Este informe estadístico también lo realizó la A.A.L.C.C., y data desde el 31 de diciembre del año 2020 al 25 de diciembre del 2021. Se llevó a cabo teniendo en cuenta los casos consultados a través de *email*, teléfono, *whats app* y redes sociales.

De él se desprende que el fraude y el *phishing* fueron aquellos delitos más consultados durante el año 2021. Por lo tanto, siguen estando en cabeza de estos datos estadísticos los ciberdelitos con interés económico.

El Centro de Ciberseguridad Ciudadana de la Ciudad recibió en enero–febrero de 2022 un 30% más de denuncias que en el mismo período de 2021. El titular

[109] Rodríguez R., P. *"2021, un año donde las estafas virtuales fueron las protagonistas"*, Télam, 2021. Disponible en: https://www.telam.com.ar/notas/202112/579148-opinion-ciberdelitos.html

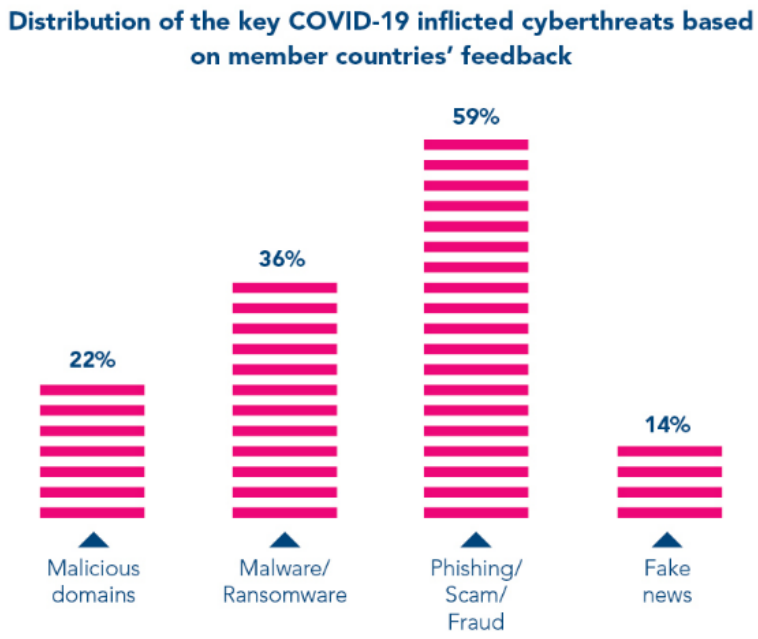
de la UFECI, Azzolin advierte que se detectó un incremento significativo de los accesos a billeteras digitales y cuentas como Mercado Pago:

> *"Detectamos un incremento significativo de los accesos a billeteras digitales y cuentas como Mercado Pago. Todas las modalidades tienden a tratar de acceder a la cuenta ya sea por engaño o por pérdida de control. Hoy cuando roban un celular no sólo monetizan con el aparato, sino con la plata que tenes accesible desde el teléfono. Todas estas nuevas aplicaciones que te permiten transferir con QR súper fácil también permiten que te afanen súper fácil."*[110]

El ataque más conocido del corriente año fue el hackeo a Mercado Libre, donde se secuestraron al menos 300 mil cuentas, la intención de éste era cobrar un rescate por los datos. Claramente esto generó temor por la seguridad de la plataforma ya que los delincuentes contaban con información que les puede permitir continuar realizando nuevos ataques y/o estafas sobre los usuarios. El responsable de este ataque es un grupo llamado *"**Lapsus$**"*, quienes extorsionaron a través de *ransomware* para lograr su cometido.

La INTERPOL hizo una evaluación sobre el panorama de la ciberdelincuencia en el período pandémico, y según ésta las estafas por internet y el *phishing* han aumentado un 59%, siendo éstos los delitos que más incrementaron en ese tiempo.

[110] Sarmiento, G. *"Se multiplican los robos virtuales sin control ni regulación",* Télam Digital, 2022. Disponible en: https://www.telam.com.ar/notas/202203/586202-se-multiplican-los-robos-virtuales-sin-control-ni-regulacion.html



Fuente: https://www.interpol.int/es/Noticias-y-acontecimientos/Noticias/2020/Un-informe-de-INTERPOL-muestra-un-aumento-alarmante-de-los-ciberataques-durante-la-epidemia-de-COVID-19

De acuerdo con este informe, durante la pandemia los ciberdelincuentes se hacían pasar por autoridades gubernamentales y sanitarias, y enviaban a sus víctimas correos electrónicos -*phishing*- sobre el *Covid-19* en los que las incitaban a facilitar datos personales y a descargar contenidos maliciosos.

En virtud de lo anteriormente expuesto queda a la luz que, durante la pandemia las defraudaciones informáticas incrementaron más que en años posteriores y esto dejó en evidencia el avance de las nuevas modalidades delictivas cometidas a través de los sistemas informáticos.

Capítulo IV

MODALIDADES DE LA ESTAFA INFORMÁTICA

Sumario: phishing, pharming, smishing, vishing, carding, hacking, ransomware, cracking, warez, viruking

Los estafadores virtuales, cometen sus maniobras delictivas de diferentes maneras, pero siempre con la misma finalidad: causar un perjuicio económico a la víctima y beneficiarse patrimonialmente.

A lo largo del presente capítulo abordaremos las maniobras a través de las cuales los autores cometen los hechos ilícitos previstos por el delito previsto por el artículo 173 inciso 16 del Código Penal de la Nación, toda vez que las figuras que se desarrollarán integran técnicas de manipulación informática prevista en el tipo penal

I. Phishing

La modalidad más conocida y utilizada es el ***phishing***, el cual consiste en apoderarse de la información personal de un usuario de Internet a través de la implementación de técnicas de ingeniería social, para engañar así a la víctima con el fin de acceder a sus cuentas de correo y obtener los datos de tarjetas de débito o crédito o el ingreso a las cuentas bancarias y, en consecuencia, disponer del dinero que se encuentra en ellas transfiriéndolo a un tercero denominado *"mule"*.

Esto es posible gracias a que el ciberdelincuente envía mensajes falsos a través del correo electrónico imitando a una persona u organización de confianza -una entidad financiera, una página de compras online o una oficina gubernamental-. Estos mensajes son una copia casi perfecta de un correo oficial del organismo falsificado y exigen que la víctima vaya a un sitio web y cumpla con las instrucciones que éste presenta.

Generalmente, estos mensajes tienen un contenido que busca provocar un miedo o preocupación a la víctima, por ejemplo:



En esta imagen, podemos ver como un usuario de Mercado Pago recibe un correo electrónico falso, en el cual se le advierte que se ha detectado un comportamiento irregular en sus operaciones y debía dirigirse a un *link*, seguir los pasos para reactivar su cuenta. El *link* redirige a la víctima a la siguiente página web:



Esta página web es idéntica al sitio web oficial de Mercado Pago, y en el momento que la víctima ingresa su nombre de usuario y clave, el estafador virtual consigue el acceso a la cuenta y, en este caso, a las tarjetas de débito y/o crédito.

"El phishing es la forma más sencilla de ciberataque y, al mismo tiempo, la más peligrosa y efectiva"[111]

i. *Cámara Federal de Casación Penal. Sala III. "Castelo, Pablo Alejandro". Causa N.º 51772/2011. 16/6/2015*

La maniobra de *phishing* ha sido calificada como una defraudación informática por la Sala III de la Cámara Federal de Casación Penal, al confirmar la sentencia dictada por el Tribunal Oral en lo Criminal N.º 18 de la Capital mediante la que condenó a la pena de un año de prisión a P. A. C., quien el 18 de noviembre de 2011 a través de la manipulación indebida de datos informáticos obtuvo el usuario y las claves de acceso a la cuenta corriente de un tercero en el Banco Francés y a través del

[111] MalwareBytes. Disponible en: https://es.malwarebytes.com/phishing/

sistema "*home banking*" efectuó una transferencia de dinero sin autorización de su titular.[112]

Hechos

El Tribunal Oral condenó a una persona a una pena de prisión por defraudación mediante técnicas de manipulación informática. La maniobra había consistido en ingresar a una cuenta de *homebanking* ajena, transferir dinero a la cuenta de un tercero para retirarlo con posterioridad. Contra esa decisión, la defensa interpuso recurso de casación. Entre otras cuestiones, se impugnó la autoría y la capacidad del condenado de realizar la maniobra defraudatoria.

El ciberdelincuente era un programador informático que prestaba tareas para A.F.I.P. y una empresa de desarrollo de software (*Global Logic*). Su condena fue de año de prisión en suspenso por ser encontrado responsable de haber cometido el delito de estafa informática empleando el método de *"phishing"* en los términos del art. 173 inc. 16 del Código Penal.

