EL TRATAMIENTO DEL FRAUDE INFORMÁTICO: UN ESTUDIO DEL DERECHO COMPARADO ENTRE PERÚ Y ESTADOS UNIDOS

DOI: https://doi.org/10.53870/lvj.390

Gloria María Armestar Bruno[1]
Universidad Antonio Ruiz de Montoya
https://orcid.org/0000-0003-1285-1657
gloria.armestar@uarm.pe

Fátima Lucía Toche Vega[2]
Pontificia Universidad Católica del Perú
https://orcid.org/0000-0002-1984-4954
fatimatoche@gmail.com

RESUMEN

El aumento del uso de las tecnologías de la información y la comunicación (TIC), en todos los ámbitos de la economía, ha desafiado al Derecho Penal con la aparición de nuevos delitos, modalidades delictivas o medios para la comisión de estos, lo cual conduce a que los gobiernos adopten regulaciones para mitigar riesgos y modernicen su legislación. Actualmente, han aumentado los delitos informáticos en la banca peruana a través de actividades ilegales en línea, de los cuales el más común es el fraude informático en sus modalidades *phishing, sim swapping* y ataques cibernéticos.

La creciente digitalización de los servicios financieros debe ofrecer seguridad a los clientes para motivarlos a utilizar los productos bancarios. Por ello, los bancos deben implementar monitoreos constantes de transacciones y preocuparse por

1 Candidata a doctor en Derecho por la Universidad San Ignacio de Loyola. Abogada por la Pontificia Universidad Católica del Perú, Magíster en Derecho Civil por la Universidad Inca Garcilaso de la Vega. Amplia experiencia en el área de Derecho Empresarial, Derecho Civil y Derecho Financiero. Actualmente se desempeña como jefa del Departamento de la Facultad de Ciencias Sociales, Defensora Universitaria y es docente a tiempo completo de la Universidad Antonio Ruiz de Montoya.

2 Abogada por la Pontificia Universidad Católica del Perú, Máster en Administración de Empresas por la Universidad de Ciencias Aplicadas, Gerente Legal de Iriarte Abogados, experiencia en el sector público y privado, especialmente en las áreas de Derecho de las Nuevas Tecnologías, Comercio Electrónico, Gobierno Electrónico y Aspectos Legales del Marketing y Publicidad, con énfasis en entornos digitales.

educar a los clientes sobre amenazas cibernéticas. Igualmente, el Estado tiene una tarea pendiente con la implementación de ciudadanía y cultura digital en las personas.

Palabras clave: delitos informáticos - fraude informático - amenazas cibernéticas - cultura digital

1. INTRODUCCIÓN

La evolución de las tecnologías de la información ha cambiado la vida de las personas, lo que ha facilitado la realización de sus actividades como, por ejemplo, realizar compra de bienes o servicios, pagos en línea, transacciones en general, sin salir de casa utilizando el sistema financiero. A pesar de estas ventajas, también encontramos la aparición de nuevos ilícitos penales como el fraude informático, el cual se ha expresado a través de diversas modalidades, lo que ha generado un efecto negativo entre los usuarios al emplear estas tecnologías, más aún cuando se utilizan canales digitales bancarios. En este sentido, nos enfrentamos a la aparición de comportamientos delictivos que han ingresado a todos los países: uno de ellos es el fraude informático. Al respecto, las legislaciones peruana y norteamericana no son ajenas a este fenómeno, lo cual ha ocasionado una normativa que previene y sanciona este delito.

Por ello, realizaremos una comparación entre ambas legislaciones con respecto al tratamiento del fraude informático analizando oportunidades de mejora en nuestra administración penal positiva. Estos nuevos delitos son complejos, muchas veces transnacionales con estructuras organizadas que evolucionan constantemente al no encontrar freno en la legislación de los países.

Esta investigación tendrá como objetivo identificar una nueva forma de criminalidad, la cual debe ser combatida con una legislación moderna, donde convergen distintos actores sociales como instituciones públicas y privadas orientadas a implementar, y fomentar la ciudadanía y cultura digital de las personas. Asimismo, la legislación en este ámbito no podrá ser rígida ni inmutable, ya que la tecnología avanza vertiginosamente. Por ello, se ha tomado como referencia el sistema legal de Estados Unidos al ser un país con legislación avanzada en fraude informático.

Finalmente, se ofrece algunas conclusiones y recomendaciones a fin de contribuir a mejorar nuestro derecho positivo en el ámbito penal haciendo uso del método de Derecho Comparado.

2. EL DELITO DE FRAUDE INFORMÁTICO EN EL DERECHO PENAL DE ESTADOS UNIDOS

2.1. Características del Sistema Legal de Estados Unidos

El Sistema Legal de los Estados Unidos tiene la legislación más completa en lo que se refiere a los delitos informáticos. Pertenece al Sistema Jurídico del Common Law, distinto al nuestro, que corresponde al Sistema Jurídico Romano Germánico.

