South American Publishing

SAP Netnography. 2024; 2:76
doi: 10.62486/net202476

ORIGINAL

New types of crime and their classification in the Argentine Criminal Code

Nuevas modalidades delictivas y su tipificación en el Código Penal Argentino

Sabrina Ivana Bof[1]

[1]Universidad Siglo XXI, Especialización en Cibercrimen. Argentina.

Cite as
Bof SI. New types of crime and their classification in the Argentine Criminal Code. SAP Netnography. 2024; 2:76. https://doi.org/10.62486/net202476

Publication History
Submitted: 05-01-2024
Revised: 28-03-2024
Accepted: 05-08-2024
Published: 06-08-2024

ABSTRACT

Introduction: the rise of information technology has transformed everyday life, but it has also created fertile ground for the emergence of new crimes. In Argentina, cyber scams are one of the fastest-growing threats, affecting both individuals and public and private institutions. These criminal activities include financial fraud, identity theft, and computer manipulation, which cause significant economic damage and undermine digital trust. This paper analyzed the evolution of cyber scams, current legislation in the country, and its adequacy in the face of current technological challenges.
Development: using a mixed approach, legal precedents such as Law 26.388 on computer crimes and adherence to the Budapest Convention were reviewed, in addition to the classification of computer fraud in the Penal Code. It was found that, although these regulations represented progress, they are insufficient in the face of new forms of digital deception. These include phishing, spear phishing, scamming, vishing, and pyramid schemes, which are enhanced by artificial intelligence and social engineering. A comparative study with foreign legislation (US, Japan, European Union) showed that Argentina lags behind in terms of regulations and needs to strengthen international cooperation, training for judicial operators, and public awareness.
Conclusion: cyber scams require a comprehensive legal and technological response. The Penal Code needs to be reformed to criminalize specific behaviors such as identity theft and fraudulent use of social media. Only through updated laws, digital education, and inter-institutional coordination will it be possible to reduce the impact of these threats on Argentine society.

Keywords: Cyber Scams; Computer Crimes; Phishing; Argentine Criminal Code; Artificial Intelligence.

RESUMEN

Introducción: el auge de las tecnologías de la información ha transformado la vida cotidiana, pero también ha generado un terreno fértil para la aparición de nuevos delitos. En Argentina, las ciberestafas constituyen una de las amenazas más crecientes, afectando tanto a personas como a instituciones públicas y privadas. Estas conductas delictivas incluyen fraudes financieros, robo de identidad y manipulación informática, que producen daños económicos significativos y socavan la confianza digital. El presente trabajo analizó la evolución de las ciberestafas, la legislación vigente en el país y su adecuación frente a los desafíos tecnológicos actuales.
Desarrollo: a partir de un enfoque mixto, se revisaron antecedentes legales como la Ley 26.388 de delitos informáticos y la adhesión al Convenio de Budapest, además de la tipificación del fraude informático en el Código Penal. Se detectó que, si bien estas normas representaron avances, resultan insuficientes ante las nuevas modalidades de engaño digital. Entre ellas destacan el phishing, spear phishing, scamming, vishing y las estafas piramidales, potenciadas por la inteligencia artificial y la ingeniería social. El estudio comparado con legislaciones extranjeras (EE.UU., Japón, Unión Europea) mostró que Argentina presenta rezagos normativos y necesita fortalecer la cooperación internacional, la capacitación de operadores judiciales y la concientización ciudadana.
Conclusión: las ciberestafas exigen una respuesta jurídica y tecnológica integral. Es necesario reformar el Código Penal para tipificar conductas específicas como el robo de identidad y el uso fraudulento de redes sociales. Solo mediante leyes actualizadas, educación digital y coordinación interinstitucional será posible reducir el impacto de estas amenazas en la sociedad argentina.

Palabras clave: Ciberestafas; Delitos Informáticos; Phishing; Código Penal Argentino; Inteligencia Artificial.

© 2024; The Authors. This Open access article is distributed under the Creative Commons Attribution 4.0 license (https://creativecommons.org/licenses/by/4.0), which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

INTRODUCCIÓN

El avance de las tecnologías de la información y la comunicación (TIC) ha traído consigo una serie de beneficios para la sociedad, pero también ha creado nuevas oportunidades para los delincuentes.

En la era digital actual, las ciberestafas se han convertido en una amenaza cada vez más frecuente y sofisticada. Estas modalidades delictivas, que se llevan a cabo a través de medios electrónicos o informáticos, generan un impacto significativo en las víctimas, tanto a nivel individual como económico.

En este trabajo, se analizará la problemática de las ciberestafas en Argentina, haciendo hincapié en las nuevas modalidades delictivas que surgieron en los últimos años. Asimismo, se examinará la regulación existente en el Código Penal Argentino para este tipo de delitos, y se evaluará si la misma es suficiente para abordar adecuadamente la complejidad de estas nuevas formas de criminalidad.

MÉTODO

Enfoque metodológico

El presente trabajo se basará en un enfoque cualitativo y cuantitavo. El enfoque cualitativo permitirá comprender las experiencias y perspectivas de las víctimas de ciberestafas, así como las opiniones de expertos en ciberseguridad y derecho informático. El enfoque cuantitativo, por su parte, permitirá analizar datos estadísticos sobre la incidencia de las ciberestafas, las modalidades más comunes y las víctimas más afectadas.[1]

Hipótesis

El Código Penal Argentino presenta limitaciones significa vas para tipificar las nuevas modalidades de ciberestafas, lo que genera dificultades para la persecución y sanción de los ciberdelincuentes contribuyendo a su vez, al aumento de estas modalidades delictivas y al impacto negativo en las víctimas. La incorporación de figuras penales específicas en el Código Penal Argentino, junto con la capacitación de operadores jurídicos y la cooperación entre el sector público y privado, son elementos fundamentales para enfrentar este desafío

Antecedentes normativos

En la última década del siglo XX, como consecuencia de la llegada del comercio electrónico la República Argentina se vio inmersa en la necesidad de actualización normativa.[2]

Así se sancionaron diversas leyes, entre las que se pueden mencionar:

Ley 24.766 (1996) Confidencialidad sobre información y productos que estén legítimamente bajo control de una persona y se divulguen indebidamente de manera contraria a los a los usos comerciales honestos.

Ley 11.723 de Propiedad Intelectual (1998): que sanciona al que reproduzca, almacene, exhiba o importe copias ilegitimas.

Con la llegada del nuevo siglo, los avances de la tecnología y la aparición de los ciberdelitos, en el año 2000, se sancionó la Ley de Protección de Datos personales (Ley 25.326), para la protección integral de los datos personales, asentados en archivos, registros, bancos de datos. En el año 2008 La ley 26.388 de Delitos informáticos, que vino a modificar el Código Penal Argentino incorporando al articulado diversos tipos penales con motivo de la utilización de las nuevas tecnologías.

En el año 2013, la Ley 26.904 que incorpora en el art. 131 del Código Penal la figura de Grooming.

Convenio sobre la Ciberdelincuencia

Conocido como Convenio de Budapest, fue firmado en la ciudad que le da nombre el 23 de noviembre de 2001, y entró en vigor el 1ro. de julio de 2004. Impulsado por el Consejo de Europa, es el primer instrumento internacional que trata de manera específica el ciberdelito, emergiendo de su preámbulo que se basa en la necesidad de aplicar una política penal común, para proteger a la sociedad de la ciberdelincuencia, mediante la adopción de una legislación adecuada y la mejora de la cooperación internacional. Manifiesta preocupación en que las redes informáticas y la información electrónica sean utilizadas para cometer delitos, reconociendo la necesidad de prevenir dichos actos que puedan poner en peligro la confidencialidad, integridad y disponibilidad de los datos y sistemas informáticos, garantizando la tipificación de dichos actos como delitos.

