UNIVERSIDAD PERUANA DE LAS AMÉRICAS

ESCUELA PROFESIONAL DE DERECHO

TRABAJO DE INVESTIGACIÓN

NUEVOS DELITOS INFORMÁTICOS POR IMPULSO DE LA TRANSFORMACION DIGITAL POR CAUSA DEL COVID-19 EN EL PERU

PARA OPTAR EL TÍTULO PROFESIONAL DE ABOGADO

AUTOR:

POZO HUAMAN FRANCISCO GABRIEL
CÓDIGO ORCID: 0000-0002-5566-247X

ASESOR: Mg.

PANTIGOZO LOAIZA MARCO HERNAN
CÓDIGO ORCID: 0000-0001-66160689

LÍNEA DE INVESTIGACIÓN: DERECHO PENAL, CIVIL Y CORPORATIVO

LIMA, PERÚ

DICIEMBRE, 2021

Resumen

El presente trabajo de investigación, tiene por finalidad realizar un estudio sobre los nuevos delitos informáticos en el actual proceso de aceleración de la transformación digital en el Perú por causa de la pandemia COVID-19, el cual nos permita conocer cómo actúan los criminales cibernéticos y poder tipificar estos nuevos delitos informáticos en el código penal vigente, saber cómo actúan las autoridades encargadas como la División de Investigación de Delitos de Alta Tecnología (DIVINDAT), que es el órgano de ejecución de la Dirección de Investigación Criminal de la Policía Nacional del Perú, la fiscalía de la Nación con la creación de su nueva Unidad Fiscal Especializada en Ciberdelincuencia, de tal forma que el estado debe promover, crear y ejecutar centros de respuestas rápidas ante ataques cibernéticos como un Centro de Operaciones de Seguridad Nacional con el objetivo de prevenir la seguridad informática y el gobierno digital del estado peruano.

Palabras claves

Nuevos delitos informáticos, ciberdelincuencia, Centro de Operaciones de Seguridad (SOC), Gobierno digital y Transformación digital

Abstract

The purpose of this research work is to carry out a study on the new computer crimes in the current process of acceleration of the digital transformation in Peru due to the COVID-19 pandemic, which allows us to know how cyber criminals act and be able to classify these new computer crimes in the current criminal code, know how the authorities in charge act such as the High Technology Crime Investigation Division (DIVINDAT), which is the executing body of the Criminal Investigation Directorate of the National Police of Peru , the National Prosecutor's Office with the creation of its new Specialized Cybercrime Fiscal Unit, in such a way that the state must promote, create and execute centers for rapid responses to cyber attacks such as a National Security Operations Center with the aim of preventing computer security and digital government of the Peruvian state

Keywords

New computer crimes, cybercrime, Security Operations Center (SOC), Digital Government and Digital Transformation

Tabla de Contenidos

Resumen 3

Abstract 4

Introducción 6

1. Antecedentes nacionales e internacionales 7
2. Desarrollo del tema 16
   - 2.1. Normatividad actual 16
   - 2.2. Delitos tipificados en nuestra legislación 18
   - 2.3. Nuevos delitos informáticos 21
   - 2.4. COVID: “Impulsor de la Transformación Digital” 28

Conclusiones 30

Aporte de la investigación 31

Recomendaciones 32

Referencias bibliográficas 33

Introducción

La presente investigación tiene por objetivo dar a conocer y establecer los nuevos delitos informáticos en el proceso acelerado de la transformación digital en el Perú por causa de la pandemia COVID-19, analizando los diferentes acciones de nuestros legisladores, desde la promulgación de la Ley 27309 que incorpora los Delitos Informáticos al Código Penal, ha transcurrido hasta la actualidad nuevas leyes, reglamentos, decretos legislativos, decretos supremos, resoluciones legislativas y decretos de urgencia sobre protección de datos personales, seguridad de la información, telecomunicaciones, vigilancia electrónica, ciberseguridad, cibercrimen y ciberdefensa. Desde la creación (2001) de la Comisión Multisectorial para el Desarrollo de la Sociedad de la Información (CODESI), donde se define un plan de acción conformado por jefes de sistemas de los ministerios públicos y de empresas privadas, distribuidos en seis (6) mesas de trabajo y se establecieron cinco (5) objetivos estratégicos plasmados en un plan de desarrollo de la sociedad de la información – La agenda digital peruana – fue el inicio de la transformación digital en el Perú llamada posteriormente la agenda digital 1.0 (2005), años más tarde se actualizo a la agenda digital 2.0 (2011) y en la actualidad la agenda digital al bicentenario (2021), son documentos de gestión que guían hacia la consolidación de poder llevar al Perú en un Gobierno Digital. En base a ello recomendaremos mejorar las leyes de delitos informáticos con especialistas y técnicos en seguridad informática y conformar un comité de vigilancia tecnológica, promoviendo la creación de un verdadero centro de Coordinación de Respuestas a Emergencias en Redes Teleinformáticas de la Administración Pública del Perú (Pe-CERT), un real Equipo