Estados Unidos cuenta con una legislación moderna para atacar el delito de fraude informático, que está creciendo a nivel mundial, lo cual permite mejorar nuestra legislación. Asimismo, se debe destacar que cada uno de los estados que integran el país norteamericano genera una legislación sobre el delito de fraude informático y su ámbito procesal.

2.2. Concepto de delito de fraude informático en Estados Unidos

Los delitos informáticos son también conocidos como delitos cibernéticos, por cuanto sanciona comportamientos ilícitos que, a través de operaciones electrónicas, atentan la seguridad de los sistemas informáticos o los datos procesados por ellos. El fraude informático se encuentra dentro de los delitos cibernéticos por estar asociado a transferencias electrónicas de fondo que utilizan las nuevas tecnologías.

Estados Unidos tiene una legislación general y leyes especiales orientadas a luchar contra esta criminalidad como, por ejemplo, la Ley Federal de Fraude y Abuso Informático 18 U.S. Code § 1030 (CFAA) de 1994 (modificó la Ley Federal de Fraude y Abuso Informático de 1986). Dicha norma tipificó conductas delictivas graves vinculadas al acceso ilegal de computadoras conectadas a internet y utilizadas por instituciones financieras, gobiernos federales o entre Estados, con penas de hasta veinte años en casos de reincidencia (Text of the Computer Fraud and Abuse Act Appendix D, 1994).

Así tenemos, que la legislación federal de Estados Unidos tiene tipificadas las siguientes conductas ilegales:

- Acceso sin permiso a un ordenador o sistema informático protegido.
- Acceso ilegal a un ordenador sin autorización para cometer fraude obteniendo información.
- Tráfico (venta, distribución, compartir ilegalmente) de contraseñas informáticas con fines fraudulentos.
- Acceso a una computadora protegida sin autorización y con la intención de defraudar.
- Transmisión de código o programa dañino (virus) para causar daño a la computadora protegida.

- Acceso a un ordenador con la intención de dañar o destruir archivos.
- Infringir las leyes de piratería informática. Por ello, bajo la ley federal, el delito de piratería informática está incluido dentro del delito de fraude informático cuando una persona abusa de ordenadores compartidos o tiene acceso no autorizado a un ordenador protegido o a un sistema informático gubernamental.

En Estados Unidos encontramos otras leyes federales complementarias, que también regulan el Fraude Informático como:

- Ley de Privacidad de las Comunicaciones Electrónicas (1986). Prohíbe el acceso no autorizado a las comunicaciones electrónicas almacenadas en un ordenador o red como el correo electrónico o los mensajes de texto.
- Ley Federal de Protección de Sistemas (1985). Fue el antecedente de la primera Ley de Fraude y Abuso Informático (Computer Fraud y Abuse Act) de 1986 y permitió que Estados como Florida, Michigan, Colorado, Rhode Island y Arizona fueran los primeros con legislación específica en esta materia.

La vigente Ley de Fraude y Abuso Informático de 1994 introdujo novedades como la regulación de virus informáticos, que contaminan programas o base de datos. Asimismo, considera delito cuando alguien modifica, destruye, copia, transmite datos o altera la operación normal de computadoras, sistemas o redes informáticas.

La ley de Fraude y Abuso Informático sigue actualizándose, debido al desarrollo de la tecnología en línea evitando que sea mal interpretada, pues dos casos relevantes permitieron a grandes empresas utilizar esta ley contra individuos que, a su criterio, eran amenaza a sus intereses comerciales. Estos son los ejemplos:

En el año 2005, el fabricante de *routers* de internet Cisco demandó al investigador en ciberseguridad Mike Lynn, quien trabajaba para la empresa Internet Security Systems (ISS) (Europa, 2001) y había encontrado fallas en el sistema operativo de internet de los *routers*, que hacían muy probables ciberataques a los clientes de Cisco. El argumento de defensa Cisco consistió en que la exposición pública de esta debilidad de ciberseguridad provocaría ciberataques incontrolables a la plataforma. Ante esta situación, el Sr. Lynn decidió firmar una orden judicial en la que se comprometía a no revelar los datos de su investigación en la empresa Cisco. Sin embargo, no recibió apoyo de su empleador, quien, por el contrario, tenía la misma posición que Cisco.

En el año 2010, el Sr. Matthew Keys, quien trabajaba en una empresa del grupo empresarial Tribune, fue acusado, luego de ser despedido, de revelar a *hackers* nombres de usuarios y contraseñas de los sitios web de dicha empresa. Se le declaró culpable de violar la Ley Federal de Fraude y Abuso Informático, por lo que fue condenado a 24 meses de prisión y 24 meses de libertad condicional, además de pagar una indemnización de 249.956 dólares.