En su articulado, establece en el artículo nro. 1 el significado: sistema informático, datos informáticos, prestador de servicio, datos de tráfico, luego entre los art. 2 y 10 compromete a las partes a tomar medidas ya sea legislativas o de otro tipo para tipificar como delito una serie de infracciones, a saber: acceso ilegítimo (art. 2), interceptación deliberada e ilegítima (art.3), ataques contra la integridad de datos (art. 4), ataques a la seguridad del sistema (art. 5), abuso de dispositivos (art.6), falsificación informática (art. 7), Fraude informático (art. 8), pornografía infantil (art. 9), Infracciones de la propiedad intelectual y derechos afines (art. 10). En el artículo 11 y s.s. compromete a las partes a adoptar medidas legislativas o de otro tipo que resulten necesarias para tipificar como delito en su derecho interno cualquier complicidad para la comisión de los delitos previstos anteriormente, dejando a criterio de las partes el aplicar en todo en parte o no aplicar en materia de tentativa.

En el art. 12 compromete a las partes a adoptar medidas para exigir responsabilidad a las personas jurídicas por los delitos previstos en el Convenio, estableciendo en el art. 13 que las sanciones deben ser efectivas, proporcionadas y disuasorias, incluidas las penas privativas de la libertad, debiéndose garantizar la imposición de sanciones o medidas penables o no penales a las personas jurídicas consideradas responsables.

El artículo 15 se refiere a las condiciones y garantías y establece: “Las partes velarán para que la instauración, puesta en funcionamiento y aplicación de los poderes y procedimientos previstos en la presente sección se sometan a las condiciones y

https://doi.org/10.62486/net202476

garantías dispuestas en su derecho interno, que debe asegurar una protección adecuada de los derechos del hombre y de las libertades y, en particular de los derechos derivados de diversos instrumentos internacionales relativos a los derechos del hombre.

En sus arts. 16 al 21 habla de medidas para la conservación, divulgación, comunicación, registro y decomiso, interceptación de datos. Así como normas referentes a competencia, cooperación internacional, extradición, colaboración, adhesión e implementación del convenio, etc.

Posteriormente se ha sancionado el "Protocolo adicional al Convenio sobre la Ciberdelincuencia relativo a la penalización de actos de índole racista y xenófoba cometidos por medio de sistemas informáticos, (el "Protocolo") y en el año 2022 se aprobó el Segundo Protocolo Adicional[3] tiene por objeto afianzar los lazos en materia de cooperación internacional y facilitar la obtención de evidencia electrónica para poder brindar una respuesta eficaz en la investigación criminal para trabajar contra el ciberdelito, en cuya redacción ha participado entre otros, la República Argentina.

Código Penal Argentino[4]

En el año 2008 se sancionó la Ley 26.388 conocida como "Ley de delitos informáticos", que recepta los principios del Convenio de Budapest, aunque nuestro país recién se adhirió a dicho Convenio en el año 2017 a través de la Ley 27.411, en su articulado puede observarse la recepción de las recomendaciones efectuadas por el Consejo de Europa.

La ley 26.388 de Delitos informáticos, vino a modificar el Código Penal Argentino incorporando al articulado diversos tipos penales con motivo de la utilización de las nuevas tecnologías.

Así, en materia de delitos informáticos contra la libertad modifica el art. 153 del C.P., el que en su párrafo primero penaliza la conducta de acceder, apoderarse, suprimir o desviar una comunicación electrónica que no le esté dirigida. La pena es mayor s el contenido de la comunicación electrónica se publica. En este caso lo que la ley vino a tutelar es la comunicación escrita entre personas u la indebida intromisión de un tercero, ya sea accediendo a ella, interceptándola o desviándola de sus fines.

El art. 153 párrafo primero segunda parte del C.P. castiga al que se apoderare indebidamente de una comunicación electrónica, una carta, un pliego, un despacho u otro papel privado, aunque no esté cerrado.

La tercera parte del art. 153 párrafo primero reprime la conducta de quien indebidamente suprimiere o desviare de su destino una correspondencia o una comunicación que no le este dirigida.

El tercer párrafo del art. 153 del CP agrava la pena si el autor además comunicare a otro o publicare el contenido de la carta, escrito, despacho o comunicación electrónica.

Asimismo, esta Ley incorpora el art. 153 bis penalizando la conducta de "acceder ilegítimamente a un sistema o dato informático de acceso restringido. La pena se agrava cuando el acceso es en perjuicio de un sistema o dato informático de un organismo público estatal o de un proveedor de servicio públicos de servicios financieros.

Por otro lado, sustituye el art. 155 del C.P. por el siguiente: "Será reprimido con multa de pesos un mil quinientos ($1 500) a pesos cien mil ($100 000), el que, hallándose en posesión de una correspondencia, una comunicación electrónica, un pliego cerrado, un despacho telegráfico, telefónico o de otra naturaleza, no destinados a la publicidad, los hiciere publicar indebidamente, si el hecho causare o pudiere causar perjuicios a terceros. Está exento de responsabilidad penal el que hubiere obrado con el propósito inequívoco de proteger un interés público".

También sustituye el art. 157 del C.P. que queda redactado del siguiente modo: "Será reprimido con prisión de un (1) mes a dos (2) años e inhabilitación especial de un (1) a cuatro (4) años, el funcionario público que revelare hechos actuaciones, documentos o datos, que por ley deben ser secretos" La única modificación al artículo 157 es el agregado de la palabra "datos". Así se actualiza esta figura en la cual el sujeto debe ser un funcionario público que tomare conocimiento de datos, actuaciones, hechos o documentos que por ley sean secretos y que además el funcionario los revelare a pesar de conocer esta circunstancia.

Artículo 157 bis- "Será reprimido con la pena de prisión de un (1) mes a dos (2) años el que: 1. A sabiendas e ilegítimamente, o violando sistemas de confidencialidad y seguridad de datos accediere, de cualquier forma, a un banco de datos personales. 2. Ilegítimamente proporcionare o revelare a otra información registrada en un archivo o en un banco de datos personales cuyo secreto estuviere obligado a preservar por disposición de la ley. 3. Ilegítimamente insertare o hiciere insertar datos en un archivo de datos personales. Cuando el autor sea funcionario público sufrirá, además, pena de inhabilitación especial de un (1) a cuatro (4) años.":

Incorpora como segundo párrafo del artículo 183 del Código Penal, el siguiente: En la misma pena incurrirá el que alterare, destruyere o inutilizare datos, documentos, programas o sistemas informáticos; o vendiere, distribuyere, hiciere circular o introdujere en un sistema informático, cualquier programa destinado a causar daños.

Dispone sustituir el artículo 184, el 197 y el 255 del Código Penal, por los siguientes:

Artículo 184: La pena será de tres (3) meses a cuatro (4) años de prisión, si mediare cualquiera de las circunstancias siguientes: 1. Ejecutar el hecho con el fin de impedir el libre ejercicio de la autoridad o en venganza de sus determinaciones; 2. Producir infección o contagio en aves u otros animales domésticos; 3. Emplear substancias venenosas o corrosivas; 4. Cometer el delito en despoblado y en banda; 5. Ejecutarlo en archivos, registros, bibliotecas, museos o en puentes, caminos, paseos u otros bienes de uso público; o en tumbas, signos conmemorativos, monumentos, estatuas, cuadros u otros objetos de arte colocados en edificios o lugares públicos; o en datos, documentos, programas o sistemas informáticos públicos; 6. Ejecutarlo en sistemas informáticos destinados a la prestación de servicios de salud, de comunicaciones, de provisión o transporte de energía, de medios de transporte u otro servicio público.

Artículo 197: Será reprimido con prisión de seis (6) meses a dos (2) años, el que interrumpiere o entorpeciere la comunicación telegráfica, telefónica o de otra naturaleza o resistiere violentamente el restablecimiento de la comunicación interrumpida.