de Respuesta a Incidentes de Seguridad (CSIRT) y tres (3) verdaderos Centro de Operaciones de Seguridad (SOC), uno por parte de la empresa privada, otro por el estado y el tercero por el comando conjunto de las fuerzas armadas del Perú.

1. Antecedentes nacionales e internacionales

1.1. Nacional

1.1.1. Primer antecedente

Como antecedente nacional sobre delitos informáticos es sobre la STC de fecha 10/12/2020, expediente 01189-2019-PHC/TC - LIMA - Marcos Morales Vargas, representado por William Benardino García Rosales (01189-2019-PHC/TC, 2020) Se presentó un recurso de agravio constitucional en contra de don William Benardino García Rosales, contra la resolución de fecha 5/11/2018, expedida por la Segunda Sala Penal para Procesos con Reos Libre de la Corte Superior de Justicia de Lima, que declaró improcedente la demanda de habeas corpus de autos.

ANTECEDENTES

Solicita que se declare la nulidad dela sentencia de 16/06/2017, que condenó al beneficiario por los delitos de fraude informático y falsificación de firma en documento privado; y la Resolución de 26/12/2017, que confirmó la precitada sentencia en cuanto a la condena, pero la revocó respecto a la pena; y reformándola, le impuso ocho años de pena privativa de la libertad efectiva (Expediente 9405-2014). Se alega la vulneración de los derechos a la libertad personal, al debido proceso y a la tutela jurisdiccional efectiva, así como del principio de legalidad penal.

Sostiene que mediante la sentencia de 16 de junio de 2017, se condenó al beneficiario a diez años de pena privativa de la libertad efectiva, que resultó de la sumatoria siguiente: ocho años por el delito de fraude informático y dos años de pena privativa de la libertad efectiva y falsificación de firma en documento privado. Posteriormente, mediante la Resolución de 26 de diciembre de 2017, se le redujo la pena a seis años de pena privativa de la libertad efectiva, por ambos delitos.

Precisa que se condenó al beneficiario a través de una norma que no se encontraba vigente al momento que se cometieron los hechos delictuosos, pues tales hechos ocurrieron durante los meses de enero, febrero, marzo, julio, setiembre y octubre de 2013, pero fue condenado mediante la Ley 30096, que entró en vigencia el 23 de octubre de 2013, por lo que la norma aplicable era el artículo 185 del Código Penal, que en su forma agravada era el artículo 186, numeral 3 del referido código.

FUNDAMENTOS

Delimitación del petitorio

El objeto de la demanda es que se declare la nulidad de la sentencia de 16/06/2017, que condenó a don William Benardino García Rosales por los delitos de fraude informático y falsificación de firma en documento privado; y la Resolución de 26/12/2017, que confirmó la precitada sentencia en cuanto a la condena, pero la revocó respecto a la pena; y reformándola, le impuso seis años de pena privativa de la libertad efectiva. Se alega la vulneración de los derechos a la libertad personal, al debido proceso y a la tutela jurisdiccional efectiva, así como del principio de legalidad penal.

Análisis del caso

El principio de legalidad penal se encuentra en el artículo 2, inciso 24, literal “d” de la Constitución, nadie será procesado ni condenado por acto u omisión que al tiempo de cometerse no esté previamente calificado en la ley, de manera expresa e inequívoca, como infracción punible, ni sancionado con pena no prevista en la ley.

Este TC se manifiesta que el principio de legalidad penal se configura también como un derecho subjetivo constitucional de todos los ciudadanos, como principio constitucional, informa y limita los márgenes de actuación de los que dispone el Poder Legislativo al momento de determinar cuáles son las conductas prohibidas, así como sus respectivas sanciones.