La Ley Federal de Fraude y Abuso Informático señala tres niveles de sanción para quienes violan la ley:

- Primer nivel: considerado delito menor para personas naturales con pena de prisión no mayor a un año y sanción monetaria no mayor a cien mil dólares. Si son empresas las que han delinquido, la sanción monetaria no excederá los doscientos mil dólares.
- Segundo nivel: para personas naturales la prisión no será mayor a cinco años y las sanciones monetarias que no deben superar los doscientos cincuenta mil dólares. Las empresas pueden ser multadas con hasta quinientos mil dólares.
- Tercer nivel: las personas naturales tendrán prisión no mayor a diez años y sanción monetaria de hasta doscientos cincuenta mil dólares, mientras que para las empresas el monto de la sanción no excederá los quinientos mil dólares.

Como podemos apreciar, esta ley de 1994 hace diferencia entre aquellos que lanzan ataques de virus de aquellos que lo realizan intencionalmente para hacer daño y de allí la variante entre las sanciones. Sin duda resulta trascendental, ya que precisa qué es un acto delictivo no permitiendo que el creador de un virus señale como argumento de defensa desconocer que sus actos iban a causar daño o que sólo pretendía enviar mensaje.

De otra parte, la ley bajo comentario no define qué es un virus informático, sino describe el acto delictivo en sí mismo para dejar abierta la posibilidad que, si a futuro aparezcan nuevos ataques tecnológicos a los sistemas informáticos, estos serán sancionados.

2.3. Delitos Informáticos reconocidos por la Organización de las Naciones Unidas

El Congreso de las Naciones Unidas sobre Prevención del Delito y Justicia Penal se originó hace 65 años con la participación de Estados, sociedad civil, académicos y especialistas en prevención del delito y justicia penal. La finalidad de este Congreso, que se celebra cada 5 años, es fomentar que los Estados desarrollen políticas públicas para frenar la delincuencia organizada,

la cual se encuentra en crecimiento (NNUU, 2020).

En el 14° Congreso de Naciones Unidas, desarrollado en Kioto (Japón), en abril de 2020, abordó el tema *Promoción de la prevención del delito, la justicia penal y el estado de derecho: hacia el cumplimiento de la agenda 2030.* Un tema central fue la utilización de las nuevas tecnologías como medio e instrumento contra el delito.

Naciones Unidas considera delitos informáticos a los siguientes:

- Fraude Informático: cometido a través de la manipulación de computadoras para sustraer datos reservados.
- Manipulación de programas: modificación de programas existentes en computadoras o insertando nuevos programas especializados en programación informática.
- Manipulación de datos de salida: efectuado a través del envío de instrucciones falsas al sistema informático.
- Fraude efectuado por manipulación informática de los procesos de cómputo.
- Falsificaciones informáticas: alteración de datos de documentos almacenados en computadora.
- Sabotaje Informático: borrar, suprimir o modificar sin autorización funciones o datos de la computadora para obstaculizar el funcionamiento normal del sistema.
- Virus: son claves programáticas que se adhieren a los sistemas para propagarse en serie por cuanto se regeneran.
- Gusanos: penetran en programas de procesamiento de datos para modificar o destruir datos, sin posibilidad de regenerarse.
- Bomba lógica o cronológica: destruye o modifica datos a futuro.
- Acceso no autorizado a servicios o sistemas informáticos: incluye piratas informáticos (hackers) hasta sabotaje o espionaje informático.
- Reproducción no autorizada de programas informáticos de protección legal: perjudica ecnómicamente a los propietarios legítimos.

De todo lo expuesto, podemos colegir que el delito de fraude informático supera la legislación nacional y se convierte en delito transnacional, lo cual genera temor en las personas que realizan transacciones a través de medios informáticos. Este problema ha sido abordado de manera amplia por la legislación norteamericana, no solo federal sino estatal, para frenar el crecimiento de este delito con una normativa amplia que puede ser aplicada a cualquier otra modalidad de fraude informático y pueda aparecer a futuro

por el avance de la tecnología. Esta visión ha sido recogida en la legislación peruana, ya que ha incorporado variantes que serán expuestas a continuación.

3.- REGULACIÓN DEL FRAUDE INFORMÁTICO EN LA LEY PERUANA

La Ley de Delitos Informáticos (Ley 30096), modificada por la Ley 30171, prevé en su artículo 8 el delito de fraude informático. El tipo penal supone que, mediante una acción deliberada e ilegítimamente, se procure para el perpetrador o un tercero algún provecho ilícito en perjuicio de un tercero. Los verbos rectores o acciones que se deben llevar a cabo para conseguir el provecho ilícito son el diseño, introducción, alteración, borrado, supresión, clonación de datos informáticos o cualquier interferencia o manipulación en el funcionamiento de un sistema informático. El artículo señala finalmente que la pena por este delito será no menor de tres ni mayor de ocho años.