El delito se configuró mediante la manipulación indebida de datos informáticos el condenado obtuvo el usuario y contraseña de la víctima, para luego efectuar una transferencia de capitales mediante el sistema "home banking" por la suma de pesos $ 3.000 hacia la cuenta bancaria de un compañero de trabajo, quien tiempo después retiró el dinero por cajero automático.

"[…]La captación de datos ocurrió el 18 de noviembre de 2011, entre las 05:00 a 19:00 horas, en tanto que el dinero fue extraído por el nombrado D. O. A. de la siguiente forma: $ 2.000 el mismo día en horas de la tarde desde el cajero automático RB062 del Banco HSBC, sito en Avda. Corrientes 500 de esta ciudad y $ 1.000 el 21 de noviembre de 2011 del cajero automático S1CR1004 del Banco Santander Río, sito en la calle San Martín 427, sumas de dinero que luego fueron entregadas a P. A. C."

Resolución y fundamentos

La Sala III de la Cámara Federal de Casación rechazó el recurso interpuesto por el condenado.

[112]Cámara Nacional de Casación Penal, Sala III, "Castelo, Pablo Alejandro s/recurso de casación", Causa N.º CCC 51772/2011/TO1/CFC1,16/06/2015, publicado en: https://www.cij.gov.ar/nota-16796-Casaci-n-Penal-confirm--condena-por-defraudaci-n-inform-tica.html

La Cámara destacó que, si bien la transferencia se había realizado desde una IP situada en Guadalajara, México, no es un impedimento para imponerle la pena ya que, con las tecnologías existentes en la actualidad, cualquier persona que tenga conocimientos en la informática puede operar con una dirección IP de otro país.

Por otra parte, hacían mención al informe expedido por *"Google Inc."*, en la cual figura que la cuenta de correo de P. A. C. se encontraba vinculada a direcciones de IP extrañas a la jurisdicción argentina.

La defensa alegó que P. A. C. tenía incapacidad técnica para realizar la manipulación informática que se le atribuyó, sin embargo, el tribunal llegó a la conclusión, la cual tenía apoyo en las declaraciones de D. O. A., de que en "*Global Logic"* poseían herramientas y software adecuado para trabajar con páginas web que requerían de usuarios y contraseñas.

ii. *Cámara Nacional de Apelaciones en lo Criminal y Correccional. Sala V. "Pemow, Melanie y otros". Causa N.º 36742/2011. 24/10/2013.*

Otro fallo en el cual se ha tratado esta maniobra de defraudación informática -*phishing*- es en el caso Pemow, Melanie.

Hechos

Banelco denunció a un grupo de personas por el delito de *"phishing"*. A tres de ellas se les atribuía haber modificado las claves de *homebanking* de las víctimas para, posteriormente, transferir dinero a cuentas de terceros. Se identificó que las operaciones se habían realizado desde sus direcciones IP, utilizando internet para poder llevar a cabo la maniobra.

A otro grupo de personas se les atribuía la percepción de ese capital en sus cuentas personales y su posterior giro al exterior por servicio postal. En su indagatoria, expusieron que fueron contactados por correo electrónico o personalmente con el objetivo de trabajar como agentes de transferencia. Esto significaba que, ellos recibían el dinero de distintas fuentes y debían girarlo a España. Además, mencionaron que a ellos también le habían retirado dinero de sus propias cuentas bancarias.

El juzgado de instrucción sobreseyó a todos los imputados. Contra esta decisión, la fiscalía y la querella interpusieron recursos de apelación.

La fiscalía sostenía que la desvinculación de quienes integrarían el último eslabón de la cadena defraudatoria era prematura, y que corresponde extender la

investigación sobre aquellas personas que habrían percibido los fondos girados al exterior y los titulares de las IP.

Por su parte, la defensa argumentó que no se había analizado la intervención de cada uno de los imputados de manera particular, y que el cierre intempestivo de la investigación redunda en perjuicio de la verdad histórica de los hechos cuando aún restaría analizar si aquellos han tenido conocimiento y voluntad de realizar algún hecho ilícito.

Resolución y fundamentos

La Sala V de la Cámara de Apelaciones confirmó el sobreseimiento.

Según el tribunal, el grupo que recibía el dinero fueron todos víctimas de una misma maniobra delictiva en la cual actuaron -engañados- como meros instrumentos que obraron sin dolo de los verdaderos autores del ilícito.

Asimismo, dejaba en claro que, en caso de que los verdaderos delincuentes fuesen detectados, serán considerados autores mediatos, explicando que el rasgo fundamental de la autoría mediata reside en que el autor no realiza personalmente la acción ejecutiva, sino mediante otro; y lo que caracteriza el dominio del hecho es la subordinación de la voluntad del instrumento a la del autor mediato.

Concluían que, el idéntico *modus operandi* detectado en cada una de las maniobras significaba una estafa masiva en la que los agentes de transferencia de dinero fueron inducidos a error mediante un engaño para poder lograr el apoderamiento patrimonial indebido. El *modus operandi* se repitió de igual forma en todos los casos:

1. Obtención de datos de cuentas bancarias mediante la inserción de virus informáticos;
2. Contratación simulada de agentes de transferencia de dinero;
3. Giro de dinero a Barcelona, España, a nombre de terceros y a través de empresas de correo postal;

Por todo ello, el Tribunal concluyó en que los imputados obraron de buena fe y sin conciencia de ilicitud, por lo que, no se pudo completar el elemento subjetivo del tipo penal y rechazaron el recurso de apelación.

iii. *Cámara Federal de Apelaciones de San Martin. Sala I. "Inc. de apelación del procesamiento de Baroni". Causa N.º 10.540. Reg. N.º 9504. 7/6/2013.*

Hechos

El juzgado de instrucción había procesado a una persona por el delito de defraudación por medios informáticos. Las maniobras fraudulentas consistieron en el envío de varios correos electrónicos desde la casilla de la víctima, originados en IP pertenecientes al imputado y a su mujer, que tuvieron como consecuencia la transferencia de dominios de Internet al imputado.

Contra esta decisión, la defensa interpuso recurso de casación. Entre otras cuestiones, discutió la existencia de perjuicio económico como requisito necesario para configuración de la estafa.

Resolución y fundamentos

La Cámara Federal de San Martín confirmó el procesamiento.

"La figura penal de estafa informática, al igual que en todas las formas de estafa, requiere para su configuración el causar un perjuicio de contenido patrimonial a otra persona. En el caso, la disposición patrimonial debe ser consecuencia de cualquier técnica de manipulación informática que altere el normal funcionamiento de un sistema informático o la transmisión de datos que produce el hecho lesivo.

Se entiende como manipulación a cualquier modificación del resultado de un proceso automatizado de datos, a través de la alteración de los existentes o la introducción de nuevos, en cualquiera de las fases del proceso […]."

La Cámara entendió que el caso cumple con todas las exigencias para que se configure el tipo penal: la manipulación informática, transferencia de un activo con contenido de apreciación económica, perjuicio del patrimonio de la víctima y beneficio del imputado.

Con relación a la falta de acreditación del perjuicio económico, este tendrá lugar cuando el sujeto pasivo se vea privado de un elemento integrante de su patrimonio por obra de la acción delictiva, cuya disminución resulta evaluable económicamente.

I. a) Pharming

Una modalidad similar al *phishing* es el ***pharming***. Éste último también utiliza información fraudulenta que parece legítima para engañar a los usuarios con el

objetivo de que compartan información confidencial, pero la diferencia radica en que el *phishing* se lleva a cabo principalmente por **correo electrónicos falsos**, mientras que el *pharming* ocurre a través de **páginas web falsas**.[113]

En este tipo de estafa, la víctima sufre un ataque a los servidores DNS[114] -público o local- que usa para resolver los dominios de internet que quiere visitar. Al atacar el servidor DNS se consigue que cuando la víctima quiera visitar una página de confianza, realmente esté visitando otra diferente que el atacante ha dispuesto para robar información o engañar al usuario. Claramente, el *pharming* es mucho más complejo de entender que el *phishing*.

I. b) Smishing

El ***smishing*** es un tipo de *phishing* que funciona del mismo modo que éste, pero esta técnica consiste en el envío de un mensaje de texto o de un mensaje a través de aplicaciones de mensajería instantánea.