. Entonces, conforme se aprecia de la Resolución de fecha 26/12/2017, al actor se le impuso en total ocho años de pena privativa de la libertad efectiva por los delitos de fraude informático y falsificación de firma en documento privado, vigente al momento de los hechos y que se encontraba dentro del marco normativo del primer párrafo del artículo 8 de la Ley 30096 y del primer párrafo del artículo 427 del Código Penal.

HA RESUELTO, Declarar **INFUNDADA** la demanda.

1.1.2. Segundo antecedente

Como antecedente nacional sobre delitos informáticos es sobre la **SENTENCIA DE CASACIÓN 536-2020** de fecha 30/09/2021

En audiencia pública mediante el aplicativo Google Meet, el recurso de casación interpuesto por el sentenciado Roberto Víctor Salas Vilca contra la resolución de

vista emitida el doce de junio de dos mil veinte por la Sala Superior Mixta de Emergencia de la Corte Superior de Justicia de Arequipa, que confirmó la resolución del 07/05/2020, expedida por el Juzgado Penal Unipersonal Transitorio Supra provincial de Corrupción de Funcionarios, que declaró improcedente su pedido de conversión de la pena privativa de libertad impuesta en su contra por haber sido condenado como autor de los delitos de peculado y fraude informático, en agravio del Estado.

Estuvo como ponente el señor juez supremo SEQUEIROS VARGAS.

FUNDAMENTOS DE HECHO

Situación jurídica del sentenciado impugnante

Con fecha 19/01/2020, el Juzgado Especializado en Delitos de Corrupción de funcionarios de la Corte Superior de Justicia de Arequipa emitió sentencia condenatoria contra Roberto Víctor Salas Vilca y lo condenó como autor de los delitos de peculado y fraude informático, en agravio del Estado; en consecuencia, le impuso la pena privativa de libertad de cuatro años y ocho meses, la pena de días multa e inhabilitación, así como la reparación civil. En tal sentido, a la fecha viene ejecutando su condena en el Establecimiento Penitenciario de Socabaya y cumplió con pagar el íntegro de la reparación civil y los días multa impuestos.

El sentenciado Roberto Víctor Salas Vilca presentó una solicitud de conversión de pena privativa de libertad a prestación de jornadas de servicio a la comunidad y, subordinada y alternativamente, la conversión por vigilancia electrónica. Invocó como sustento legal el artículo 29-A del Código Penal y como sustento fáctico su estado de salud.

Con fecha 07/05/2020, el Juzgado Penal Unipersonal Transitorio Supra provincial de Corrupción de funcionarios de la Corte Superior de Justicia de Arequipa atendió su pedido y lo declaró improcedente.

Inconforme con lo resuelto, el sentenciado Salas Vilca interpuso recurso de apelación contra la citada resolución. Elevados los autos y vista la causa, la Sala Superior Mixta de Emergencia de la Corte Superior de Justicia de Arequipa emitió la resolución del 12/06/2020, que confirmó la resolución de primera instancia en todos sus extremos.

El sentenciado recurrente interpuso recurso de casación excepcional conforme al artículo 427.4 del CPP contra la resolución de vista emitida el 12/06/2020 y solicitó que se ordene casar la recurrida, se examine lo actuado y se declare fundado su pedido de conversión de pena. No planteó un tema en específico para el desarrollo de la doctrina jurisprudencial; únicamente refirió que la Corte Suprema debe conocer el caso concreto, en el cual se estaría afectando un catálogo de derechos humanos y fundamentales, como el derecho a la vida, la salud, la libertad, la igualdad y la debida motivación de las resoluciones judiciales.

FUNDAMENTOS DE DERECHO

La conversión de las penas se encuentra regulada en el Decreto Legislativo número 1300, publicado el 30/12/2016, que en el artículo 3 determina los supuestos de procedencia e improcedencia:

Con motivo de la crisis sanitaria nacional ocasionada por la pandemia de la COVID-19, se adoptaron medidas excepcionales para la población penitenciaria, a fin de lograr el des hacinamiento en los centros penitenciarios y con ello,

disminuir el riesgo de contagio, por lo que se emitió el Decreto Legislativo número 1513, publicado el 04/06/2020, que refiere lo siguiente respecto a la remisión condicional de la pena:

Los derechos constitucionales sobre los que se alega vulneración son los siguientes: A la vida, a su identidad, a su integridad moral, psíquica y física y a su libre desarrollo y bienestar. El concebido es sujeto de derecho en todo cuanto le favorece; A la igualdad ante la ley. Nadie debe ser discriminado por motivo de origen, raza, sexo, idioma, religión, opinión, condición económica o de cualquiera otra índole.