Asimismo, se establece como agravante las situaciones en las que se afecte el patrimonio del Estado destinado a fines asistenciales o a programas de apoyo social. En este caso la pena pasará a ser no menor de cinco ni mayor de diez años.[3]

Como se puede apreciar, un requisito indispensable para que se configure el delito es que la acción sea deliberada e ilegítima. Si bien nuestra ley no establece un apartado de definiciones, podemos recurrir para la interpretación de estos términos al Convenio de Budapest y su informe explicativo, tratado internacional referente en el mundo en materia de cibercriminalidad y el cual el Perú ha ratificado. El citado informe explicativo señala que la intención deliberada se refiere a que el delito requiere también la existencia de una intención deliberada específica de índole fraudulenta o dolosa para obtener un beneficio económico o de otro tipo para sí o para otra persona. Con respecto a la acción ilegítima, menciona que puede referirse a una conducta realizada sin facultades para hacerlo (ya sean de orden legislativo, ejecutivo, administrativo, judicial, contractual o consensual) o a una conducta que no está de otro modo comprendida dentro de las justificaciones, excusas y defensas legales establecidas o los principios pertinentes con arreglo a las leyes nacionales.

---

3 "El que deliberada e ilegítimamente procura para sí o para otro un provecho ilícito en perjuicio de tercero mediante el diseño, introducción, alteración, borrado, supresión, clonación de datos informáticos o cualquier interferencia o manipulación en el funcionamiento de un sistema informático, será reprimido con una pena privativa de libertad no menor de tres ni mayor de ocho años y con sesenta a ciento veinte días-multa.
La pena será privativa de libertad no menor de cinco ni mayor de diez años y de ochenta a ciento cuarenta días-multa cuando se afecte el patrimonio del Estado destinado a fines asistenciales o a programas de apoyo social.

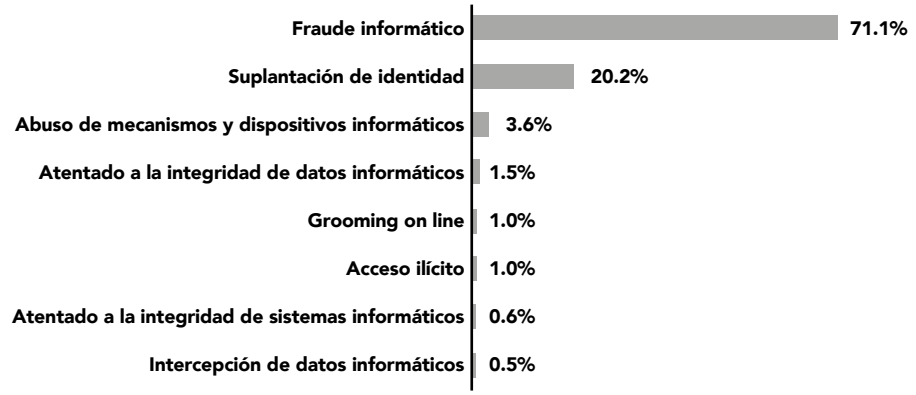
Para Villavicencio Terreros (2014), se clasifica como un delito de resultado, porque no basta cumplir con el tipo penal para que se consuma el delito de fraude informático. Además, es necesario que esa acción vaya seguida de un resultado que va por cuerdas separadas de las acciones informáticas, el causar un perjuicio a tercero; de otro modo, el delito quedaría en tentativa.

El fraude informático presenta ciertos retos para su persecución penal, entre los cuales se encuentran:

- El anonimato
- Su carácter transnacional
- Falta de capacitación de jueces en materia informática
- Demora en el levantamiento del secreto bancario
- Falta de peritos informáticos forenses
- Poca cooperación de las operadoras de telecomunicaciones.

A pesar de ello, el fraude informático es el más denunciado, como lo muestra la estadística del Registro de Denuncias de Investigación Criminal de la PNP.

Tipos de ciberdelitos denunciados ante la PNP (Perú, 2021)



Fuente: Sistema de Registro de Denuncias de Investigación Criminal PNP
Elaboración: Defensoría del Pueblo

3.1.- Modalidades más comunes de fraude informático

3.1.1.- Phishing

El *phishing* es una técnica consistente en el envío de un correo electrónico en el que los ciberdelincuentes suplantan la identidad de entidades públicas o empresas privadas, como un banco o una empresa reconocida o un servicio que utilicemos. Su objetivo es obtener toda la información personal y bancaria como usuarios y contraseñas, direcciones, datos de tarjetas de crédito, etc., realizar un cargo económico o infectar el dispositivo. Para ello, adjuntan archivos infectados o enlaces a páginas fraudulentas.

3.1.2.- Vishing

Este término deriva de la unión de dos palabras: *'voice'* y *'phishing'* y, por tanto, se refiere a una modalidad que combina una llamada telefónica fraudulenta con información previamente obtenida, ya sea por internet o fuentes ilícitas como compras de bases de datos personales en el mercado negro.