Siguiendo con el ejemplo de Mercado Libre, en 2021 se difundió mediante la aplicación de mensajería instantánea *Whats App* un mensaje de un supuesto sorteo por el aniversario de Mercado Libre:



[113] Bodnar, D. *"Qué es el pharming y cómo protegerse de él"*, Avast, 2016. Disponible en: https://www.avast.com/es-es/c-pharming

[114] "Sistema de Nombre de Dominio": método utilizado por Internet para traducir de forma fácil de recordar los nombres de dominio como *www.google.com* en lugar de su IP, de manera que sean entendibles por las personas y más fácil que si se trata de recordar secuencias numéricas, como es el caso de las IPs.

En el mensaje se promocionaban "unos 2000 productos gratis" por el 20 aniversario de la empresa. También envían un link que, al abrirse, se reenvía automáticamente a todos los contactos. Con ese simple clic, quedan expuestos los datos e información del usuario de cualquier celular.[115]

II. Vishing

Otra maniobra de defraudación informática es el ***vishing*** y, al igual que los anteriores, el ciberdelincuente suplanta la identidad de un tercero, pero a través de llamadas telefónicas, para obtener información personal de sus víctimas.

Para eso, el atacante debe tener previamente información de su víctima -nombre, apellidos, domicilio, etc.-, y que, al momento de realizar la llamada telefónica haciéndose pasar por un banco, por ejemplo, la víctima confíe en él. Con ello, el cibercriminal tratará de obtener más información, conseguir que el usuario instale algún *malware* en su equipo o realice algún tipo de pago.[116]

III. Carding

El ***carding*** consiste en la obtención de los datos de tarjetas de débito o crédito a través de plataformas digitales en las que se requieran estos datos o mediante dispositivos *posnet* o cajeros automáticos que reproducen los datos de las tarjetas, para realizar pequeñas compras con ellas y que de esta manera la víctima no detecte que se está realizando un uso fraudulento de la tarjeta.[117]

De lo anterior expuesto, se deduce que el *carding* puede cometerse personal o virtualmente. Es perpetrado personalmente gracias a un dispositivo denominado ***skimmer***, éste se instala en los cajeros automáticos o *posnet* y copia la información de la banda magnética. Además, generalmente, el delincuente instala una microcámara que apunte hacía el teclado numérico para copiar el pin que la víctima ingresa.

En la siguiente imagen, podemos apreciar el *skimmer* y observamos que es una réplica del lector de tarjetas que contienen los cajeros automáticos.

---

[115] *"Alerta por estafa: circula por WhatsApp un mensaje que ofrece regalos de Mercado Libre",* La Voz, 2021. Disponible en: https://www.lavoz.com.ar/ciudadanos/alerta-por-estafa-circula-por-whatsapp-un-mensaje-que-ofrece-regalos-de-mercado-libre/

[116] Oficina de Seguridad del Internauta. Disponible en: https://www.osi.es/es/actualidad/blog/2021/11/17/que-es-el-vishing

[117] Rojas, N. *"El Carding"*, Atalayar, 2022. Disponible en: https://atalayar.com/content/el-carding



El *carding* virtual se consuma a partir de plataformas digitales en las cuales se requiera el ingreso de los datos de tarjetas de crédito o débito.

IV. Hacking

Radica en el uso de herramientas informáticas para acceder a distancia a una computadora que tiene información confidencial sin autorización. Una vez que el delincuente se encuentra dentro del ordenador puede robar contraseñas, números de cuentas, datos de tarjetas de crédito o débito para posteriormente causar un daño patrimonial a la víctima. Solamente en ese caso, el *hacking* quedaría encuadrado en el tipo penal del 173 inciso 16.

V. Cracking

El ***cracking***, es una técnica que vulnera software informático o todo un sistema de seguridad con intenciones maliciosas. Aunque funcionalmente es lo mismo que el hackeo, el crackeo se usa estrictamente en un sentido delictivo.[118]

Existen distintos tipos de craqueos: de contraseñas, de software o de redes, y todas tienen fines maliciosos o delictivos.

Craqueos de contraseña:

a) **Crackeo por fuerza bruta**: El algoritmo de crackeo genera cadenas aleatorias de caracteres hasta que alguna coincida.

[118] Belcic, I. *¿Qué es el craqueo?"*, Avast, 2020. Disponible en: https://www.avast.com/es-es/c-cracking

b) **Crackeo de diccionarios**: Es parecido al crackeo por fuerza bruta, pero, en lugar de usar caracteres aleatorios, el crackeo por diccionarios se limita a palabras reales.

c) **Crackeo por tablas arcoíris**: Una tabla arcoíris usa valores de hash precalculados para averiguar el cifrado de *hashing* aplicado a una contraseña.

Craqueos de software:

a) **Generador de claves**: Se trata de un programa creado por un cracker para generar números de serie válidos para un producto de software. Si desea usar el software gratis, puede descargar el generador de claves y crear su propio número de serie, de modo que engañará a la protección anticopia del desarrollador para que piense que ha pagado por el software.

b) **Parche**: Los parches son pequeños fragmentos de código que modifican programas. Los desarrolladores lanzan parches para su software muy a menudo. Los crackers también pueden crearlos y, cuando lo hacen, la tarea del parche es alterar cómo funciona el programa eliminando las características no deseadas.

c) ***Loader***: La tarea del *loader* es bloquear las medidas de protección del software cuando este se inicie. Algunos *loaders* evitan las protecciones anticopia, mientras otros se usan para hacer trampas en juegos multijugador.

Craqueo de redes:

El crackeo de redes sucede cuando alguien vulnera la seguridad de una red LAN, es decir, una red de área local.[119]

Esta maniobra informática quedaría encuadrada en el artículo 173 inciso 16 del Código Penal de la Nación, en el caso que el *cracker* utilizase esta técnica para causar un perjuicio económico a un tercero. Por ejemplo, si el atacante, por medio de la **fuerza bruta,** logra descubrir la clave de alguna plataforma de compras -MercadoLibre, Amazon, Tienda Mía, entre otras- de una persona y adquiere bienes. Esta conducta quedaría configurada como una defraudación informática.

[119] Belcic, I. *¿Qué es el craqueo?"*, 2020. Disponible en: https://www.avast.com/es-es/c-cracking

VI. Warez

La conducta descripta anteriormente se vincula estrictamente con la ejecución de la maniobra del ***warez***. Éste es un término que define la recolección de intercambio de software comercial sin comprarlo y sin pagar derechos de autor.[120]

Es simplemente el tráfico y/o contrabando de programas protegidos por *copyright* que supuestamente tiene que ser comprado para su uso. En una palabra, el *warez* es Piratería. En la mayoría de los casos, los programas traficados y/o contrabandeados están crackeados para evitar las claves de acceso de los mismos.[121]

VII. Ransomware

El ***ransomware***, según el National Institute of Standards and Technology[122], es un tipo de ataque malicioso en el que los atacantes cifran los datos de una organización y exigen un pago para restaurar el acceso. Podría decirse que es un tipo de *hacking*, ya que con el uso de herramientas y conocimientos informáticos se logra acceder a un ordenador y bloquean el ingreso del mismo.



[120] La Web del Programador, Comunidad de Programadores, Diccionario Informático. Disponible en: https://www.lawebdelprogramador.com/diccionario/warez/

[121] Mesenzani, S., Cristiano, G. I. *"Algunas consideraciones sobre las conductas delictivas más habituales en la red. Cibercrimen"* Revista del Instituto de Estudios Penales - Número 7, IJ-LXV-884, IJ Editores, 2012. Disponible en: https://ar.ijeditores.com/articulos.php?idarticulo=62884&print=1#indice_2

[122] National Institute of Standards and Technology (NIST): https://www.nist.gov/itl/smallbusinesscyber/guidance-topic/ransomware

Aquí podemos ver un ejemplo de este ataque, en el cual el computador de la víctima se encuentra completamente bloqueado para el acceso, y el delincuente le impone una cuenta regresiva para que abone una determinada cantidad de dinero y que recupere sus archivos encriptados.

VIII. Viruking

Para finalizar, el ***viruking*** consiste en crear virus informáticos como los gusanos, troyanos o bombas lógicas y, posteriormente, acceder a la información personal de la víctima. El autor examina la computadora infectada y detecta archivos de interés como podrían ser aquellos que contienen el dato de las claves de acceso bancario, las que posteriormente pueden utilizarse para beneficiarse económicamente y de este modo consumar el delito de fraude informático.

Ahora bien, es dificultoso detallar todas las modalidades de estafa informática ya que, en primer lugar, existe una gran cuantidad de ellas y, por otro lado, los ciberdelincuentes renuevan y amplían rápidamente las formas de cometer el ilícito, aunque la mayoría son variantes de los *modus operandi* previamente expuestos. Sin embargo, las técnicas abordadas son las más importantes y utilizadas.