Análisis jurisdiccional

El presente recurso de casación se admitió por el motivo previsto en el inciso 1 del artículo 429 del CPP, esto es, la inobservancia de garantías constitucionales de carácter material o procesal. En específico, el impugnante alegó que se habría vulnerado su derecho a la vida, la salud, la igualdad y la debida motivación de las resoluciones judiciales. Ello será materia de análisis por esta Sala Suprema.

De igual manera, respecto a su pedido de que se evalúe la vigilancia electrónica personal como una medida alternativa a la pena privativa de libertad que le fu impuesta, resulta inaplicable y solo para aquellos condenados por el delito de peculado.

Cabe precisar que, en mérito de la crisis sanitaria por causa de la pandemia por la COVID-19, el Estado adoptó políticas públicas enfocadas a evitar el hacinamiento en los establecimientos penitenciarios, a fin de disminuir el riesgo de contagio de la enfermedad y de esta manera preservar la integridad, la vida

y la salud de las personas internas en establecimientos penitenciarios y centros juveniles; asimismo, de modo indirecto, de los servidores públicos que laboran en dichas instituciones y de la ciudadanía en general.

Finalmente, este Tribunal Supremo, luego de haber realizado una evaluación de la resolución de vista materia del recurso de casación, ha logrado advertir que el ad quem no incurrió en la causal casacional alegada -inciso 1 del artículo 429 del CPP-, específicamente al haber emitido pronunciamiento en el marco del principio de legalidad y respetando el derecho de igualdad ante la ley, sin perjudicar los derechos constitucionales del recurrente, tanto más si también ha sido confirmado el extremo de la resolución de primera instancia en que se dispuso exhortar al Instituto Nacional Penitenciario, en la persona del director del Establecimiento Penitenciario de Arequipa, a efectos de que tome las medidas pertinentes y urgentes en relación con la situación de riesgo por enfermedades preexistentes que refirió el sentenciado recurrente.

Consideraciones finales

En conclusión, de la revisión de la resolución de vista recurrida, no se ha configurado el motivo casacional alegado, esto es, el inciso 1 del artículo 429 del CPP (inobservancia de garantías constitucionales), por lo que es correcta la decisión de la Sala Superior, la cual ha sido debidamente motivada y se ha sustentado en el principio de legalidad e igualdad ante la ley; por lo tanto, corresponde declarar infundada la casación.

DECISIÓN

DECLARARON INFUNDADO el recurso de casación interpuesto por el sentenciado Roberto Víctor Salas Vilca contra la resolución de vista emitida el doce de junio de dos mil veinte por la Sala Superior Mixta de Emergencia de la Corte Superior de Justicia de Arequipa, que confirmó la resolución del siete de mayo de dos mil veinte, expedida por el Juzgado Penal Unipersonal Transitorio Supra provincial de Corrupción de Funcionarios, que declaró improcedente su pedido de conversión de la pena privativa de libertad impuesta en su contra por haber sido condenado como autor de los delitos de peculado y fraude informático, en agravio del Estado; en consecuencia, **NO CASARON** la referida resolución de vista del doce de junio de dos mil veinte .

CONDENARON al recurrente Salas Vilca al pago de costas procesales; en consecuencia, cumpla la Secretaría de esta Sala Suprema con la respectiva liquidación de costas, para su ejecución por el Juzgado de Investigación Preparatoria competente.

DISPUSIERON que, la presente sentencia casatoria sea leída en audiencia pública, se notifique a todas las partes apersonadas en esta sede suprema y, acto seguido, se publique en la página web del Poder Judicial.

MANDARON que, cumplidos estos trámites, se devuelva el proceso al órgano jurisdiccional de origen para los fines de ley.

1.2. Internacionales

1.2.1. Primer antecedente

En el año 2012 el Sr. Albert González fue condenado a 20 años de cárcel, la pena más larga que la justicia norteamericana a impuesto a un cibercriminal. Albert fue el responsable de uno de los delitos informáticos a bancos en los Estados Unidos y usando técnica de SQL injection, sustrajo más de 170 millones de números de tarjetas de crédito y débito con sus respectivas claves de cajeros automáticos.

El Sr. Albert González, en esa época de 28 años de edad, se declaró culpable de tres (3) delitos cibernéticos en el proceso del juicio en el año 2009 por los cuales fue sentenciado separadamente con dos (2) condenas que acumulan mas de 20 años de prisión efectiva.