La modalidad se despliega en dos pasos. Primero, el ciberdelincuente debe contar con información personal conseguida a través de internet, el mercado negro o alguna acción previa. Sin embargo, necesita la clave SMS o *token* digital para realizar y validar operaciones bancarias o compras por internet. El segundo paso consiste en que el ciberdelincuente llama por teléfono al cliente haciéndose pasar por personal de la entidad bancaria, con mensajes particularmente alarmistas e intenta que el cliente revele el número de su clave SMS o *token* digital, que son necesarios para autorizar transacciones.

3.1.3.- Smishing

Este término deriva de la unión de dos palabras: *'sms'* y *'phishing'*, dado que esta modalidad se realiza a través de mensajes de texto o mensajes por WhatsApp. La víctima recibe un mensaje, donde el ciberdelincuente se hace pasar por el banco y alerta sobre una supuesta compra sospechosa con su tarjeta de crédito. Luego, le alienta a cancelar dicha compra llamando a un número de banca telefónica falso, en el cual le pedirán sus datos confidenciales. El cliente devuelve la llamada y es ahí cuando el ciberdelincuente, haciéndose pasar por el banco, solicita información confidencial para supuestamente cancelar la compra. En una variante de esta modalidad, el mensaje también podría incluir un enlace a una web fraudulenta para solicitar información sensible.

3.1.4.- Sim swapping

El SIM *swapping* es una técnica fraudulenta donde se clona de manera ilícita la tarjeta SIM del móvil de un individuo. En este proceso, el atacante se hace pasar por el dueño legítimo para lograr esta duplicación. Una vez que logra interrumpir el servicio del propietario real, se apodera de sus datos y asume el control de sus

servicios financieros digitales, aprovechando los mensajes de verificación que se envían al número de teléfono comprometido.

Los delincuentes, para lograr su cometido, suelen comunicarse con los proveedores de servicios telefónicos, ya sea vía telefónica o en persona. Para ello, suministran datos privados y personales de la víctima, tales como su número de identificación. Esta información puede haber sido recolectada por medio de técnicas de ingeniería social, donde se hacen pasar por entidades legítimas mediante mensajes de texto, correos electrónicos o llamadas, o bien investigando en sus perfiles de redes sociales.

La mayor amenaza del SIM *swapping* es que, al hacerse por teléfono, no hay una comprobación directa de la identidad del solicitante. Si el operador solo pide ciertos datos y el delincuente ya dispone de ellos, debido a los métodos de infiltración antes descritos, puede conseguir el duplicado sin mayores obstáculos.

3.1.5. Clonación de tarjetas de crédito

Esta modalidad se materializa cuando se duplica una tarjeta mediante la falsificación de la banda magnética. Los estafadores copian la banda magnética de la tarjeta pasándola por un *skimmer* (dispositivo que almacena los datos de la banda magnética). Además, se encargan de conocer tu clave secreta (de diferentes maneras) y utilizan estos datos para generar una nueva tarjeta idéntica a la tuya, con la que podrán realizar diversos fraudes.

3.2. Rol del Estado peruano frente al delito de fraude informático y la comparación con el Sistema Jurídico de Estados Unidos

A nivel global todos los países están preocupados en evaluar las circunstancias que conducen a la realización del delito de fraude informático. El Estado peruano no es ajeno a ello, desempeña un rol fundamental en la prevención, persecución y sanción del fraude informático. Con la Ley N° 30096 y su modificatoria Ley N° 30171 se han establecido conductas delictivas y sanciones muy similares a las establecidas en la legislación de Estados Unidos. En este sentido, no solo regula la conducta sino el resultado. Además, en ambas legislaciones el delito de fraude informático no se encuentra en el Código Penal sino regulado en ley específica.

Si bien la División de Investigación de Alta Tecnología de la Policía Nacional de Perú se creó en el 2005, sin fiscales especializados, las investigaciones tenían muy poca probabilidad de éxito. Por ello, entre 2014 y 2018, la American Bar Association – Rule of Law Initiative desarrolló diversos cursos especializados en cibercrimen y prueba digital. Además, publicó el Manual de Evidencia Digital (2017), aprobado por el Ministerio Público y la Policía Nacional del

Perú. El objetivo de dichas acciones fue sensibilizar a los operadores jurídicos, capacitarlos en la Ley de Delitos Informáticos (2013) y explicar cómo se desarrolla un plan de investigación.

Adicionalmente, como un compromiso asumido en el marco del Convenio de Budapest, mediante las Resoluciones de Fiscalía de la Nación N°1025-2020-MP-FN, de fecha 18 de setiembre de 2020 y N°1194-2020-MP-FN, de fecha 30 de octubre de 2020, la Fiscalía de la Nación conformó una comisión encargada de evaluar técnicamente la creación de un piloto de fiscalía especializada o Unidad Especializada en Ciberdelincuencia. Esta comisión recibió apoyo técnico del Programa de Asistencia contra el Crimen Transnacional Organizado (PACCTO) y la Embajada de los Estados Unidos.