Así pues, del artículo 173 inciso 16 del Código Penal de la Nación surge que la defraudación informática debe cometerse a través de una técnica de manipulación informática. A partir de este término, se originan las modalidades mediante las cuales se configura el delito, y las que ya existían se van renovando con el tiempo. Hasta la actualidad son: *phishing, pharming, smishing, vishing, carding, hacking, cracking, warez, ransomware* y *viruking*.

A continuación, se analizará el principio de legalidad a los fines de verificar si con la implementación de la expresión manipulación informática se trastoca dicho precepto constitucional debido a la amplitud del concepto.

Capítulo V

PRINCIPIO DE LEGALIDAD

Sumario: principio de legalidad, características, ley cierta.

I. Introducción

En este capítulo se desarrollará el **principio de legalidad** haciendo, sobre todo, hincapié en la **ley cierta**; se detallarán las características del mismo.

II. Principio de legalidad

Un Estado de Derecho no sólo debe proteger a sus ciudadanos a través del Derecho Penal, sino que también del Derecho Penal. Para ello, se consagra el **principio de legalidad**.

El jurista y filósofo alemán Von Feuerbach fue quien en 1847 formuló el aforismo *"nullum crimen, nulla poena sine praevia lege poenali",* que, traducido a nuestro idioma, significa **"no hay delito, no hay pena, sin ley penal previa"**. El principio constituye una garantía individual que le exige al Estado que el delito esté previsto por una ley **escrita, cierta, previa y estricta emanada del órgano competente** para permitir la imposición de una pena.

El principio de legalidad es conocido universalmente por el apotegma mencionado *ut supra* donde el autor pone de relieve el rol funcional que cumple la ley, para la determinación de la infracción punible y de la sanción penal[123].

El Diccionario Panhispánico del Español Jurídico lo define como el principio jurídico según el cual no puede castigarse una acción u omisión si no está prevista como delito en una ley y que prohíbe el cumplimiento de las penas y de las medidas de seguridad en forma distinta de la prevista por la ley.[124]

Es un axioma de valoración de lo justo por una sociedad, en virtud del cual no se puede aplicar una sanción si no está escrita previamente en una ley cierta.[125]

Nuestro ordenamiento jurídico, en el artículo 18 de la Constitución Nacional, establece que *"ningún habitante de la Nación puede ser penado sin juicio previo fundado en ley anterior al hecho del proceso".* En el artículo 19 de la Carta Magna añade que *"[…] Ningún habitante de la Nación será obligado a hacer lo que no manda la ley, ni privado de lo que ella no prohíbe".* Además, la Convención

---

[123] López Pérez, Luis. *"El Principio de Legalidad Penal"*, 2021 Disponible en: https://www.studocu.com/pe/document/universidad-cesar-vallejo/derecho-penal-i/principio-de-legalidad/14313160

[124] Diccionario Panhispánico del Español Jurídico. https://dpej.rae.es/lema/principio-de-legalidad

[125] Velarde R., J. A. *"El Principio de Legalidad en el Derecho Penal"*, Revista LEX N° 13, ISSN 1991 – 1734, 2014. Disponible en: http://revistas.uap.edu.pe/ojs/index.php/LEX/article/view/44

Interamericana de Derechos Humanos, tratado de jerarquía constitucional, en su artículo 9 determina que *"Nadie puede ser condenado por acciones u omisiones que en el momento de cometerse no fueran delictivos según el derecho aplicable. Tampoco se puede imponer pena más grave que la aplicable en el momento de la comisión del delito."*

El **principio de legalidad** del artículo 18 constitucional, condiciona el ejercicio del *ius puniendi* dentro de las limitaciones legales (ley previa) y del cumplimiento de determinados procedimientos de aplicación (debido proceso legal) y ejecución de la pena, especificando con ello finalidades de la pena que el legislador penal no puede desconocer con relación a alguna de sus especies (las privativas de libertad) y hasta prohibiendo otras (penas corporales, pena de muerte para delitos políticos, penas pecuniarias, confiscatorias).

Bramont Arias entiende al principio de legalidad como la sumisión del Derecho Penal a la ley como única fuente creadora de delitos y penas, por lo cual solamente la ley tiene el monopolio en la creación de normas penales.[126]

Este principio está vinculado en diferentes niveles a todos los poderes del Estado.[127] En primer lugar, aporta una limitación de poder, sobre todo de poder judicial, porque los jueces deben aplicar exclusivamente lo que viene determinado por la ley, que debe ser lo más taxativa y precisa posible. De igual modo, restringe al poder legislativo, ya que se prohíben las leyes *ex post facto* o su modificación o derogación singular.[128]

Garantiza exigencias de seguridad jurídica, donde sólo la descripción precisa de las conductas que serán susceptibles de ser sancionadas penalmente habilita su reproche, demanda a su vez el reconocimiento de cierta idea republicana de distribución de poderes. En ese sentido, exige la existencia de una estructura estatal que sanciones las leyes y otra que defina las consecuencias ante su incumplimiento.[129]

---

[126] Bramont, A., L. *"El principio de legalidad de la represión y la nueva Constitución Política del Perú"*. En La Nueva Constitución y el Derecho Penal, ed. José Hurtado Pozo, pág. 27.
[127] Pérez P., K. *"Principio de igualdad: alcances y perspectivas*", Instituto de Investigaciones Jurídicas, iii-ii, 2005, pág. 55.
[128] Lamarca P., C. *"Principio de Legalidad Penal"*, Eunomía, Revista en Cultura de la Legalidad N.º 1, ISSN 2253-6655, 2011.
[129] Almada, J. M. *"Las Bases del Derecho Penal Liberal en Thomas Hobbes",* Revista Pensamiento Penal (ISSN 1853-4554), N° 405, 2021 Disponible en: https://www.pensamientopenal.com.ar/doctrina/89660-bases-del-derecho-penal-liberal-thomas-hobbes

El propósito de este principio es limitar al poder penal con lo que está descripto dentro de la ley y que los ciudadanos conozcan cuáles son las consecuencias jurídicas de su conducta delictiva y sus posibles sanciones.

Prohíbe las penas sin ley y sin ley previa escrita y estricta; declara ilícitas e ilegítimas las penas de hecho impuestas por cualquier autoridad, las penas retroactivas o sea las creadas *ad-hoc* y, en todo caso, después de la realización del hecho, las que pudieran dimanar de la costumbre y las que se pudieran aplicar por una integración analógica de la ley.[130]

Esto último quiere decir que, en primer lugar, el principio de legalidad exige que la ley sea **escrita**, por lo que prohíbe el derecho consuetudinario y, en segundo lugar, impide la implementación de la analogía porque la ley debe ser **estricta**. Del mismo modo, impone que la ley debe ser **previa** a la comisión del delito, sin importar que la conducta cause un daño a otro, si no existe una norma anterior que sancione la acción realizada, ésta no podrá ser juzgada. Además, obliga que esa ley sea **cierta**, de forma tal que debe describir de manera precisa y clara el hecho delictivo.

III. Características

El principio de legalidad tiene cuatro aspectos clásicos: *nullum crimen sine lege* ***scripta****; nullum crimen sine lege* ***previa*** y *nullum crime sine lege* ***stricta*** *o sine lege* ***certa***.

i. Lex Scripta

Bajo éste descansa la idea de que las conductas punibles (delitos) y sus consecuentes sanciones (penas) deben tener un fundamento normativo, un fundamento legislado en Derecho escrito. Sin embargo, no todo Derecho escrito es válido: la norma que los define debe provenir del poder legislativo, tener rango de ley. Prohíbe la aplicación de otros derechos que no se encuentren escritos, por lo que, el derecho consuetudinario, la jurisprudencia o los principios generales no puede ser fuente de los delitos y sus correspondientes consecuencias jurídicas.

Por tanto, existe reserva de ley para los delitos. Esto es un instituto que obliga a regular la materia concreta con normas que posean rango de ley, particularmente aquellas materias que tienen que ver con la intervención del poder

[130] Gómez R., N. *"Análisis de los Principios del Derecho Penal",* Disponible en: https://www.corteidh.or.cr/tablas/R06737-4.pdf

público en la esfera de derechos del individuo; resguarda la afectación de derechos al Poder Legislativo y refleja la doctrina liberal de la separación de poderes. [131]

Cabe aclarar que, esto no impide la existencia de los llamados "Tipos Penales en Blanco", mediante los cuales la conducta típica se completa en norma extrapenales a través de una remisión a éstas por parte del supuesto hecho de la norma penal legal.[132]

ii. Lex Previa

No hay delito si la ley no ha sido sancionada previamente antes de la comisión de la conducta o resultado prohibido, prohibiéndose la aplicación retroactiva de la norma penal, con la excepción de la ley penal más benigna.