Artículo 255: Será reprimido con prisión de un (1) mes a cuatro (4) años, el que sustrajere, alterare, ocultare, destruyere o inutilizare en todo o en parte objetos destinados a servir de prueba ante la autoridad competente, registros o documentos confiados

https://doi.org/10.62486/net202476

a la custodia de un funcionario público o de otra persona en el interés del servicio público. Si el autor fuere el mismo depositario, sufrirá además inhabilitación especial por doble tiempo. Si el hecho se cometiere por imprudencia o negligencia del depositario, éste será reprimido con multa de pesos setecientos cincuenta ($ 750) a pesos doce mil quinientos ($ 12 500).

La ley incorpora como inciso 16 del artículo 173 del Código Penal, el siguiente:

Inciso 16. El que defraudare a otro mediante cualquier técnica de manipulación informática que altere el normal funcionamiento de un sistema informático o la transmisión de datos.

Además de los artículos señalados, si bien el Código Penal Argentino no contiene un capítulo específico existen algunas disposiciones que pueden ser aplicadas a este tipo de delitos. Por ejemplo:

Art. 172: " 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."

Art. 173: inc. 15 El que defraudare mediante el uso de una tarjeta de compra, crédito o débito, cuando la misma hubiere sido falsificada, adulterada, hurtada, robada, perdida u obtenida del legítimo emisor mediante ardid o engaño, o mediante el uso no autorizado de sus datos, aunque lo hiciere por medio de una operación automática. (Inciso incorporado por art. 1° de la Ley N° 25.930 B.O. 21/9/2004)

Sin embargo, estas disposiciones han sido criticadas por ser genéricas y no contemplar las particularidades de las ciberestafas.[5]

Nuevas modalidades de Ciberestafas

Como se mencionó anteriormente, a diario van apareciendo nuevas modalidades de delitos en los que resultan victimas los titulares de cuentas bancarias y para lo cual los delincuentes recurren a distintas maniobras delictivas.[6,7,8]

En particular los delitos de fraude con tarjetas de crédito han sido de los que mayor crecimiento han tenido en los últimos tiempos. Este tipo de delito, además de incluir el robo de tarjetas, comprende otros métodos que se utilizan para capturar los datos de las tarjetas de crédito. Por ejemplo, mediante el skimming (robo de datos en cajeros automáticos para la clonación de tarjetas) y el phishing.[9,10,11]

Los sujetos pasivos, víctimas de esta clase de delitos, pueden ser particulares, empresas, organizaciones gubernamentales, etc.

De un informe reciente presentado por el CERT.AR,[12] se desprende que el phishing sigue siendo la principal amenaza, representando el 75 % de los incidentes reportados en el 2023, observándose una evolución en las técnicas empleadas y ataques más sofisticados a través de las redes sociales.

Ingenieria social

En la página de Interpol puede leerse que "El fraude basado en la ingeniería social abarca todos los métodos utilizados por los delincuentes para explotar la confianza de una persona con el fin de obtener dinero directamente o información confidencial que les permita cometer un delito posterior. Los medios sociales son el canal preferido para ello, aunque no es inusual que el contacto se realice por teléfono o en persona.[13]

Fraudes con tarjetas de crédito

Siguiendo la redacción del art. 173 inc. 15 del C.P, el fraude comprende a las tarjetas de compra, crédito o debido cuando haya sido falsificada, adulterada, hurtada, robada, perdida u obtenida del legítimo emisor mediante ardid o engaño, o mediante el uso no autorizado de sus datos, aunque lo hiciere por medio de una operación automática.

Siguiendo a Donna,[14] la doctrina ha clasificado los fraudes cometidos con tarjetas de crédito o débito en:

1. Pagos mediante presentación de una tarjeta ajena (hurtada, robada o perdida);
2. Pagos mediante la presentación de tarjetas falsas;
3. Utilización de tarjetas en cajeros automáticos.

El tipo exige que la tarjeta haya sido: falsificada (esto es que su emisor nunca la haya confeccionado para la persona que la ostenta, se trata de hacer pasar como genuina una tarjeta que no lo es); adulterada (es decir que materialmente se haya alterado la tarjeta, lo cual supone que exista una genuina y que se le hayan agregado elementos que no lo son); Hurtada, robada (desapoderada ilegítimamente), perdida (esto es que este fuera de la esfera de custodia o disponibilidad de su titular por alguna causa distinta de las mencionadas, ya sea porque la olvidó en por ejemplo en algún comercio, o la extravió); por último contempla que el sujeto la haya obtenido de legítimo emisor mediante ardid o engaño, entendiendo como emisor la entidad bancaria o financiera que emita tarjetas de crédito, por ejemplo falseando su identidad.

El otro supuesto es que a defraudación se hay dado "mediante el uso no autorizado de datos", en este caso no importa la utilización de la tarjeta en forma material, sino de los datos contenidas en ella, lo cual adquiere relevancia al tratarse de operaciones a distancia

Hoy en día es normal realizar compras en la web en la que se solicita al comprador los números de la tarjeta de débito o crédito y el DNI del titular de la misma, no existiendo modo de cotejar que quien realice la compra sea quien figura como titular de la tarjeta.

Finalmente, el artículo menciona "aunque lo hiciere mediante operaciones automáticas", tratándose de aquellas operaciones donde el sujeto no trata con otra persona sino con una máquina, siendo aquí donde más discusiones se dan a nivel doctrinario, por cuanto "no se puede engañar a una máquina".

Dentro de este tipo podemos mencionar por ejemplo el Skiming: que son dispositivos colocados en los cajeros que copian en

forma fraudulenta la banda magnética para luego clonar físicamente la tarjeta.[15] A esta maniobra muchas veces se le agrega la utilización de una cámara o dispositivo que permita filmar u obtener el PIN de la tarjeta y luego con ello poder realizar la maniobra fraudulenta.

Phishing

Podemos definirlo como la capacidad de duplicar una página web a fin de hacerle creer al usuario que está ingresando en la página web original y de esa manera obtener información sensible, como claves, nombres de usuario, números de tarjetas, etc., como así también el envío de correos electrónicos o mensajes de texto falsos que aparentan ser de una institución legítima para obtener datos personales o financieros de la víctima.[16,17,18,19]

En definitiva, es un conjunto de técnicas de ingeniería social que utilizan los ciberdelincuentes para obtener información confidencial de una persona de forma fraudulenta y así apropiarse de la identidad de ese sujeto.

En este caso, "el autor (phishermen) utiliza los medios informáticos para obtener de manera fraudulenta los datos personales del titular de una cuenta bancaria para acceder a ella mediante home backing".[20,21]

Este delito se trata de un fenómeno complejo que requiere una etapa de preparación, esto es la utilización de ingeniería social, la creación de una página web similar a la de la empresa, organización o institución original, necesaria para el fin propuesto, y luego comienza el engaño.

Puede cometerse enviando correos electrónicos simulando ser una entidad bancaria o un organismo o comercio, a fin de que el destinatario acceda al link enviado o complete un formulario y una vez ello, apoderarse de información sensible y de ese modo realizar transferencias o retiros de dinero, a ya sea a una sola cuenta, a varias cuenta o sucesivas transferencias.

Los sujetos activos del delito de phishing, conocidos como phishers, "simulan pertenecer a entidades bancarias de reconocido prestigio y solicitan a los cibernavegantes datos de tarjetas de crédito o claves bancarias, a través de un formulario o un correo electrónico con un enlace que conduzca a una falsa página web con una apariencia similar a la web original".

Una vez obtenida la información, el ciberdelincuente puede o utilizar los datos para realizar por ejemplo una compra en la web aportando los números de tarjetas, claves, usuario etc., que le fuera aportado por la víctima, o bien realizar una transferencia de fondos a otras cuentas que el delincuente pueda tener.

Spear Phishing: es una modalidad de ataque de phishing dirigido a un individuo específico. El objetivo suele ser alguien con acceso privilegiado a datos confidenciales o con determinada autoridad que pueda ser aprovechada por el estafador como por ejemplo un director financiero, un tesorero, etc personas que puedan mover dinero de las cuentas de una empresa.[22]

El ciberdelincuente utiliza la ingeniería social, realiza un estudio del objetivo con el fin de reunir la información necesaria para suplantar o hacerse pasar por una persona o entidad en la que realmente confía (un amigo, un jefe, un colega, un proveedor o una institución financiera de confianza). Mucha de esa información es obtenida de las redes sociales, o páginas profesionales donde las personas felicitan o saludan a sus compañeros o promociona a sus proveedores y tiende a compartir demasiado.