Posteriormente, mediante la Resolución de la Fiscalía de la Nación N° 1503-2020- MP-FN, de fecha 30 de diciembre de 2020, se creó la Unidad Fiscal Especializada en Ciberdelincuencia del Ministerio Público con competencia a nivel nacional. El Perú mantiene una relación de coordinación con la Policía Nacional y la Fiscalía Especializada en Delitos de Alta Tecnología, las cuales tienen la función de investigar y perseguir delitos informáticos, muy similar a la colaboración que ofrece la Agencia Federal de Investigación e Inteligencia (FBI) en Estados Unidos. En el año 2022 han sido reportados 800.944 denuncias por delitos informáticos. En los últimos cinco años el delito de *phishing* es el más común (FBI, 2023, Federal Bureau, 2022).

Esta información coincide con lo que ocurre en el Perú, ya que la modalidad más frecuente del delito de fraude informático es el *phishing* (El Peruano, 2023).

El Estado peruano, en aras de fomentar la cultura digital en la población, realiza campañas de educación y concientización sobre seguridad cibernética en colaboración con entidades financieras llegando a sensibilizar a través de programas de formación. En ellas participan entidades del Estado unidas en la Política Nacional de Inclusión Financiera, a efectos de dar cumplimiento al objetivo de desarrollar plataformas digitales, que favorezcan la seguridad digital y el uso óptimo de tecnologías digitales (SBS, 2019).

De otra parte, el Estado peruano promueve un entorno seguro en línea, identificando y persiguiendo a quienes cometen delitos de fraude informático en labor conjunta con entidades privadas y la sociedad civil. Cabe destacar la labor que realiza el Ministerio Público, a través de la Fiscalía Especializada en Ciberdelincuencia de Lima Centro, colaborando con el Poder Judicial a efectos de lograr entre el mes de enero a setiembre 2023 treinta y cinco sentencias por delitos de fraude informático y abuso de mecanismos y dispositivos informáticos.

La legislación norteamericana sanciona a aquellas personas que intencionalmente causan daños transmitiendo virus, así como a aquellas que

de manera temeraria e imprudente lanzan ataques de virus, es decir, diferencia niveles de delitos. De esta manera, prohíbe la transmisión de programas, información, códigos o comandos que dañen las computadoras, sistemas informáticos, redes, información, datos o programas.

Nuestra legislación peruana no contempla definiciones como la legislación norteamericana, por lo que deben recurrir al Convenio de Budapest para interpretar la norma. Sin embargo, es útil acudir a la legislación de Estados Unidos, porque ambos tienen en común la vulneración de derechos a través del uso de *hardware o software*.

Asimismo, ambas legislaciones enfrentan el reto de adecuar su legislación para responder a las nuevas modalidades de fraude informático que se sirven de la inteligencia artificial, especialmente la tecnología del *deepfake*, para engañar a sus víctimas. Ninguno de los dos países ha expedido aún normativa que permita prevenir este tipo de situaciones.

Los *deepfakes* se definen como medios audiovisuales manipulados o sintéticos que parecen auténticos, y que presentan a personas que aparentan decir o hacer algo que nunca han dicho o hecho, producidos utilizando técnicas de inteligencia artificial, incluyendo aprendizaje automático y aprendizaje profundo.

Los *deepfakes* se pueden entender mejor como un subconjunto de una categoría más amplia de "medios sintéticos" generados por IA, que no solo incluye video y audio, sino también fotos y texto. Este informe se centra en un número limitado de medios sintéticos impulsados por IA: videos *deepfake*, clonación de voz y síntesis de texto. (EPRS | European Parliamentary Research Service, 2021)

Ya se vienen registrando casos de fraude utilizando *deepfake* como, por ejemplo, el de una pareja en Houston, la cual fue engañada por estafadores que clonaron la voz de su hijo. Mediante el uso de inteligencia artificial, los convencieron de que necesitaban cinco mil dólares para ayudar a su hijo tras un supuesto accidente y arresto por conducir ebrio. Los padres entregaron el dinero en efectivo, pero se percataron después de la estafa luego de que su propio hijo les asegurara de que se encontraba laborando (McCord, 2023).

Otro caso se produjo en Emiratos Árabes Unidos, en donde se usó inteligencia artificial, *deepfake* de voz, para clonar la voz de un director de empresa. Los delincuentes llamaron al gerente de un banco imitando la voz del director, y le solicitaron autorizar transferencias de dinero para una supuesta adquisición empresarial. Creyendo que era una petición legítima, el gerente transfirió 35 millones de dólares (Hernández, 2021).