La garantía de *lex praevia* se manifiesta en la prohibición de la aplicación retroactiva de la ley penal, esto es, para que una conducta pueda sancionarse como delictiva, la misma debe estar prevista como delito con anterioridad a su realización; en tal sentido, la ley penal creadora de delitos solo tiene efectos *ex nunc* (desde el momento en que se crea hacia el futuro; por regla general hasta que sea derogada), pero no *ex tunc* (retrotrayendo sus efectos a acciones anteriores).[133]

Asegura al ciudadano que una acción no sancionada como delito al momento de su comisión no podrá ser sancionada como delictiva con posterioridad a ésta. Con dicha garantía se restringe también la aplicación de consecuencias jurídicas que no hayan estado previstas con anterioridad a la comisión del delito y que agraven la situación jurídica del imputado.

La referida prohibición presenta su excepción, en materia penal, cuando favorece al reo, evitando el castigo o la agravación de una conducta que la sociedad ha decidido dejar sin reproche o atenuar el mismo.

iii. Lex Stricta

Este precepto se vincula con el de *lex certa*, ya que exige un cierto nivel de exactitud en el desarrollo del tipo penal para que la analogía no sea posible de aplicarla.

---

[131] Velarde R., J. A. *"El Principio de Legalidad en el Derecho Penal"*, Revista LEX N° 13, ISSN 1991 – 1734, 2014. Disponible en: http://revistas.uap.edu.pe/ojs/index.php/LEX/article/view/44

[132] Ayala G., A. *"El Principio de Legalidad Penal y su Configuración como Derecho Subjetivo en el Sistema Regional Europeo de Protección de los Derechos Humanos",* Foro, Nueva época, vol. 20, núm. 1, ISSN:1698-5583, 2017. Disponible en: https://revistas.ucm.es/index.php/FORO/article/view/57529

[133] Polaino N., M. *"Derecho Penal, Modernas Bases Dogmáticas"*, Editora Jurídica Grijley, 1° Edición, Lima, 2004, pág. 330.

Si el tipo penal es ambiguo, no está determinado con precisión, más necesaria será la analogía para completar su vaguedad.

Cuanto más completa y precisa sea en su redacción, menor uso se hará de la analogía no hay delito si la ley no es detallada al fijar el injusto, prohibiéndose la interpretación analógica de la norma penal.[134]

iv. Lex Certa

Este es el principio que importa al presente trabajo de investigación, por lo que será ahondado con más detalle que los anteriores.

Según el Diccionario Panhispánico del Español Jurídico, éste es *"la exigencia de que la ley describa exactamente el supuesto de hecho y defina la acción prohibida de modo que sea posible a los destinatarios de la norma programar su conducta y saber anticipadamente las consecuencias del incumplimiento"*.[135]

Esta exigencia comprende la obligación de determinar, dentro de la ley penal, las conductas punibles y sus consecuencias de manera clara, precisa y definida, esto es así para que no exista ningún tipo de incertidumbre con respecto al contenido y el alcance del tipo penal. El propósito es enumerar taxativamente las conductas que tengan una consecuencia penal.

El legislador al momento de formular el texto de la ley, no debe dar lugar a ambigüedades al momento de su aplicación para evitar la actuación arbitraria del Juez. Para ello, los tipos penales deben redactarse con la mayor exactitud posible evitando los conceptos clásicos o las expresiones notablemente imprecisas.

La Corte Interamericana de Derechos Humanos tiene dicho que *"la ambigüedad en la formulación de los tipos penales genera dudas y abre el campo al arbitrio de la autoridad, particularmente indeseable cuando se trata de establecer la responsabilidad penal de los individuos y sancionarla con penas que afectan severamente bienes fundamentales, como la vida o la libertad."*[136]

---

[134] Ayala G., A. *"El Principio de Legalidad Penal y su Configuración como Derecho Subjetivo en el Sistema Regional Europeo de Protección de los Derechos Humanos",* Foro, Nueva época, vol. 20, núm. 1, ISSN:1698-5583, 2017. Disponible en: https://revistas.ucm.es/index.php/FORO/article/view/57529

[135] Diccionario Panhispánico del Español Jurídico, https://dpej.rae.es/lema/claridad-de-la-ley

[136] Corte Interamericana de Derechos Humanos en Castillo Petruzzi y otros c/ Perú. Disponible en: https://www.corteidh.or.cr/cf/jurisprudencia2/ficha_tecnica.cfm?nId_Ficha=367&lang=es

La Dra. Loianno[137] entiende que las normas están hechas, principalmente, para aquellas personas que no tienen conocimientos académicos de Derecho y que son quienes van a interpretarlas -además de jueces y abogados-, por lo que aquellas leyes deben ser redactadas de una manera que al ciudadano "común" (como los define la Dra.) no se le dificulte entenderlas, y pueda comprender qué conductas están prohibidas, cuáles permitidas o qué sanciones existen.

Claramente, sostiene Loainno, que en el caso de conflicto serán los Jueces quienes tengan que interpretar esas normas. Por todo ello, la **ley cierta** es importante, para que la redacción de estas leyes no sea confusa y sean fáciles de comprender tanto para el ciudadano común como para aquellas personas que han estudiado al Derecho.

Los tipos penales no pueden quedar configurados de cualquier manera y por ello para respetar la legalidad debe estar determinada la conducta punible y su marco penal. Muchas veces el cuidado extremo de que la ley designe todas las propiedades relevantes de los casos genéricos puede conducir a extremos de sofisticación que haga poco entendible el tipo penal. En casos de esta naturaleza también la ley dejaría de ser una pauta clara de decisión para el juez. [138]

Recordemos que un tipo penal abierto es aquél que no individualiza totalmente la conducta prohibida, sino que exige que el juez lo haga, para lo cual debe acudir a **reglas generales** que se encuentran fuera del tipo penal y que pueden encontrarse en otras partes del mismo ordenamiento, en otros ordenamientos de igual o inferior jerarquía (ley de tránsito, reglamentos deportivos, etc.), en pautas éticas, sociales o de costumbre, cuando no se trata de actividades reglamentadas. El juez dispone de un punto de orientación suficientemente determinado por la ley, por lo que las posibilidades de cierre no son absolutamente amplias y libradas al arbitrio judicial, sino que aparecen referidas en el tipo (*el deber de cuidado* o *la posición de garante*). El juez determina los elementos que cierran el tipo y luego los incluye en él para subsumir la conducta bajo estudio en un caso concreto.

Ahora bien, a lo largo del presente trabajo se ha evidenciado que la forma en la que se encuentra redactado el tipo penal de defraudación informática en cuanto

[137] Loianno, A. *"¿Cómo Interpretar el Derecho Constitucional?"*, Maestros del Derecho UAI, 2011. Disponible en: https://www.youtube.com/watch?v=tyfpPoKxK_o

[138] Montiel, J. P. "E*structuras Analíticas del Principio de Legalidad"*, InDret, Revista para el Análisis del Derecho, InDret 1/2017, 2017. Disponible en: https://www.pensamientopenal.com.ar/system/files/2017/02/doctrina44842.pdf

establece que la comisión del delito a través de técnicas de manipulación informática, podría trastocar el principio de legalidad, más precisamente, la ley cierta. Ello debido a que, tal como se ha desarrollado, las maniobras de defraudación informática son diversas y con la pandemia se han incrementado, creándose nuevas modalidades comisivas de la figura típica del artículo 173 inciso 16 del Código Penal de la Nación.

Todo ello nos hace cuestionarnos si el artículo 173 inciso 16 del Código Penal obedece al principio de legalidad (ley cierta) en cuanto a la necesidad de que las conductas punibles y sus consecuencias estén determinadas de manera clara, precisa y definida en la ley penal para que no haya duda en cuanto a su contenido y alcance.

Con respecto a esta problemática, Palazzi y Righi tomaron su postura. Ellos entienden que la redacción del tipo penal trastoca el principio de legalidad.

Palazzi sostiene que la expresión "mediante cualquier técnica de manipulación informática" está haciendo alusión en forma abierta al accionar de la estafa informática, al que no se precisa, como hacen otras legislaciones, porque se trata de un elenco muy abierto de posibilidades.[139]

Por su parte, Righi ha adoptado la tesitura de que "será difícil que la norma pueda superar objeciones constitucionales vinculadas a su escaso apego al principio de legalidad".[140]

Por lo tanto, la problemática se genera entre la necesidad de la ley penal de abarcar los hechos ilícitos fraudulentos cometidos por las nuevas tecnologías, cuyas modalidades irán variando de un modo tan efímero que no será posible encuadrar mediante la ley penal cada formato de acción típica ejecutada por medios informáticos; y la demanda constitucional del principio de legalidad que exige la certeza de las conductas punibles.