Estos ciberdelincuentes utilizan su investigación para elaborar mensajes con detalles personales específicos, de modo que los hacen parecer muy creíbles para el objetivo.

Pharming

Si bien tiene la misma finalidad del Phishing, en el Pharming no hay un señuelo con el que atraer al usuario a una web en la que robarle sus datos, sino que el pharming lo ataca directamente, accediendo a su ordenador (bien al host o al servidor DNS) y enviándolo directamente a la web en la que se le sustraerá la información (en lugar de darle la opción de clicar, o no, en un enlace).

Es un ataque informático cuyo objetivo es el robo de información sensible. En estos casos, los ciberdelincuentes realizan un ataque DNS con el que consiguen redirigir a los usuarios a una página web falsa, la cual tiene el nombre de dominio oficial, ello a los fines de poder robarles información privada.

En la web del Banco Santander, puede leerse al respecto: "Imagina por un momento que estás en un coche conduciendo por una carretera rumbo a una casa de campo para disfrutar algunos días de vacaciones. Vas siguiendo todas las indicaciones que hay en el camino, incluida una señal que te hace girar a la derecha y que, sin que lo notes, te desvía de tu destino. Entonces, en lugar de llegar a la casa original, terminas en otro sitio sin saber por qué, cómo ocurrió o dónde estuvo el fallo. De esa misma forma, pero en el mundo virtual, funciona el pharming, un fraude que consiste en alterar las páginas web o servidores legítimos para desviar a los usuarios hacia páginas que suplantan las originales con el fin de apropiarse de sus datos personales o de dinero".[23]

Vishing

Fraude en el que el delincuente clona la voz de la víctima y la utiliza para enviar mensajes por WhatsApp solicitando dinero u otro tipo de maniobra fraudulenta.

Scamming

Es uno de los mayores riesgos que enfrentan los usuarios de internet.[24]

Se trata de estafas cometidas a través de internet o por medios electrónicos, generalmente a través de webs fraudulentas, correos electrónicos, redes sociales, perfiles de apps de citas, teléfonos, etc.

A diferencia de otros ciberdelitos aquí el Scammer no requiere ser un hacker ni tener amplios conocimientos informáticos, porque lo que generalmente hace es uso de la ingeniería social para engañar a sus potenciales víctimas.

El objetivo de los ciberdelincuentes es engañar al usuario para obtener algún fin, generalmente obtener dinero de su víctima

bajo el pretexto de ofrecer una recompensa mayor. Generalmente, ofrecen oportunidades de viajes, premios, préstamos, donaciones, loterías, ofertas, cursos, promociones, becas, y de esa manera logran convencer al usuario que proporcione sus datos personales, números de cuentas, etc.[15]

Hay distintos tipos de scamming pudiéndose mencionar entre las más comunes:

El Romance Scam

Se da a través de las webs de citas. En este caso el estafador se hace pasar por una persona falsa, entabla una relación de confianza con otra persona – la victima- hasta que logra que ésta tenga sentimientos amorosos, y una vez que obtiene la dependencia emocional de la víctima, le solicita dinero por ejemplo para poder comprar los pasajes para viajar al país y conocerse personalmente, o refiriendo tener problemas económicos. Se trata de una de las estafas más peligrosas porque al estar vinculada sentimentalmente la víctima, no advierte haber sido estafada hasta que entregó grandes sumas de dinero.

Este tipo de ciberdelincuencia no es algo reciente, sino que viene desarrollándose desde el surgimiento de Internet. Al principio los estafadores actuaban a través de las salas o foros de chat, o a través de correos electrónicos con la finalidad de lograr que una víctima le entregara dinero. Ahora los métodos han evolucionado, con grandes organizaciones fraudulentas, con técnicas complejas, a través de perfiles falsos o con fotografías retocadas o con la obtención e información de relevancia para la víctima, haciendo del uso de la ingeniería social un elemento clave para cometer esta clase de delitos.

Ofertas de empleo

Aquí el delincuente utiliza la desesperación de la víctima por tener una fuente de ingresos, ofreciéndole un trabajo falso y a cambio le solicita que deposite dinero a los fines de adquirir por ejemplo material de trabajo o incluso que deposite una pequeña suma para poder ingresar a formar parte de la "empresa".

Alquiler inmobiliario

La forma es similar a la de la oferta de trabajo falsa, pero aquí el delincuente publica el alquiler de una propiedad, una vez que entra en contacto con la victima le envía fotos de la vivienda, indicaciones del lugar, etc, y a cambio de la reserva le solicita a la víctima un depósito de dinero. Luego cuando la víctima se constituye en el lugar no encuentra la vivienda, ni puede ubicar al supuesto locador.

Estafa nigeriana o timo nigeriano

Es muy frecuente, en estos supuestos se llama por teléfono a la víctima o se le envía un mail, diciéndole que tiene una gran suma de dinero para cobrar por ejemplo de una herencia o por alguna resolución judicial, y que para recibirla debe pagar un adelanto.

Utilización de la Inteligencia Artificial para cometer estafas a través de la ingeniería social

Con el avance de la IA las técnicas utilizadas por los ciberdelincuentes se han vuelo más sofisticadas para lograr manipular a las personas y hacer que estas revelen información confidencial, ello con resultado efectivo. Dentro de estos supuestos se pueden mencionar:

Phishing: Así la IA puede analizar datos de las redes sociales y crear correos electrónicos de phishing muy convincentes, dirigidos a individuos específicos.

Así también, se pueden utilizar herramientas de inteligencia artificial generativa para crear mensajes de phishing. Las características de estas herramientas es que permite crear o generar mensajes de textos o correos electrónicos personalizados, que carezcan de errores gramaticales o de cualquier otra señal de alarma o sospecha habitual en los casos de suplantación de identidad.

A su vez, la IA generativa también puede ayudar a los estafadores a ampliar sus operaciones. Según el Indice X- Force Trheat Inteligence de IBM, un estafador tarda 16 horas en crear un correo electrónico de suplantación de identidad de forma manual. Con la IA, los estafadores pueden crear mensajes aún más convincentes en solo cinco minutos.

Los estafadores también utilizan generadores de imágenes y sintetizadores de voz para dar más credibilidad a sus estafas. Por ejemplo, en 2019, unos atacantes utilizaron la IA para clonar la voz del director general de una empresa energética y estafar 243 000 dólares a un director de banco.[25]

Deepfakes y suplantación de identidad: los deepfakes son videos, imágenes y/o archivos de voz que para parecer reales y auténticos son manipulados con software de inteligencia artificial y son utilizados por los ciberdelincuentes para extorsionar o manipular a las víctimas o realizar fraudes.

Chatbots maliciosos: que interactúan con las víctimas de manera de poder obtener datos sensibles.

Exploración de vulnerabilidades, ya que la IA puede detectar rápidamente fallos en el software y las redes, que los atacantes pueden explotar antes de que se solucionen.

Robo, usurpación o suplantación de identidad

Se trata de aquellos hechos en que los delincuentes utilizan los datos personales para hacerse pasar por otra persona al que le han robado su identidad.

Estos robos sumados al anonimato de las transacciones en línea, son utilizados para cometer distintos tipos de delitos desde fraudes hasta actos terroristas, entre las más importantes y actuales se pueden mencionar: fraude bancario, la extorsión en línea, blanqueo de dinero.[26]

https://doi.org/10.62486/net202476

Este delito se puede llevar a cabo a través del robo, perdida o fotocopiado del DNI e incluso con la obtención de datos personales que se pueden obtener de distintos lugares.