Comenzó a delinquir con su computadora infiltrándose en los sistemas de pagos electrónicos y computarizados que procesaban las transacciones de miles de establecimientos comerciales en EE.UU.

Usando solo su computadora portátil en una tienda cómodamente se descargaba los números de cuentas de las tarjetas de crédito y débito de los clientes. Con este método robó los datos de las tarjetas con lo que pudo retirar hasta US$200 millones de cajeros automáticos.

El Sr. Albert González logro ser condenado porque residía en Florida, donde el servicio secreto de los Estados Unidos lo pudo ubicar. Sin embargo, trabajaba con dos socios rusos que continúan no habidos por la justicia.

1.2.2. Segundo antecedente

En el año 2013 fue condenado a 24 meses y aplicada a Lewis Martin luego de que fuera encontrado culpable de ingresos no autorizados a diferentes sistemas informáticos. Dentro de los sistemas atacados y vulnerados se encuentran universidades de Inglaterra, páginas web de policías y base de datos del gobierno del Reino Unido y otros sitios de departamentos oficiales del gobierno de Estados Unidos.

2. Desarrollo del tema

2.1. Normatividad actual

- Ley de Delitos Informáticos (y por medios informáticos)
- Código Penal.
- Código Procesal Penal.
- Código de Ejecución Penal.
- Ley 27697, Ley que otorga facultad al fiscal para la Intervención y control de comunicaciones y documentos privados en caso excepcional.
- Ley 28774, Ley que crea el Registro nacional de Terminales de Telefonía Celular, Establece Prohibiciones y Sanciona Penalmente a quienes alteren y comercialicen celulares de procedencia dudosa.
- Ley 28820, mediante la presente Ley se modifican los siguientes artículos del Código Penal, Artículo 281°: Atentado contra la seguridad común; Artículo 283°: Entorpecimiento al funcionamiento de servicios públicos; y, Artículo 315°: Disturbios.
- Ley 29499, Ley que establece la vigilancia electrónica personal.

- Ley 29867, Ley que incorpora diversos artículos al Código Penal relativos a la Seguridad en los Centros de Detención o Reclusión.
- Ley 30076, Ley para combatir la inseguridad ciudadana.
- Ley 30077, Ley contra el crimen organizado.
- Decreto Legislativo 982, que modifica el Código Penal, aprobado por Decreto Legislativo Nº 635.
- Decreto Legislativo 1182, Decreto que regula el uso de los datos derivados de las telecomunicaciones para la identificación, localización y geolocalización de equipos de comunicación, en la lucha contra la delincuencia y el crimen organizado.
- Decreto Legislativo 1218, Regula el uso de las cámaras de video vigilancia.
- Ley 30618, Ley que modifica el DL 1141, DL de fortalecimiento y modernización del Sistema de Inteligencia Nacional – SINA y de la Dirección Nacional de Inteligencia, DINI, a fin de regular la seguridad digital.
- DS 058-2018-PCM: Aprueban la definición de Seguridad Digital en el Ámbito Nacional.
- Decreto Legislativo 1412, Ley de Gobierno Digital.
- Resolución Legislativa 30913. Resolución Legislativa que aprueba el Convenio sobre la Ciberdelincuencia (Convenio de Budapest).
- Ley 30099, Ley de Ciberdefensa
- Decreto de Urgencia 007-2020. .Decreto de Urgencia que aprueba el marco de Confianza Digital y dispone medidas para su fortalecimiento.

2.2. Delitos tipificados en nuestra legislación

- Abuso de mecanismos y dispositivos informáticos: Ley de Delitos Informáticos art. 10, Código Penal 20B
- Acceso a Datos de Tarjetas de Banco: Código Penal art. 196A.5
- Acceso Ilícito: ley de delitos informáticos art. 2
- Acoso Sexual: Código Penal art. 176B
- Actos contra el Pudor: Código Penal art. 176, 183
- Apología del Delito: Código Penal art. 316
- Apología del Terrorismo: Código Penal art. 316A
- Atentados contra el Espectro Radioeléctrico: Código Penal art. 186.7
- Atentado contra Integridad de datos informáticos: ley de delitos informáticos art. 3 Código Penal 220A
- Atentando contra Integridad de Sistemas Informáticos: Ley de Delitos Informáticos art. 4, Código Penal 283
- Atentado contra la seguridad común: Código Penal art. 281
- Atentado contra las Telecomunicaciones: Código Penal art. 186.10, 222A, 281, 283 Atentado contra señales de satélite: Código Penal art. 186A, 194A, 444A
- Calumnia: Código Penal art. 131
- Chantaje: Código Penal art. 201
- Chantaje Sexual: Código Penal art. 177C
- Delitos contra Derechos Intelectuales: Código Penal art. 216, 217, 218, 219, 220, 220A, 220B, 220C, 220D, 220E, 220F, 222, 222A, 223