Finalmente, en cuanto a la modalidad de *phishing*, se ha evaluado el uso de inteligencia artificial Devising and Detecting Phishing: large language models vs. Smaller Human Models (Fredrik Heiding, 2023), que explora el uso de grande

modelos de lenguaje (LLM) para crear y detectar correos electrónicos de *phishing*. Los autores compararon la efectividad de estos *emails* creados usando el marco V-Triad, contra los creados por el LLM GPT-4. También evaluaron la habilidad de varios LLM (incluyendo GPT, Claude, PaLM y LLaMA) para detectar la intención detrás de los *emails de phishing*.

Los resultados mostraron que los *emails* creados manualmente tuvieron más éxito engañando a los participantes que los *emails* generados por GPT-4. Sin embargo, cuando se combinó GPT-4 con las mejores prácticas del marco V-Triad, la tasa de éxito fue similar o mejor que usando solo humanos. Esto sugiere que la automatización parcial puede ser útil para crear *emails* de *phishing* efectivos. En cuanto a la detección, los LLM demostraron buenas habilidades, a veces superando la detección humana de *emails* de *phishing* no obvios. El modelo Claude tuvo el mejor desempeño, correctamente detectando la intención maliciosa del 75% de los *emails* de control y del 100% de los de phishing generados cuando se le preguntó explícitamente si un email era sospechoso.

Como se aprecia, las amenazas cibernéticas están en apogeo vulnerando la seguridad informática que compromete la integridad, confidencialidad y disponibilidad de datos de personas naturales y jurídicas. Es decir, son riesgos que se cometen a través de plataformas empresariales (Apps) burlando la tecnología del sistema financiero. Por ello, resulta necesario tomar medidas de seguridad, porque la tecnología se encuentra al servicio de las personas. En este sentido, recomendamos los siguiente:

- Actualizar periódicamente los sistemas operativos para corregir posibles vulnerabilidades.
- Instalar antivirus para detectar y eliminar amenazas de virus.
- Cambiar periódicamente contraseñas utilizando dos factores de autentificación.
- No abrir correos electrónicos, enlaces o mensajes sospechosos.
- Utilizar Firewalls para proteger la red de intrusos.
- Actualizar los dispositivos conectados a internet.
- Realizar periódicamente copias de seguridad de información relevante.
- Recibir educación en materia de amenazas cibernéticas.
- Monitorear constantemente las cuentas bancarias en línea para detectar cualquier movimiento sospechoso.
- Reportar incidentes sospechosos.

Estas son medidas adoptadas a nivel global; sin embargo, los ciberdelincuentes encuentran alguna manera de burlar la ley. De allí la importancia de crear cultura

digital, es decir, familiarizar a las personas para que interactúen con la tecnología, realicen operaciones en línea utilizando todas las herramientas digitales que hoy existen para facilitar sus actividades diarias. Asimismo, conduce a promover el uso responsable y ético de la tecnología, tarea que requiere trabajo conjunto del Estado, actividad privada y la sociedad civil.

Todo lo expuesto genera una ciudadanía digital donde el uso de la tecnología y la interacción con otros a quienes no vemos implica el respeto de los derechos de las personas con un comportamiento positivo en línea en el mundo digital, donde todos debemos sentirnos seguros de participar sin el temor a ser víctimas de fraudes informáticos en todas las modalidades que hemos descrito.

4.- CONCLUSIONES

- Se ha incrementado el delito de fraude informático en los últimos años bajo la modalidad de phishing tanto en Perú como en Estados Unidos.
- Es necesaria una colaboración articulada con la policía especializada en delitos informáticos en ambos países en la búsqueda de frenar el delito de fraude informático que llega a tener características de delito transnacional.
- Estados Unidos propone una legislación abierta, flexible ante la velocidad de cambios tecnológicos para detectar el delito de fraude informático en sus versiones más sofisticadas.
- El Perú adopta una legislación flexible ante la velocidad del avance de la tecnología, lo cual permite estar alerta ante la aparición de nuevas modalidades de fraude informático.
- Ninguno de los países materia de análisis ha adoptado aún medidas para la prevención de modalidades de fraude informático que utilicen inteligencia artificial.

5.- RECOMENDACIONES

- Evitar revelar datos personales respecto a situación económica o movimientos financieros a través de redes sociales.
- No compartir contraseñas con ninguna persona ni revelarlas como medida de precaución ante fraudes informáticos.
- Brindar capacitación constante en temas de amenazas cibernéticas a fin de frenar el avance de la ciberdelincuencia. Estos temas deben ser difundidos a través de todos los medios de comunicación para generar ciudadanía digital.
- Difundir el trabajo que realizan la Policía Nacional del Perú y la Fiscalía

Especializada en ciberdelincuencia a fin de que la población conozca los delitos cibernéticos y sus modalidades y qué acciones tomar cuando ocurre un hecho de esta naturaleza.

- Establecer mayores estándares de seguridad informática a bases de datos personales administradas por la administración pública y empresas privadas.