En términos digitales, el robo de la identidad digital, ya sea en internet o en redes sociales, se produce o bien suplantando la identidad digital de un usuario de Internet y redes sociales, o robando sus claves y contraseñas para acceso a las mismas, con fines generalmente, delictivos.[27]

El robo de identidad no está tipificado en nuestro ordenamiento jurídico como un delito específico, por lo que hay que recurrir al tipo general de defraudación. No obstante, se han presentados distintos proyectos de Ley al Congreso Nacional.

La identidad es aquel conjunto de rasgos propios de un individuo que lo caracteriza frente a los demás, entendiendo a la identidad digital como una manifestación de la identidad en la vida virtual en el ciberespacio.

En virtud de ello el bien jurídico tutelado en este tipo delictivo es la identidad y por lo tanto la dignidad e intimidad.

El robo de identidad digital puede ocurrir de diversas maneras, aunque los elementos básicos y la finalidad son los mismos: la obtención de información personal para realizar algún tipo de perjuicio.

La suplantación y usurpación de identidad tienen en común la manipulación indebida de la identidad de una persona sin su consentimiento y que el delincuente busca algún tipo de beneficio a través del engaño, pudiendo sufrir las víctimas, perjuicios financieros, emocionales e incluso a su reputación. Sin embargo, existen alunas diferencias entre ellos.[28,29]

La principal diferencia es que la suplantación se centra en la imitación superficial como por ejemplo usar el nombre o la imagen de alguien en línea; en tanto que, en la usurpación, hay una apropiación completa y continuada de la identidad, haciendo que su planificación y ejecución sea más compleja.

Esta conducta, suele ser la antesala o el primer eslabón, para la comisión de algunas actividades ilícitas que sí están castigadas penalmente, como es el caso de fraudes y delitos contra la integridad sexual como el grooming.

Sin embargo, esa conducta per se, no constituye delito, en tanto y en cuanto se trataría de un acto preparatorio de otro delito.

Estafa Piramidal y Esquema Ponzi

Las estafas piramidales y los esquemas Ponzi tienen puntos en común, y también algunas diferencias. En ambos casos, se trata de reclutar cada vez más participantes para lograr las ganancias que prometen.

Tienen su origen en un hecho delictivo que tuvo lugar en EEUU en la década de 1920, en el que un italiano llamado Carlo Ponzi, inició una empresa que prometía a sus clientes un 50 % de rentabilidad dentro de un plazo de 45 días, o 100 % dentro de 90 días. Lo interesante de la propuesta estaba en que estas ganancias se daban con el simple hecho de comprar cupones postales descontinuados en otros países y redimiéndolos a su valor nominal en los Estados Unidos.

Este esquema ideado por Carlo Ponzi no dependía realmente tal como afirmaba del comercio de cupones, sino que los rendimientos para los primeros inversores se pagaban con el dinero de los nuevos inversores.[30]

Con esta propuesta de altos rendimientos, Ponzi atrajo a machismos inversores, pues más conocido se hacía mayor era la cantidad de personas que invertían y aún más se propagaba el fraude.

Ponzi atrajo a miles de personas con la promesa de rendimientos extraordinarios, y mientras más personas invertían, más se propagaba su fraude.

Al principio todo funcionaba o al menos parecía funcionar normal, sin embargo, a medida que se iban sumando personas al fraude, las obligaciones de pago aumentaban, por lo que se requería de más dinero para poder cumplir con las promesas realizadas.

Finalmente, en 1920, el esquema colapsó y Ponzi terminó siendo arrestado, juzgado y condenado por fraude.

En el año 2013, ya con la aparición de las criptomonedas, en EEUU, la Comisión de Mercado de Valores (S.E.C.) presentó la primera demanda civil en contra de Trendon T. Shavers, también conocido como “Pirateat40” y su compañía Bitcoin Savings and Trust.

La maniobra de Shavers es conocida como el primer esquema Ponzi en el mundo cripto, él lo que hacía era prometer a los inversores grandes ganancias, de hasta un 7 % semanal, comprando bitcoin a bajo precio y vendiéndolos a un precio más alto en el mercado. Obviamente ello atrajo a muchos inversores.

Sin embargo, ese dinero no lo invertía, ni realizaba las actividades comerciales de bitcoin que prometía, sino que usaba el dinero de los nuevos inversores para pagar a los antiguos. Cuando dejó de poder pagar a todos, la estafa colapsó, dejando pérdidas estimadas en más de 700 000 bitcoins. Este caso marcó el inicio de una serie de fraudes similares en el mundo cripto y en el mundo entero.

¿En qué consiste una estafa piramidal? es un esquema de negocios que se presenta como una oportunidad para obtener un gran retorno económico, se les hace creer que van a formar parte de un atractivo modelo de negocios, en el que van a duplicar o triplicar sus inversiones en poco tiempo. Para formar parte, deben hacer una inversión de dinero y se los alienta a captar nuevos inversionistas que quieran formar parte de esta red.

La cuestión se centra en que el negocio es una fachada, en realidad no existe tal negocio, y con el dinero que ingresa de los nuevos participantes, se les paga a los inversores más antiguos, haciéndoles creer que todo funciona a la perfección. Se le dice “piramidal” porque son pocos los que reciben dinero, mientras que los que están en la base de la pirámide son los que se ven damnificados.

Algunas de estas estafas son conocidas bajo nombres como la “Flor de la Abundancia”, “Mandala de la Prosperidad”, “Telar de los Sueños”, “Ruedas de amistad” entre otros. Todas ellas prometen ingresos rápidos y elevados a cambio de un aporte inicial.

Este modelo se relaciona con el “esquema Ponzi”, que es otro sistema fraudulento que solo se diferencia por un solo detalle: que sí se invierte en algo.

En lo que concierne a nuestro país en el año 2022 comenzó a tener difusión en los medios de comunicación el Grupo Zoe, el que era presentado como una entidad que combinaba coaching, educación y servicios financieros, y otro en el que daban cuenta

del gran crecimiento el grupo al punto de lanzar la criptomoneda Zoe Chash, la ONG BITCOIN ARGENTINA, realizó la denuncia en contra del CEO de la Generación Zoe, Leonardo Positorto, por los delitos de estafa, intermediación financiera no autorizada, y captación ilegal.

La maniobra del Grupo consistía en que:

1. Promocionaban que la criptomoneda Zoe Cash como inversión que estaba respaldada por oro, lo cual no era cierto
2. Ofrecían programas de coaching con promesas de ganancias exorbitantes, con lo que atraían una gran cantidad de inversores con falsas expectativas
3. Promovían inversiones a través de un fideicomiso que no tenía autorización ni del Banco Central ni de la Comisión Nacional de valores.
4. Utilizaban el logo de la comisión Nacional de valores, haciendo creer que tenían el respaldo o autorización del organismo
5. Realizaban publicaciones engañosas en medios de comunicación y redes sociales promoviendo a Zoe Cash como una inversión de alto rendimiento.
6. Funcionaba como esquema Ponzi, porque el dinero ingresado era utilizado no para invertir sino para pagar a los viejos inversionistas

Tanto la estafa piramidal como el sistema de esquema Ponzi son delitos que se encuentran tipificados en los artículos 309 y 310 del Código Penal, que pena el delito de intermediación financiera no autorizada.

Encuadre Legal

Una vez establecida la modalidad delictual de estas nuevas conductas, queda por definir en que figura delictiva encuadrarían los hechos y, a falta de una legislación específica, llegado el punto deberá optarse entre las figuras de Hurto o estafa.

Al respecto se alzan voces a favor y en contra.

Así si tenemos en cuenta una clásica maniobra de phishing en la que una persona utilizando los datos de otra realiza una compra por mercado libre, por ejemplo, donde los datos son registrados por una máquina, aquí no hay una estafa por cuanto la máquina no puede ser engañada, o en los casos en que se accede a home banking con los datos de otra persona, aquí tampoco hay error, engaño ni disposición patrimonial.

Ahora bien, con la reforma de la Ley 26.388 se incluyó el art. 173 inc. 16 del C.P., como un caso especial de defraudación, contemplando el supuesto cuando la maniobra se lleve a cabo "mediante cualquier técnica de manipulación informática que altere el normal funcionamiento de un sistema informático o la transmisión de datos."