- Delitos contra la administración pública (equipos electrónicos y teléfonos móviles en penales): Código Penal art. 368A, 368B, 368C, 368D
- Delitos contra la seguridad pública: Código Penal art. 281
- Delitos contra Software: Código Penal art. 220F
- Difamación: Código Penal art. 132
- Discriminación: Código Penal art. 323
- Entorpecimiento al funcionamiento de servicios públicos: Código Penal art. 283
- Espionaje: Código Penal art. 331, 331A
- Estafa / Phishing: Código Penal art. 196, 196A
- Exhibiciones y publicaciones obscenas: Código Penal art. 183
- Explotación sexual comercial infantil y adolescente en ámbito del turismo: Código Penal art. 181A
- Falsedad Ideológica: Código Penal art. 428
- Falsificación de Documentos: Código Penal art. 427
- Fraude Informático: Ley de Delitos Informáticos art. 8
- Delito de grave perturbación de la tranquilidad pública: Código Penal art. 315A.
- Hacking Ético: ley de delitos informáticos art. 12
- Injuria: Código Penal art. 130
- Interceptación de Comunicaciones (Datos Informáticos y Telefónica): Ley de Delitos Informáticos art. 7, Código Penal art 162
- Interferencia de comunicaciones electrónicas, de mensajería instantánea y similares: Código Penal art 162B
- Pánico Financiero: Código Penal art. 249

- Penalización de Clonación o Adulteración de Terminales: Código Penal art. 222A Pornografía Infantil / Pedofilia: Código Penal art. 176A, 182A, 183A
- Posesión o Comercialización de equipos para interceptación telefónica: Código Penal art. 162A
- Publicación en los medios de comunicación sobre delitos de libertad sexual contra niñas, niños y adolescentes: Código Penal art. 182-A.
- Proposiciones a Menores: ley de delitos informáticos art. 5, Código Penal art. 183B Revelación de Secretos Nacionales: Código Penal art. 330
- Suplantación de Identidad: ley de delitos informáticos art. 9
- Tocamientos, actos de connotación sexual o actos libidinosos en agravio de menores: Código Penal art. 176A
- Tráfico de Datos Personales y Bases de Datos: Código Penal art. 154A, 157
- Violación de Correspondencia: Código Penal art. 161, 163, 164
- Violación de Intimidad: Código Penal art. 154, 154B, 156,
- Violación de la libertad de expresión: Código Penal art. 169

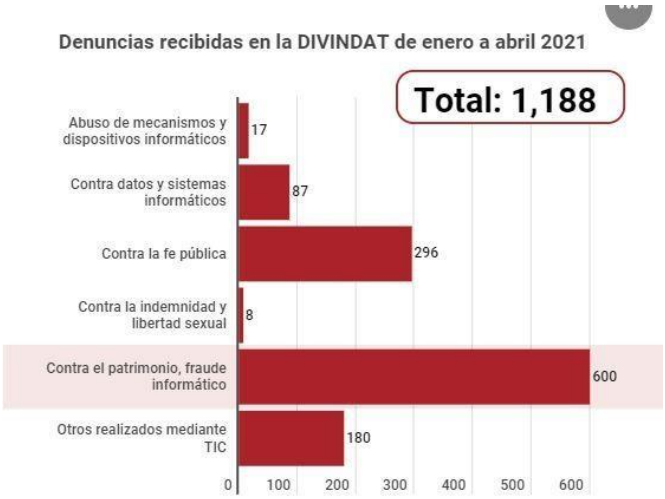
2.3. Nuevos delitos informáticos

Los nuevos delitos informáticos y con el uso masivo del internet y los teléfonos celulares como Smartphone, tabletas, laptops, etc., nos han traído muchos beneficios, en el entorno académico, económico, cultural y social, el cual se ha convertido en una herramienta habitual en nuestra vida cotidiana, que utilizamos diariamente en todas nuestras actividades y no escapa también es el contexto para conductas delictivas.

Ciberdelitos en el Perú

Cada mes se registran cerca de 300 denuncias de delitos informáticos en promedio en la División de Investigación de Delitos de Alta Tecnología (DIVINDAT).