[139] Palazzi, P. *"Los delitos informáticos en el Código Penal. Análisis de la ley 26.388*", Ed. Abeledo Perrot, Bs. As., 2009

[140] Donna, E. Alberto. "*Derecho Penal. Parte Especial",* Tomo II-B, tercera edición actualizada y reestructurada en relación al Código Civil y Comercial de la Nación, Rubinzal-Culzoni. Santa Fe, 2016, p. 593.

Conclusión

A lo largo del presente trabajo de investigación se ha expuesto sobre los sistemas informáticos y transmisión de datos, profundizando en su funcionamiento, origen y evolución para luego adentrarnos en los delitos informáticos, y el modo en que se cometen los delitos a través de las tecnologías. Además, se hizo mención al modo en que su comisión se profundizó en la pandemia, corroborando los datos estadísticos arrojados al respecto.

Posteriormente, ahondamos en el delito de defraudación informática (artículo 173 inciso 16 del Código Penal de la Nación) y analizamos el tipo penal y la redacción del mismo. De ello surgió la posibilidad de que su redacción colisione con el principio de legalidad, concretamente con la garantía de certeza de la norma.

Como hemos visto a lo largo del presente texto, las modalidades que podrían derivarse del elemento típico **cualquier técnica de manipulación informática** son diversas y al evolucionar la tecnología surgen otras, por ello, es importante determinar si la normativa cumple con el mandato de taxatividad.

Según nuestro punto de vista, en el caso de la estafa informática sería complejo prever cada conducta posible en este tipo penal, ya que del desarrollo del capítulo IV se vislumbra que favorece a que la comisión de este delito vaya progresando a la par del avance tecnológico. En consecuencia, el legislador redactó el artículo 173, inciso 16 del Código Penal de una manera amplia para abarcar todas las posibles conductas a través del término **manipulación informática**.

En este sentido, entendemos que el modo en que se encuentra redactado el tipo penal no trastoca el principio de legalidad, por cuanto es necesaria su redacción amplia para prever cada conducta posible. Es necesaria la flexibilización del mandato de taxatividad a fin de estar a la altura de los avances tecnológicos de la nueva era digital y no dejar impunes numerables de maniobras que podrían surgir como consecuencia de las técnicas empleadas en la comisión de este tipo de delitos.

Recordemos que la *lex certa* exige un mandato de taxatividad para que no haya dubitación respecto al contenido y alcance de la norma.

Caso contrario, debería modificarse y actualizarse cada un corto período de tiempo ya que, debido al avance tecnológico perenne, aparecen nuevas maniobras informáticas y otras quedan en desuso por parte de los atacantes informáticos.

Por ello, el legislador decidió redactar el tipo penal de manera amplia y general, enmarcando todas aquellas conductas específicas posibles dentro del término **"manipulación informática"**.

Cabe aclarar que, este tipo penal no describe las conductas típicas que se pretenden alcanzar de modo cerrado, sino que deja librado al juez la interpretación del elemento abierto de "manipulación informática". Esto es que, el magistrado debe, sin caer en la arbitrariedad, interpretar si la maniobra desplegada constituye una modalidad de manipulación informática.

Conviene subrayar que, no en todos los casos resulta posible cumplir la redacción clara y precisa del tipo penal, y este principio debe ser entendido con cierta elasticidad.[141]

Destacamos lo que resolvió la Corte Constitucional Colombiana en la Sentencia Nro. C-127/93[142] es que el Derecho Penal actual debe responder a "maquinarias delictivas" en movimiento que trascienden los viejos esquemas de los tipos cerrados, de modo que el tipo penal cerrado corresponden a los delitos **estáticos** y el tipo penal abierto a los delitos **dinámicos** o fruto de las nuevas y sofisticadas organizaciones y medios delincuenciales.

La estafa informática podría ser considerada un delito dinámico puesto que, los medios informáticos están en constante evolución y esto genera que los modos de cometer este tipo de delito varíen en cortos períodos de tiempo. Según lo dicho por la Corte Colombiana, lo conveniente para este delito sería un **tipo penal abierto**.

Coincidimos con el Dr. Donna cuando expresa que las modalidades para ejecutar el delito son tan variadas que el legislador prefirió dejar de lado la casuística y, en consecuencia, armó un tipo penal comprenda toda técnica que haga a la informática.[143]

En conclusión, por todo lo expuesto anteriormente, sostenemos que la redacción actual del tipo penal de estafa informática permite abarcar cada conducta específica posible y mantiene al elemento típico "actualizado" a través del uso del

---

[141] Piñeiro, J. L. *"Las Fuentes del Derecho Penal entre la Modernidad y Posmodernidad",* 2003. Disponible en: https://dialnet.unirioja.es/descarga/articulo/5028419.pdf

[142] Sentencia Nro. C-127/93, https://jurisprudenciaconstitucional.com/resolucion/110291-corte-constitucional-de-colombia-c-127-93

[143] Donna, E. A. "*Derecho Penal. Parte Especial."* Tomo II-B, 3° edición actualizada y reestructurada en relación al Código Civil y Comercial de la Nación, Rubinzal-Culzoni, 2016, pág. 593.

término **manipulación informática**, sin llegar a trastocar el principio constitucional de legalidad.

Entendemos que la exigencia de ley cierta, en este caso, debe ser entendida de una manera elástica y no restrictiva para así poder contemplar cada conducta, ya sea actual o que surja en un futuro. Tengamos en cuenta que la estafa informática es un delito dinámico y, por ello, se requiere cierta flexibilidad a la hora de interpretar el principio de legalidad.

Por todo lo expuesto, consideramos confirmada nuestra hipótesis.

Referencias

Bibliografía

- Andreu, R.; Ricart, J. y Valor, J. "*Estrategia y Sistemas de Información"*, Editorial McGraw-Hill, Barcelona, 1991
- Beladiez R., M. *"Los Principios Jurídicos*", Tecnos, 1° edición, Madrid, 1994
- Bramont, A., L. *"El principio de legalidad de la represión y la nueva Constitución Política del Perú"*. En La Nueva Constitución y el Derecho Penal, ed. José Hurtado Pozo
- Buompadre, J.E. "*Derecho Penal: parte especial",* 1° edición, ConTexto Libros Editorial, 2018
- Carrara, F. "*Programa di Diritto Criminale",* Editor Tip. Giusti, Sapienza - Università di Roma (Biblioteca Interdipartimentale di Scienze Giuridiche - Filosofia del Diritto Giorgio Del Vecchio, 1867.
- Cassagne, J. C. "*Los Principios Generales del Derecho*", Abeledo-Perrot, Buenos Aires, 1992
- Donna, E. A. "*Derecho Penal. Parte Especial."* Tomo II-B, 3° edición actualizada y reestructurada en relación al Código Civil y Comercial de la Nación, Rubinzal-Culzoni, 2016
- Donna, E. A. "*Derecho penal: parte especial"*, T° II-B, Editorial: Rubinzal-Culzoni, Santa Fe, 2007
- Fontán Balestra, C. "*Tratado de Derecho Penal"*, Tomo I, Abeledo Perrot, 2° edición, Buenos Aires, 1980
- Laudon, K. C.; Laudon, J. P. "*Sistemas de Información Gerencial"*, Editorial Pearson, ISBN: 978-607-32-0949-6, México, 1996
- Migliorisi, D. "*Crímenes en la Web: los delitos del siglo XXI"*, Editorial: Del Nuevo Extremo, ISBN 978-987-609-611-9, Ciudad Autónoma de Buenos Aires, 2014
- Molinario, A. J. "*Los delitos"*, T° II, Editorial: TEA Buenos Aires, 1999
- Palazzi, P. A. *"Los Delitos Informáticos en el Código Penal. Análisis de la ley 26.388"*, 3º Ed. actualizada y ampliada, AbeledoPerrot, Argentina, 2016
- Palazzi, P. *"Los delitos informáticos en el Código Penal. Análisis de la ley 26.388*", Ed. Abeledo Perrot, Bs. As., 2009.