REFERENCIAS

Castillo, C. (s.f.). *BBVA*. Obtenido de https://www.bbva.com/es: https://www.bbva.com/es/innovacion/phishing-vishing-smishing-que-son-y-como-protegerse-de-estas-amenazas/

Congreso. (21 de octubre de 2013). *Ley de Delitos Informáticos Ley N° 30096*. Obtenido de https://www2.congreso.gob.pe/sicr/cendocbib/con5_uibd.nsf/C5F98BB564E5CCCF052 583160060 64AB/$FILE/6_Ley_30096.pdf

Defensoría del Pueblo (2023). *La Ciberdelincuenica en el Perú: Estrategias y Retos del Estado.* Defensoría del Pueblo. https://www.defensoria.gob.pe/wp-content/uploads/2023/05/INFORME-DEF-001-2023-DP-ADHPD-Ciberdelincuencia.pdf

EPRS | European Parliamentary Research Service. (2021). *Tackling deepfakes in European policy*. Bruselas: Parlamento Europeo.

Europa, C. d. (2001). *Informe Explicativo Convenio sobre la Coberdelincuencia.* Consejo de Europa.

Europe, C. o. (2001). Convenio sobre la ciberdelincuencia. *Serie de Tratados Europeos N°185* (pp. 1-26). Budapest: Organization of American States.

FBI. (2023). *FBI en Español*. Obtenido de https://www.fbi.gov/news/espanol

Federal Bureau, I. (2022). *Internet Crime Report.* USA: Internet Crime Complaint Center. Fredrik Heiding, B. S. (2023). Devising and Detecting Phishing: large language models vs. Smaller Human Models. arXiv:2308.12287, 20.

Hernández, G. (15 de octubre de 2021). Obtenido de https://www.xataka.com.mx/robotica-e-ia/alguien-clono-voz-director-empresa-ia-para-llamar-a-sus-empleados-hacer-estafa- 400-000-dolares

Mayer Lux, L., & Oliver Calderón, G. (2020). El delito de fraude informático: concepto y delimitación. *Revista Chilena de Derecho y Tecnología, 9*(1), 151–184. https://doi.org/10.5354/0719-2584.2020.57149

McCord, C. (21 de Marzo de 2023). *KHOU*11*. Obtenido de https://www.khou.com/article/news/local/phone-voice-clone-scam-houston-area-crime/285-999031eb-d3c8-41db-8d0a-0ccf05273194

Morán Espinoza, A. (2021). Responsabilidad penal de la Inteligencia Artificial (IA). ¿La próxima frontera?. *Revista IUS, 15*(48), 289-323. https://doi.org/10.35487/rius.v15i48.2021.706

NN.UU. (2020). *Congresos de las Naciones Unidas sobre prevención del delito y justicia penal.*

OSI, O. d. (11 de noviembre de 2021). INCIBE. Obtenido de Instituto de Ciberseguridad de España: https://www.incibe.es/ciudadania/blog/que-es-el-phishing

Peruano, D. E. (22 de junio de 2023). *El Peruano*. Obtenido de https://www.elperuano.pe/noticia/216043-cuidado-con-los-fraudes-informaticos-estas-son-las-modalidades-mas-denunciadas-en-peru#:~:text=El%20phishing%20es%20el%20m%C3%A9todo,de%20la%20mitad%20del%20total.

Prado, O. Z. (30 de abril de 2021). *IUS360.* Obtenido de https://ius360.com/delitos- informaticos-breves-alcances-de-la-nueva-unidad-fiscal-especializada-en-la-ciberdelincuencia-del-ministerio-publico-oscar-zevallos/

Ramirez-Asis, E. H., Norabuena-Figueroa, R. P. ., Toledo-Quiñones, R. E. ., & Henostroza Márquez Mázmela, P. R. . (2022). Validación de una escala de conciencia sobre ciberdelito en estudiantes universitarios de Perú. *Revista Científica General José María Córdova*, 20(37), 209–224. https://doi.org/10.21830/19006586.791

SBS (5 de agosto de 2019). *Política Nacional de Inclusión Financiera.* Obtenido de Decreto Supremo N° 255-2019-EF: https://www.sbs.gob.pe/Portals/4/jer/EST-MONITOREO- ENIF/2023/PNIF.pdf

Scotiabanck. (s.f.). *Scotiabank.com.pe.* Obtenido de https://www.scotiabank.com.pe/Acerca- de/seguridad/tipos-de-fraude/clonacion

Text of the Computer Fraud and Abuse Act Appendix D. (1994). USA: Willey online library.

Villavicencio Terreros, F. (2014). Delitos Informáticos. *Ius et Veritas, 24*(49), 284-304.https://revistas.pucp.edu.pe/index.php/iusetveritas/article/view/13630

Vinelli Vereau, R. (2021). Los delitos informáticos y su relación con la criminalidad económica. *Ius et Praxis*, *53*(53), 95-110. https://doi.org/10.26439/iusetpraxis2021.n053.4995

Zapata, J. A. (2023). *La eficacia de la persecución penal del delito de fraude informático en el Perú.* UTP.