A los fines del análisis del tipo debemos remitirnos a la figura básica contemplada en el art. 172 del C.P. esto es, ardid o engaño, error, acto de disposición patrimonial perjudicial. No obstante, se advierte que en primer lugar para la configuración del tipo delictual la norma exige la alteración del normal funcionamiento de un sistema informático o de transmisión de datos.

Pero si tenemos en cuenta la maniobra desplegada por los sujetos activos de estos delitos, esto es, el envío de un correo electrónico simulando ser una empresa, entidad bancaria, etc. que induzca al error de la víctima, la cual facilita datos sensibles, los que luego serán utilizados por el delincuente a los fines de apoderarse del dinero de la víctima, aquí no hay una alteración del normal funcionamiento de un sistema informático, e incluso la víctima no realizo una disposición patrimonial, porque es el propio sujeto activo el que utiliza las credenciales para hacerse luego el dinero, con lo cual para configurase este tipo especial de defraudación alcanzaría con sólo tres elementos típicos: ardid o engaño, error y disposición patrimonial perjudicial.

Distinta es la situación del phishing a través de malware, en el que el sujeto activo implanta en el sistema de la víctima un virus o un troyano de manera de poder sustraer información o hacerse de las claves de acceso.

La suplantación de identidad digital es otra actividad que en la actualidad no se halla tipificada en derecho argentino no obstante los diversos proyectos que se encuentran pendientes de tratamiento parlamentario.

Se trata de aquellas conductas en las que se utilizan el nombre y apellido, fotografías o imágenes para crear un perfil ya sea en alguna red social o en alguna página web, para hacerse pasar por la persona que se señala ser o cuya imagen se muestra.

Dicha conducta puede perseguir distintos propósitos ya sea en casos de grooming, o en casos de fraudes como el romance scam – entre otros- o incluso para cometer calumnias e injurias, no obstante, y hasta tanto se pueda llegar a determinar cuál es el propósito el delincuente quedará como acto preparatorio.

A nivel nacional ninguna de estas conductas está penalizada como delito autónomo. Sólo en la Ciudad Autónoma de Buenos Aires se encuentra regulada en el Código Contravencional:

- Art. 64 CC: Suministro de material pornográfico a menores de edad a través de medios informáticos.
- 71 bis CC: Difusión no autorizada de imágenes o grabaciones íntimas. La víctima pudo haber consentido la obtención de dichas imágenes en un espacio privado, pero NO su distribución masiva.
- 71 quinquiés CC: Suplantación digital de identidad. Son los casos en los que el ciberagresor crea un perfil digital falso haciéndose pasar por la víctima y, a través de aquel, comete otros delitos en nombre ajeno.

Cibermulas: Participes, encubridores o víctimas

En esta relación de victima-delincuente, viene a sumarse la figura de las cibermulas. Que son personas que muchas veces sin saberlo, brindan su cuenta bancaria a fin que se les deposite o realicen transferencias con el dinero obtenido del ciberfraude.

En varios casos estas personas son contactadas a través de una oferta laboral, en la que se los "contrata" para realizar tareas de

https://doi.org/10.62486/net202476

intermediación comercial, y para lo cual deberán tener una cuenta bancaria a la cual le harán trasferencias y desde la cual realizará transferencias o retirará el dinero a los fines de entregárselo al phisher, es decir son tareas sencillas a cambio de una suma de dinero.

Ahora bien, desde el punto de vista jurídico se plantea la duda de si estamos ante un encubridor o un participe.

Quienes sostienen que la conducta de las cibermulas encuadra en la figura prevista en el art. 277 inc. 1 ap. C, del C.P., consideran que presta una ayuda posterior a los autores del fraude.

Para otros, en cambio, la mula recibe dinero proveniente de un ilícito penal y le da apariencia de origen lícito, quedando comprendida su conducta en el blanqueo de capitales (art. 303 del C.P.)

La mayoría de la doctrina entiende de que en realidad se está en presencia de participes necesarios del fraude, ya que su actuación favorece la comisión del delito el que no habría podido llevarse a cabo ni consumarse sin su participación.

Así lo ha sostenido la Sala 7 de la Cámara Nacional de Apelaciones en lo Criminal y Correccional de la Ciudad autónoma de Buenos Aires, en su fallo del 2/11/22, en el que confirma el procesamiento del imputado en orden al delito de estafa, acusado de aportar su cuenta bancaria para recibir dinero de origen fraudulento, para transferirlo inmediatamente a otras cuentas, dado que el aporte de una cuenta bancaria como destino intermedio o conclusivo de la transferencia de dinero electrónico obtenido mediante cualquier forma de fraude sirve para la consumación material del ilícito penal. (Magistrados: Mariano A. Scotto - Juan Esteban Cicciaro - Id SAIJ: FA22060033)

Derecho comparado

Algunos de los países que han sido pioneros en la lucha contra las ciberestafas y cuentan con legislaciones robustas incluyen:

Estados Unidos

Con una economía altamente digitalizada, Estados Unidos posee una gran cantidad de leyes federales y estatales para combatir el cibercrimen.

Así, en 1988 aprobó la Ley Usurpación de Identidad, penalizando hasta con 15 años de prisión la conducta de aquel sujeto que utilice ilegalmente un medio de identificación de otra persona para la realización de cualquier actividad ilegal. Dicha conducta es considerada un crimen federal.

También su Ley de Fraude Informático y Abuso (CFAA, por sus siglas en inglés), que castiga una amplia gama de delitos informáticos, incluyendo las ciberestafas, resultando pionero en la materia.

Atención especial merece la denominada "Anti Phishing Act" del Estado de New York, la cual sanciona penalmente a cualquier persona que, valiéndose de medios electrónicos, solicite, requiera o colecte información personal para representar de manera engañosa a una empresa u organismo del gobierno, sin la debida autorización para ello.

Japón

Con una fuerte tradición en la protección de la privacidad, ha implementado leyes específicas para combatir las ciberestafas.

En el año 2000, se aprobó la Ley sobre la Prohibición de Actos de Acceso Ilegal", la que consta de 14 artículos, estableciendo en el art. 1 su objetivo de prevenir el cibercrimen y mantener el orden de las telecomunicaciones.

Esta Ley hace referencia al acceso no autorizado a la computadora de otra persona haciendo foco en la suplantación de identidad, de igual manera prohibe la acción de obtener, almacenar o solicitar de manera ilegal los códigos de identificación (ID, contraseña) de otra persona.[31]

Países de la Unión Europea

La UE ha adoptado una serie de directivas y regulaciones para armonizar las leyes nacionales en materia de ciberseguridad y cibercrimen de sus países miembros. En el año 2023 entró en vigor la nueva Ley de Servicios Digitales[32] (DSA) de la Unión Europea por medio de la cual las 19 mayores grandes plataformas digitales operativas en territorio europeo, entre ellas Facebook, Instagram, TikTok o X (antiguo Twitter), pero también para los gigantes comerciales intermediarios como Amazon, Zalando o AliExpress deben tener sistemas que les permitan señalar y retirar contenidos ilegales de manera más rápida, para lo que deberán contar con mecanismos para que los usuarios alerten de contenidos ilícito, pudiendo ser sancionadas con grandes multas en caso de incumplimiento.[33]

De esta manera la Unión Europea se convirtió en la primera región en el mundo en regular la actividad de las plataformas on line y a partir de febrero de 2024 aplicó dichos principios al resto de las plataformas en línea independientemente del que sea su tamaño.

Dentro de lo que es la Comunidad Europea, en España, la reforma del Código Penal efectuada por la Ley Orgánica 14/2022, de 22 de diciembre, tipifica por separado las estafas comunes de las conductas de ciberestafas que requieren de la manipulación del sistema informático o la utilización de una tarjeta de débito y/o crédito, a las que considera delitos de propia actividad.