- Polaino N., M. *"Derecho Penal, Modernas Bases Dogmáticas"*, Editora Jurídica Grijley, 1° Edición, Lima, 2004
- Sain, G. y Azzolin H. *"Delitos informáticos. Investigación criminal, marco legal y peritaje"*, Editorial BdeF, ISBN 978-9974-745-27-8, Montevideo-Buenos Aires, 2017
- Soler, S. "*Derecho Penal argentino"*, T° IV, Editorial: TEA, Buenos Aires, 1996
- Sutherland, E. "*Delitos de cuello blanco",* Editorial La Piqueta, Madrid, 1999
- Telléz V., J. "*Derecho Informático"*, Mc Graw Hill, 4° edición, México, 1987
- Tobares C., G. H. y Castro A., M. J. "*Delitos informáticos"*, 1° Edición, Editorial Advocatus, ISBN: 978-987-551-151-4, Córdoba, 2010
- Zaffaroni, E. R. "*Estructuras Básicas del Derecho Penal"*, EDIAR, 1° edición, 2009

Legislación

- Código Penal de la Nación;
- Convención Interamericana de Derechos Humanos.
- Convenio de Budapest (https://www.oas.org/juridico/english/cyb_pry_convenio.pdf);
- Ley N° 26.388. (http://servicios.infoleg.gob.ar/infolegInternet/anexos/140000-144999/141790/norma.htm);
- Ley N° 27.411. Disponible en: http://servicios.infoleg.gob.ar/infolegInternet/anexos/300000-304999/304798/norma.htm
- X° Congreso de las Naciones Unidas sobre Prevención del Delito y Justicia Penal, Salvador, Brasil, 2010

Otros

- *"Alerta por estafa: circula por WhatsApp un mensaje que ofrece regalos de Mercado Libre",* La Voz, 2021. Disponible en:

https://www.lavoz.com.ar/ciudadanos/alerta-por-estafa-circula-por-whatsapp-un-mensaje-que-ofrece-regalos-de-mercado-libre/

- Abogados Portaley, 2013. Disponible en: https://delitosinformaticos.com/04/2013/fraudes/estafas-en-internet
- Almada, J. M. *"Las Bases del Derecho Penal Liberal en Thomas Hobbes",* Revista Pensamiento Penal (ISSN 1853-4554), N° 405, 2021 Disponible en: https://www.pensamientopenal.com.ar/doctrina/89660-bases-del-derecho-penal-liberal-thomas-hobbes
- Arocena, G. A. *"La Regulación de los Delitos Informáticos en el Código Penal Argentino. Introducción a la Ley Nacional N° 26.388",* Boletín mexicano de derecho comparado, 45(135), 2011. Disponible en: http://www.scielo.org.mx/scielo.php?script=sci_arttext&pid=S0041-86332012000300002&lng=es&tlng=es
- Asociación Argentina de Lucha contra el Cibercrimen. *"Los delitos informáticos se dispararon en el país desde la pandemia",* 2021. Disponible en: https://www.cibercrimen.org.ar/2021/04/20/los-delitos-informaticos-se-dispararon-en-el-pais-desde-la-pandemia/
- Ayala G., A. *"El Principio de Legalidad Penal y su Configuración como Derecho Subjetivo en el Sistema Regional Europeo de Protección de los Derechos Humanos",* Foro, Nueva época, vol. 20, núm. 1, ISSN:1698-5583, 2017. Disponible en: https://revistas.ucm.es/index.php/FORO/article/view/57529
- Barzanallana, R. *"Historia de la informática. Introducción a la informática"*, Universidad de Murcia, Murcia, 2013. Disponible en: https://www.um.es/docencia/barzana/II/Ii04.html
- Belcic, I. *¿Qué es el craqueo?",* Avast, 2020. Disponible en: https://www.avast.com/es-es/c-cracking
- Blog de LINUBE. Disponible en: https://linube.com/blog/ciberespacio-no-es-internet/
- Bodnar, D. *"Qué es el pharming y cómo protegerse de él"*, Avast, 2016. Disponible en: https://www.avast.com/es-es/c-pharming
- Bottke, W. "*¿Qué es o a qué se llama estafa?"*, Revista de Derecho Penal, ISBN 9789507273049, 2001
- Callegari, N. "*Delitos informáticos y legislación".* Revista de la Facultad de Derecho y Ciencias Políticas de la Universidad Pontificia

Bolivariana, N° 70, Colombia, 1985, pág. 115. Disponible en: https://egov.ufsc.br/portal/sites/default/files/6054-12231-1-sm.pdf

- Celli T., S. "*Las nuevas tecnologías y los delitos informáticos. Análisis de la ley 26.388. Modificación del Código Penal Argentino.",* Tesis de Grado, Universidad Siglo 21, 2019.
- Ceruzzi, P. E. *"Historia de la informática",* Fronteras del conocimiento, Madrid, 2010, pág. 110 Disponible en: https://www.bbvaopenmind.com/wp-content/uploads/2009/01/BBVA-OpenMind-Fronteras_del_conocimiento.pdf
- Cruz R., J. E. "El Avance Tecnológico", 2009. Disponible en: http://www.rvcmar.org/otros/mapasc/JCR_EL_AVANCE_TECNOLoGICO.pdf
- Curtis E., L. "*Introduction to cyberspaceoperations",* 2011.
- Diccionario Panhispánico del Español Jurídico. https://dpej.rae.es/lema/principio-de-legalidad
- Garzón T., P. N. y Gallardo V., M. F. "*Fraude informático: valoraciones técnico-jurídicas"*. Tesis de Grado, Universidad Técnica de Cotopaxi, 2009. Disponible en: http://repositorio.utc.edu.ec/bitstream/27000/139/1/T-UTC-0066.pdf
- Garzón T., P. N. y Gallardo V., M. F. "*Fraude informático: valoraciones técnico-jurídicas*", Tesis de Grado, Universidad Técnica de Cotopaxi, 2009. Disponible en: http://repositorio.utc.edu.ec/bitstream/27000/139/1/T-UTC-0066.pdf
- Glosario digital de Arimetrics. Disponible en: https://www.arimetrics.com/glosario-digital/internet
- Gómez R., N. *"Análisis de los Principios del Derecho Penal",* Disponible en: https://www.corteidh.or.cr/tablas/R06737-4.pdf
- Hernández T., A. "*Los Sistemas de Información: Evolución y Desarrollo",* Proyecto social: Revista de Relaciones Laborales, ISSN 1133-3189, N.º 10-11, 2003. Disponible en: https://dialnet.unirioja.es/servlet/articulo?codigo=793097
- INTERPOL. Disponible en: https://www.interpol.int/es/Delitos/Ciberdelincuencia
- Jefatura de Gabinete de ministros, Secretaría de Innovación Tecnológica del Sector Público. *"Delitos Informáticos en Argentina: modalidades*

detectadas durante la pandemia del Covid-19". Disponible en: https://www.argentina.gob.ar/sites/default/files/2022/04/ciberdelitos_en_pandemia.pdf

- L.M. *"Los ciberataques en Argentina se duplicaron durante 2021",* Portal de Noticias "*Perfil",* 2022. Disponible en: https://www.perfil.com/noticias/economia/los-ciberataques-en-argentina-se-duplicaron-durante-2021.phtml
- La Web del Programador, Comunidad de Programadores, Diccionario Informático. Disponible en: https://www.lawebdelprogramador.com/diccionario/warez/
- Lamarca P., C. *"Principio de Legalidad Penal"*, Eunomía, Revista en Cultura de la Legalidad N.º 1, ISSN 2253-6655, 2011 Gutiérrez F., M. L. "*Fraude informático y estafa",* Ministerio de Justicia, 1991.
- Loianno, A. *"¿Cómo Interpretar el Derecho Constitucional?"*, Maestros del Derecho UAI, 2011. Disponible en: https://www.youtube.com/watch?v=tyfpPoKxK_o
- López N. *"Sanciones para los Ciberdelincuentes"*, Revista Ciudad Segura, N.º Ecuador, 2011. Disponible en: https://repositorio.flacsoandes.edu.ec/bitstream/10469/6501/1/BFLACSO-CS44-03-Lopez.pdf
- López Pérez, Luis. *"El Principio de Legalidad Penal"*, 2021 Disponible en: https://www.studocu.com/pe/document/universidad-cesar-vallejo/derecho-penal-i/principio-de-legalidad/14313160
- López Pérez, Luis. *"El Principio de Legalidad Penal"*, 2021. Disponible en: https://www.studocu.com/pe/document/universidad-cesar-vallejo/derecho-penal-i/principio-de-legalidad/14313160
- MalwareBytes. Disponible en: https://es.malwarebytes.com/phishing/
- Mesenzani, S., Cristiano, G. I. *"Algunas consideraciones sobre las conductas delictivas más habituales en la red. Cibercrimen"* Revista del Instituto de Estudios Penales - Número 7, IJ-LXV-884, IJ Editores, 2012. Disponible en: https://ar.ijeditores.com/articulos.php?idarticulo=62884&print=1#indice_2