Entre enero y abril del 2021, se investigaron 1,188 denuncias de delitos cibernéticos en la División de Investigación de Delitos de Alta Tecnología (DIVINDAT) de la Policía. Los casos más comunes están relacionados al fraude informático y a la suplantación de identidad.



Fuente: DIVINDAT.

La División de Investigación de Delitos de Alta Tecnología (DIVINDAT), los delitos mas comunes que los ciberdelincuentes utilizan es el correo masivo, las redes sociales como Facebook, paginas falsas y mensajes de texto para estos crímenes informáticos (ciberdelitos). Cada mes se reciben 300 denuncias por fraudes informáticos.

Se registraron 600 investigaciones sobre fraudes informáticos hasta abril de este año, las denuncias que mas se presentan son la clonación de tarjetas, compras fraudulentas por internet, retiros no autorizados o transferencias no autorizadas.

La suplantación de identidad es uno de los nuevos delitos, las investigaciones se duplicaron en el 2020 (de 247 en el año previo a 572 casos) y, hasta abril se han atendido 296 denuncias.

Modalidades frecuentes

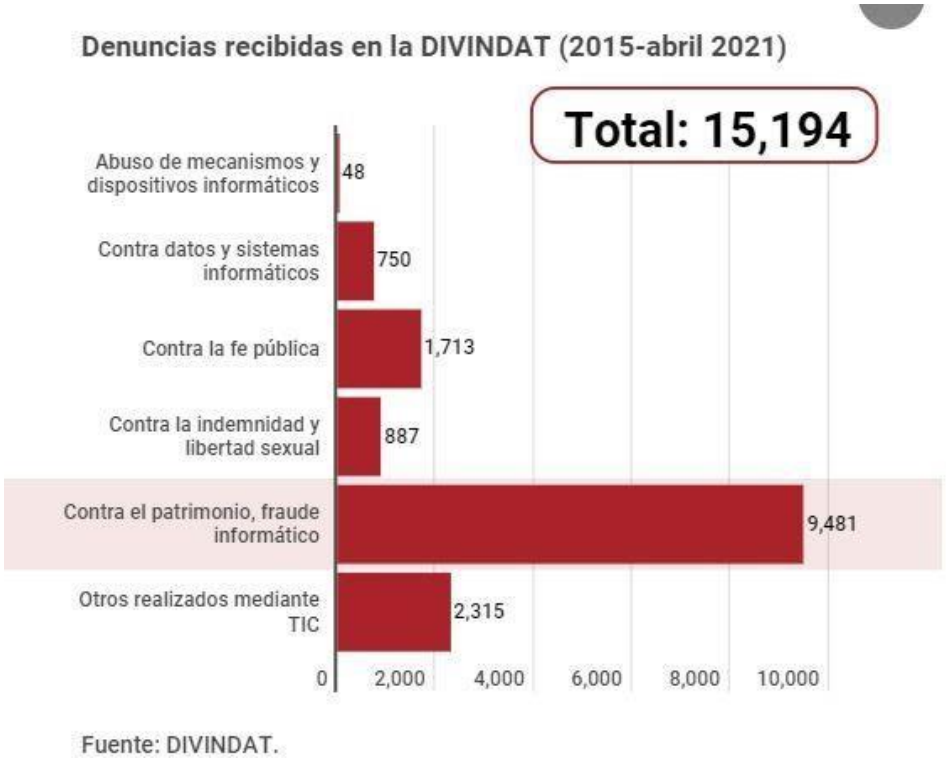
El phishing en el idioma informatico, es una forma que los ciberdelincuentes primero se gana la confianza de las personas y al final la engañan solcitandoles que ingresen a sitios falsos que simulan ser las painas web de los bancos o entidades financieras. Las usuarios son víctimas del fraude y por insistencia llegan a registrar sus datos personales y claves de sus tarjetas de creditos o debitos, con esos datos, los criminales realizan depósitos sin autorización.

Otro forma de delito o fraude, son que los ciberdelincuentes ofrecen productos a muy bajos precios en redes sociales y servicios de mensajerias, registrando informacion de locales comerciales, de ventas exitosas y comentarios que son buenos vendedores, las personas son engañadas para realizar los pagos y luego

los datos de los vendedores son borrados de ese servicio y no pueden ser localizados..