Dentro del Derecho Penal Español, el phishing es un delito novedoso, que está encuadrado en diversos tipos delictivos, dependiendo de las circunstancias y daño causado.[34]

El phishing es considerado una forma de estada, encontrándose regulado en el art. 249 del Código Penal Español, castigado con penas de prisión que van de 6 meses a 3 años, dependiendo de la forma de realización, a quienes: Manipulen sistemas informáticos o datos para obtener transferencias no consentidas; usen fraudulentamente tarjetas, cheques de viaje u otros instrumentos de pago, a quienes fabriquen, posean, o distribuyan herramientas para cometer estafas o adquieran cheques o tarjetas ilegalmente.[35]

En el caso que el phishing incluya el uso indebido de la identidad de otra persona, podría encuadrar en el delito de usurpación de identidad, cuya pena oscila de 6 meses a 3 años de prisión.

https://doi.org/10.62486/net202476

Sin embargo, pareciera que dichas modificaciones no resultan suficientes a los fines de la prevención. Así el Diario El País de España publicó el 10/3/24 que más de la mitad de los ciudadanos españoles habrían resultado víctimas de estos delitos, siendo los más frecuentes los "románticos o de inversiones, resultando ser el segundo delito más denunciado luego del hurto.[36]

Alemania: En dicho país, las conductas cibercriminales, están reguladas en distintos cuerpos legales.

Así, el Código Penal tipifica varias conductas, entre ellas: espionaje e interceptación de datos (art. 202a-c StGB), fraude informático (art. 263a StGB), sabotaje informático (art. 303b StGB) y modificación de datos (art. 303a StGB), penalizándose también los los actos preparatorios, como la producción o adquisición de programas informáticos cuyo objeto sea la comisión de fraude informático (art. 202c StGB). El manejo descuidado de las contraseñas también puede dar lugar a la iniciación de procedimientos preliminares.

El hacking constituye un delito penal según las secciones 202a y 202b del Código Penal, llamados espionaje de datos e interceptación de datos (phishing), respectivamente: Respecto de una conducta preparatoria para los delitos de espionaje de datos y phishing, el artículo 202c CP sanciona la fabricación, venta y adquisición con el fin de utilizar, distribuir o poner a disposición de otro modo un dispositivo, incluidos los programas informáticos, que se diseñaron o prepararon principalmente con el fin de cometer determinados ataques cibernéticos

La usurpación de identidad puede dar lugar a diversas figuras delictivas, dependiendo de cómo el delincuente obtenga acceso a la información de datos. Si es mediante métodos de phishing, queda comprendido en el supuesto del artículo 202b CP, ya mencionado. Si lo es mediante el uso de dichos datos de identidad con fines fraudulentos, podría dar lugar a los delitos de fraude o fraude informático, con penas de entre 5 a 10 años de prisión en casos graves. El uso de la identidad de otra persona puede dar lugar a los delitos de falsificación de documentos o de falsificación de datos con valor probatorio.

Además, cuenta con la Ley Federal de Protección de Datos, la Ley de Derechos de Autor, la Ley de Derechos de Autor de Arte, la Ley Alemana de Telemedios y la Ley de Competencia Desleal (UWG).[37]

CONCLUSIONES

El análisis de las nuevas formas de ciberestafas en Argentina revela una preocupante realidad: la legislación actual no está completamente preparada para enfrentar estos desafíos modernos. A pesar de que el Código Penal argentino contempla delitos informáticos, la rápida evolución de las técnicas de fraude en línea supera a menudo las medidas preventivas y punitivas existentes. Los ciberdelincuentes aprovechan las herramientas de inteligencia artificial y otras tecnologías avanzadas para llevar a cabo estafas sofisticadas.

A lo largo del trabajo se ha podido evidenciar, el perjuicio que esta clase de delitos provoca no sólo en las víctimas, sino también a empresas, instituciones e incluso al Estado por lo que resulta imperiosa la necesidad de tipificar no sólo el phishing, sino también la suplantación de identidad, y la recolección de información personal, dando trámite a los diversos proyectos presentados en el Congreso.

Es necesario poder plantear una reforma profunda y seria del Código Penal en lo que hace al tema de las plataformas digitales, criptomonedas y ciberdelitos para poder implementarlo en los procesos e investigaciones, ya sea a través de la creación de tipos específicos como también la incorporación como agravante del "uso de las redes sociales" para la comisión de determinadas clases de delitos.

La inclusión de una cláusula general en el Código Penal que establezca una agravante para todos los delitos cuando se utilizan las redes sociales para cometerlos, permitiría una mayor flexibilidad y adaptabilidad a las nuevas modalidades delictivas.

Por otro lado, también resulta evidente la necesidad de ampliar la protección de los sistemas informáticos, y datos personales, tipificando como delitos los ataques cibernéticos, el robo de identidad y la extorsión informática.

Como se ha podido ver, las ciberestafas tienen penas infimas comparadas con los perjuicios que provocan en la vida de las personas como en las instituciones.

Sin embargo, la sola modificación de las leyes, si bien es un gran paso, no alcanza. Es importante capacitar a quienes abordan estos delitos para que tengan las herramientas necesarias para combatirlos

La implementación de estas reformas plantea diversos desafíos, entre los que se destacan:

- Es necesario encontrar un equilibrio entre la protección de la libertad de expresión y la necesidad de combatir los delitos cometidos a través de las redes sociales.
- Las tecnologías de la información evolucionan rápidamente, por lo que las normas penales deben ser lo suficientemente flexibles para adaptarse a estos cambios.
- Es fundamental garantizar la protección de los datos personales de los usuarios de internet, al tiempo que se permite la investigación de los delitos.
- Se requiere una estrecha colaboración entre el Poder Judicial, el Poder Legislativo, las fuerzas de seguridad y las empresas tecnológicas para combatir la cibercriminalidad.

En conclusión, la tipificación de agravantes en delitos cometidos a través de redes sociales es un tema complejo que requiere un análisis profundo y un debate amplio.

La ciberestafa es una amenaza creciente que afecta a individuos, empresas y estados. Para combatirla de manera efectiva, es necesario un enfoque multidisciplinario que involucre a gobiernos, empresas, organizaciones de la sociedad civil y a cada uno de nosotros como ciudadanos.

https://doi.org/10.62486/net202476

FINANCIACIÓN

Los autores no recibieron financiación para el desarrollo de la presente investigación.

CONFLICTO DE INTERESES

Los autores declaran que no existe conflicto de intereses.

CONTRIBUCIÓN DE AUTORÍA

Conceptualización: Sabrina Ivana Bof.
Curación de datos: Sabrina Ivana Bof.
Análisis formal: Sabrina Ivana Bof.
Investigación: Sabrina Ivana Bof.
Metodología: Sabrina Ivana Bof.
Administración del proyecto: Sabrina Ivana Bof.
Recursos: Sabrina Ivana Bof.
Software: Sabrina Ivana Bof.
Supervisión: Sabrina Ivana Bof.
Validación: Sabrina Ivana Bof.
Visualización: Sabrina Ivana Bof.
Redacción – borrador original: Sabrina Ivana Bof.
Redacción – revisión y edición: Sabrina Ivana Bof.

REFERENCIAS BIBLIOGRÁFICAS

1. Unidad Fiscal Especializada en Ciberdelincuencia. Informe de gestión 2023. Disponible en: https://www.fiscales.gob.ar/ciberdelincuencia/la-unidad-fiscal-especializada-en-ciberdelincuencia-senalo-un-alza-continua-de-los-delitos-informaticos-en-su-informe-de-gestion-2023

2. Bekerman U. Ciberseguridad en Argentina: la protección de las infraestructuras críticas. En: Sistema Penal e Informática. Tomo 4. Buenos Aires: Hammurabi; 2021. p. 35–50.