- Montiel, J. P. "E*structuras Analíticas del Principio de Legalidad"*, InDret, Revista para el Análisis del Derecho, InDret 1/2017, 2017. Disponible en: https://www.pensamientopenal.com.ar/system/files/2017/02/doctrina44842.pdf
- National Institute of Standards and Technology (NIST): https://www.nist.gov/itl/smallbusinesscyber/guidance-topic/ransomware
- Next U, Tecnología de la Información, Disponible en: https://www.nextu.com/blog/generaciones-de-las-computadoras/
- NIC Argentina. Disponible en: https://nic.ar/es/enterate/novedades/que-es-internet
- Novoa T., I., Venegas C., L. *"Herramientas del Convenio de Budapest sobre ciberdelincuencia, y su adecuación a la legislación nacional"*, Tesis de Grado, Universidad de Chile, 2020. Disponible en: https://repositorio.uchile.cl/handle/2250/176344
- Observatorio Guatemalteco de Delitos Informáticos. Disponible en: https://ogdi.org/historia-del-cibercrimen
- Oficina de Seguridad del Internauta. Disponible en: https://www.osi.es/es/actualidad/blog/2021/11/17/que-es-el-vishing
- Pacheco J., Universidad Jaume I. Disponible en: https://www3.uji.es/~pacheco/INTERN~1.html
- Página Oficial del Gobierno argentino. Disponible en: https://www.argentina.gob.ar/justicia/convosenlaweb/situaciones/que-es-el-ciberdelito#:~:text=Los%20ciberdelitos%20que%20se%20cometen,fines%20econ%C3%B3micos%20y%20de%20da%C3%B1o.
- Pérez P., K. *"Principio de igualdad: alcances y perspectivas*", Instituto de Investigaciones Jurídicas, iii-ii, 2005
- Piñeiro, J. L. *"Las Fuentes del Derecho Penal entre la Modernidad y Posmodernidad",* 2003. Disponible en: https://dialnet.unirioja.es/descarga/articulo/5028419.pdf
- Pons G., V. "*Internet, la nueva era del delito: ciberdelito, ciberterrorismo, legislación y ciberseguridad"*. URVIO, Revista Latinoamericana de Estudios de Seguridad, Vol. núm.20, ISSN: 1390-

3691, 2017, págs. 80-93. Disponible en: https://www.redalyc.org/articulo.oa?id=552656641007

- Real Academia Española. https://dle.rae.es/internet?m=form
- Rinaldi, P. *"¿De dónde viene el delito cibernético? Origen y evolución del delito cibernético",* Le VPN, 2017. Disponible en: https://www.le-vpn.com/es/delito-cibernetico-origen-evolucion/
- Rodríguez R., P. "*2021, un año donde las estafas virtuales fueron las protagonistas"*, Télam, 2021. Disponible en: https://www.telam.com.ar/notas/202112/579148-opinion-ciberdelitos.html
- Rodríguez, P. *"Estafas y otras defraudaciones"*, Revista Pensamiento Penal, 2013. Disponible en: https://web.archive.org/web/20200327152749/http://www.pensamientopenal.com.ar/system/files/cpcomentado/cpc37767.pdf
- Rojas, N. *"El Carding"*, Atalayar, 2022. Disponible en: https://atalayar.com/content/el-carding
- Sanz L., F. J. "*El Derecho Ante las Nuevas Tecnologías de la Información",* 1997. Disponible en: https://ruc.udc.es/dspace/bitstream/handle/2183/1934/AD-1-26.pdf
- Sorbo, H. D. "*Delitos Informáticos - Aspectos a tener en cuenta de la Ley 26.388"*, 2013. Disponible en: http://server1.utsupra.com/doctrina1?ID=articulos_utsupra_02A00376672921
- Tribunal Superior de Justicia de la Provincia de La Rioja. Disponible en: https://justicialarioja.gob.ar/index.php/typography/noticias-e-informacion-general/558-peligros-en-la-web-el-avance-de-los-ciberdelitos
- Unidad Fiscal Especializada en Ciberdelincuencia. Disponible en: https://www.fiscales.gob.ar/ciberdelincuencia/la-unidad-fiscal-especializada-en-ciberdelincuencia-dimensiono-el-crecimiento-de-los-delitos-informaticos-en-su-informe-de-gestion-2020/#:~:text=Modalidades%20delictivas%20como%20fraudes%2C%20usurpaciones,e%20inici%C3%B3%20289%20investigaciones%20preliminares.

- Uriarte, J. M. "*Sistema Informático"*. Para Características.co, 2020. Disponible en: https://www.caracteristicas.co/sistema-informatico/
- Vaninetti, H. A. "*Estafa en internet. Transferencia electrónica de fondos. Operatoria de home banking. La competencia en los delitos informáticos"*, Suplemento Penal y Procesal Penal, Revista Jurídica LA LEY, 2017
- Vaninetti, H. A. "*Estafa en internet. Transferencia electrónica de fondos. Operatoria de home banking. La competencia en los delitos informáticos*", revista jurídica La Ley N.º 2017 a, 2017.
- Velarde R., J. A. *"El Principio de Legalidad en el Derecho Penal"*, Revista LEX N° 13, ISSN 1991 – 1734, 2014. Disponible en: http://revistas.uap.edu.pe/ojs/index.php/LEX/article/view/44

Jurisprudencia

- Cámara Nacional de Casación Penal, Sala III, "Castelo, Pablo Alejandro s/recurso de casación", Causa N.º CCC 51772/2011/TO1/CFC1,16/06/2015, publicado en: https://www.cij.gov.ar/nota-16796-Casaci-n-Penal-confirm--condena-por-defraudaci-n-inform-tica.html
- Castillo Petruzzi y otros c/ Perú. Disponible en: https://www.corteidh.or.cr/cf/jurisprudencia2/ficha_tecnica.cfm?nId_Ficha=367&lang=es
- Corte Interamericana de Derechos Humanos en Castillo Petruzzi y otros c/ Perú. Disponible en: https://www.corteidh.or.cr/cf/jurisprudencia2/ficha_tecnica.cfm?nId_Ficha=367&lang=es
- Sentencia Nro. C-127/93, https://jurisprudenciaconstitucional.com/resolucion/110291-corte-constitucional-de-colombia-c-127-93
- Sentencia Nro. C-127/93. Disponible en: https://jurisprudenciaconstitucional.com/resolucion/110291-corte-constitucional-de-colombia-c-127-93

CARTA DE ACEPTACIÓN DE TUTOR

Capital Federal, a los 3 días del mes abril del año 2022

Estimada alumna:

Iona Anabella Scandizzo

Por medio de la presente me dirijo a Ud. A fin de aceptar el cargo de tutora para su trabajo final titulado ***"Las defraudaciones informáticas en la época de pandemia y la implicancia del principio de legalidad."***

Saludo a Ud. Atte.



Dra. Desirée De Libano Elorrieta
Universidad Abierta Interamericana

Trabajo de Investigación Final

MM Miceli, Marilina <marilina.miceli@uai.edu.ar>
Para: Usted
Mié 16/3/2022 11:42

perfecto

De: Iona Scandizzo <ionascandizzo@hotmail.com>
Enviado el: miércoles, 16 de marzo de 2022 11:39 a. m.
Para: Miceli, Marilina <Marilina.Miceli@UAI.edu.ar>
Asunto: Trabajo de Investigación Final

ATENCIÓN: Este email proviene de un origen externo a la institución. No ingrese a links y tampoco abra archivos adjuntos en el mismo, salvo que Ud. conozca a la persona que se lo envía y sepa que el contenido es seguro.

...

Responder Reenviar

Iona Scandizzo
Para: Marilina.Miceli@UAI.edu.ar
Mié 16/3/2022 11:38

Buen día Marilina!
Soy Iona Scandizzo, D.N.I. 40.985.789, egresada regular de Abogacía.
Me comunicaba con usted para comentarle que cambié de tutor y de tema de tesis (nuevamente).
Mi nueva tutora es Desirée De Líbano Elorrieta, y reservar el tema "La defraudación informática y su impacto en el principio de legalidad en tiempos de pandemia."

NOTA DE ELEVACION DE TESIS

Capital Federal, a los 2 días del mes de agosto del año 2022

De mi mayor consideración:

Por la presente comunico, que la alumna ha confeccionado bajo mi supervisión el trabajo final, titulado: ***"Las defraudaciones informáticas en la época de pandemia y la implicancia del principio de legalidad."*** A mi entender por la calidad de su contenido y requisitos, está en condiciones de ser defendido ante el tribunal que se designe.

Saluda a Ud. Con mi mayor consideración,



Dra. De Libano Elorrieta, Derisée