3. Ministerio de Seguridad de la Nación. Ciberdelito: aprobación del Segundo Protocolo Adicional del Convenio de Budapest. Disponible en: https://www.argentina.gob.ar/noticias/ciberdelito-se-aprobo-el-texto-del-2deg-protocolo-adicional-del-convenio-de-budapest

4. Código Penal Argentino. Disponible en: https://www.argentina.gob.ar/normativa/nacional/ley-11179-16546/texto

5. Centro de Ciberseguridad del Gobierno de la Ciudad de Buenos Aires. Delitos y contravenciones en el mundo digital: las normas que nos amparan. 2024 may. Disponible en: https://buenosaires.gob.ar/sites/default/files/2024-05/B4_Delitos%20y%20contravenciones%20en%20el%20mundo%20digital.pdf

6. Roibón MM. La estafa informática en el Código Penal. 2019. Disponible en: https://www.pensamientopenal.com.ar/system/files/2019/01/doctrina47322.pdf

7. Peña M, Lofeudo I. Fraudes: cuáles son las modalidades de ciberdelitos más habituales. Infobae. 2023 sep 21. Disponible en: https://www.infobae.com/opinion/2023/09/21/fraudes/

8. Ministerio de Seguridad de la Provincia de Buenos Aires. Cibercrimen y delitos informáticos: guía de estudio 2. 2021. Disponible en: https://www.mseg.gba.gov.ar/areas/Vucetich/GUIAS%20DE%20MATERIAS%202021/2%20Cibercrimen.pdf

9. Ministerio Público Fiscal de la Ciudad Autónoma de Buenos Aires. Delitos informáticos. 2018 mar 9. Disponible en: https://mpfciudad.gob.ar/tematicas/2020-03-09-18-42-38-delitos-informaticos

10. Ministerio de Justicia de la Nación. Qué es el ciberdelito. Disponible en: https://www.argentina.gob.ar/justicia/convosenlaweb/situaciones/que-es-el-ciberdelito

11. Brodowski D, Linares MB. Los delitos informáticos en el Código Penal Argentino. En: Cibercrimen y protección de la seguridad informática. Buenos Aires: Ad-Hoc; 2021. p. 155–91.

12. CERT.ar. Incidentes informáticos. Informe anual de incidentes de seguridad registrados en 2023. Dirección Nacional de Ciberseguridad; 2024. Disponible en: https://www.argentina.gob.ar/jefatura/innovacion-publica/ssetic/direccion-nacional-ciberseguridad/informes-de-la-direccion-7

13. Interpol. Fraudes basados en la ingeniería social. Disponible en: https://www.interpol.int/es/Delitos/Delincuencia-financiera/Fraudes-basados-en-la-ingenieria-social

14. Donna EA. Derecho penal: parte especial. Tomo II-B. 2ª ed. Santa Fe: Rubinzal-Culzoni; 2012.

15. Martínez M. Algunas cuestiones sobre delitos informáticos en el ámbito financiero y económico: implicancias y consecuencias en materia penal y de responsabilidad civil. En: Cibercrimen y delitos informáticos. Buenos Aires: Errepar; 2018. p. 33–47.

16. Petrone D, Basso M, Emiliozzi A. Phishing attacks: problemáticas de su recepción en el ordenamiento local y nuevos desafíos. En: Cibercrimen: aspectos del derecho penal y procesal penal. Buenos Aires: IBdeJF; 2017.

17. Luján S. El problema de phishing en Argentina. Infobae. 2024 jul 1. Disponible en: https://www.infobae.com/opinion/2024/07/01/el-problema-de-phishing-en-argentina/

18. Departamento de Ciberdelitos y Tecnologías Aplicadas de la SPC. Ciberseguridad, phishing y estafas digitales. Disponible en: https://www.mpba.gov.ar/phishing

19. Bisquert SO. La figura del "phishing" como modalidad delictiva: problemática en cuanto a su encuadre jurídico. 2006. Disponible en: http://www.saij.gob.ar/doctrina/dacf060096-bisquertfiguraphishingcomomodalidad.htm

20. Aboso G. Cibercriminalidad y delitos contra la propiedad. En: Sistema Penal e Informática. Tomo 4. Buenos Aires: Hammurabi; 2021. p. 241–305.

21. Aboso G. Ciberdelitos: análisis doctrinario y jurisprudencial. Buenos Aires: elDial Libros; 2022.

22. Instituto Nacional de Ciberseguridad (INCIBE). Spear-phishing. Disponible en: https://www.incibe.es/aprendeciberseguridad/spear-phishing

23. Santander. "Pharming": otro motivo para detenerse y pensar antes de hacer clic. 2022 sep 12. Disponible en: https://www.santander.com/es/stories/pharming

24. Grupo Ático 34. El scamming o los peligros de las estafas por internet. Disponible en: https://protecciondatos-lopd.com/empresas/scamming/

25. IBM. ¿Qué es el phishing? Disponible en: https://www.ibm.com/es-es/topics/phishing

26. Saij. G. R. M. s/ Procesamiento. Estafa. Disponible en: http://www.saij.gob.ar/camara-nacional-apelaciones-criminal-correccional-nacional-ciudad-autonoma-buenos-aires--procesamiento-estafa-fa22060033-2022-1102

27. Secretaría de Innovación Tecnológica del Sector Público. Delitos informáticos en Argentina: modalidades detectadas durante la pandemia COVID-19. Recomendaciones preventivas para los ciudadanos. 2022. Disponible en: https://www.argentina.gob.ar/sites/default/files/2022/04/ciberdelitos_en_pandemia.pdf

28. Defensa del Consumidor. Cuadernillos COFEDEC. Disponible en: https://www.argentina.gob.ar/produccion/defensadelconsumidor/cuadernilloscofedec

29. Departamento de Delitos Tecnológicos de la Policía Federal Argentina. Denunciar un delito informático. Disponible en: https://www.argentina.gob.ar/servicio/denunciar-un-delito-informatico

30. Ámbito Financiero. Quién fue Carlo Ponzi, uno de los estafadores más famosos de la historia. 2024 oct 12. Disponible en: https://www.ambito.com/economia/quien-fue-carlo-ponzi-unolos-estafadores-mas-famosos-la-historia-n6069767

31. Toki K. Acciones prohibidas bajo la Ley Japonesa de Prohibición de Acceso No Autorizado. 2024 mar 21. Disponible en: https://monolith.law/es/it/unauthorized-computer-access

32. Centro Europeo del Consumidor de España. Noticias: Ley de Servicios Digitales. 2023 ago 25. Disponible en: https://cec.consumo.gob.es/CEC/comunicacion/noticias/2023/NI_Ley_De_Servicios_Digitales_25_08_2023.htm

33. Ayuso S. La UE pone coto a las grandes plataformas: empieza a aplicarse la nueva Ley de Servicios Digitales. El País. 2023 ago 25. Disponible en: https://elpais.com/economia/2023-08-25/la-ue-pone-coto-a-las-grandes-plataformas-empieza-a-aplicarse-

la-nueva-ley-de-servicios-digitales.html

34. Sunkel & Paz. Phishing en España: ¿qué es y cómo se castiga este delito en el derecho penal?. 2024. Disponible en: https://www.sunkel-paz.es/post/phishing-en-espana-que-es-como-se-castiga

35. Abogacía Española, Consejo General. Delitos en internet: ciberestafas. Disponible en: https://www.abogacia.es/actualidad/opinion-y-analisis/delitos-en-internet-ciberestafas/

36. Pérez-Colomé J. Las ciberestafas ya son el segundo delito más denunciado: nadie está a salvo de caer en la trampa. El País. 2024 mar 10. Disponible en: https://elpais.com/tecnologia/2024-03-10/las-ciberestafas-ya-son-el-segundo-delito-mas-denunciado-nadie-esta-a-salvo-de-caer-en-la-trampa.html

37. Weidenslaufer C, Juan Pablo, Cifuentes P. Jurisdicción y ciber-delitos. Biblioteca Nacional del Congreso de Chile; 2022 nov. Disponible en: https://obtienearchivo.bcn.cl/obtienearchivo?id=repositorio/10221/33744/1/BCN_jurisdiccion_ciber_delitos_CW_JPC_PC_2022.pdf