La adulteración de ofertas o descuentos de tiendas comerciales de buen prestigio en línea es cada vez más frecuente. Las personas reciben mensajes de texto y/o notificaciones y acceden a paginas web falsas (clonados) para realizar pagos en línea.

El el cuadro siguiente se observa que las denuncias recibidas en la DIVINDAT.[1] desde el año 2015 hasta abril del 2021 el total de denuncias son un total de 15,194.



Fuente: DIVINDAT.

Fraude informático

[1]https://elperuano.pe/noticia/121876-ciberdelitos-en-el-peru-se-elevan-denuncias-de-fraude-informatico-y-suplantacion-de-identidad

Un total de 1,771 personas han sido víctimas de los ciberdelincuentes según estadísticas de la DIVINDAT, de este total 1582 fueron blancos de transferencias de dinero de sus cuentas bancarias y de 187 utilizaron los datos de sus tarjetas para hacer compras por Internet.

Las transferencias bancarias y compras por Internet presentan el mayor número de denuncias de los ciudadanos y en el mes de diciembre aumenta la incidencia de estos casos. De acuerdo a las estadísticas de la División de Investigación de Alta Tecnología de la DIRINCRI, hasta el 2 de diciembre, han recibido 2,600 denuncias por delito informático y de ellos 1,771 casos corresponden al fraude informático.

DENUNCIAS DIVINDAT	2019	2020
ABUSO DE MECANISMOS Y DISPOSITIVOS INFORMATICOS	2	5
ABUSO DE MECANISMOS Y DISPOSITIVOS INFORMATICOS	2	5
CFP-SUPLANTACIÓN DE INDENTIDAD	206	392
SUPLANTACIÓN DE IDENTIDAD	206	388
SUPLANTACION DE IDENTIDAD VIRTUAL		4
CILS-PROPOSICIONES A NIÑOS, NIÑAS Y ADOLESCENTES CON FINES SEXUALES POR MEDIOS TECNOLÓGICOS	37	67
CONTRA LA INDEMNIDAD SEXUAL DE MENORES		2
PROPOSICIONES A NIÑOS, NIÑAS Y ADOLESCENTES CON FINES SEXUALES POR MEDIOS TECNOLÓGICOS	37	65
CONTRA DATOS Y SISTEMAS INFORMÁTICOS	118	113
ACCESO ILICITO	96	95
ACCESO ILICTO A UNA BASE DE DATOS		2
ATENTADO A LA INTEGRIDAD DE DATOS INFORMÁTICOS	4	4
ATENTADO A LA INTEGRIDAD DE SISTEMAS INFORMATICOS	1	6
ATENTADO CONTRA LA INTEGRIDAD DE DATOS Y SISTEMAS INFORMÁTICOS	17	6
CP-FRAUDE INFORMÁTICO	1761	1771
CLONACIÓN DE TARJETA	23	2
COMPRAS FRAUDULENTAS POR INTERNET	376	187
OPERACIONES Y TRANSFERENCIA ELECTRONICAS Y/O DE FONDOS NO AUTORIZADOS	1362	1582
CONTRA LA INTIMIDAD Y EL SECRETO DE LAS COMUNICACIONES	1	6
INTERCEPTACIÓN DE DATOS		2
INTERCEPTACIÓN DE DATOS PERSONALES		1
TRÁFICO ILEGAL DE DATOS	1	3
TOTAL GENERAL	2125	2354

Fuente: Denuncias de fraude informático de acuerdo a las estadísticas de la DIVINDAT-DIRINCRI.

En el delito de fraude informático están las operaciones y transferencias electrónicas y/o fondos no autorizados que son las estafas y robos que se dan con las tarjetas bancarias. En este caso se han registrado 1,582 denuncias.

En este mismo delito –también con el uso de los datos de las tarjetas bancarias- con la modalidad de compras fraudulentas por Internet ha recibido 187 denuncias, precisó el coronel Mendieta.

Otro grueso de denuncias que ha atendido dicha unidad es el delito de suplantación de identidad en el que 392 personas han sido víctimas de los delincuentes.

Precisiones en torno al riesgo de ataque cibernético y el cybercrimen

¿En qué consisten los ataques cibernéticos? y, desde una perspectiva de corte más jurídico, ¿Qué es el cybercrimen?

Un ataque cibernético puede ser entendido, de manera sencilla, como todo ataque o agresión que se efectué empleando el ciberespacio, el cual puede conllevar a la destrucción de bienes físicos o una afectación puramente virtual, y puede estar motivado por intereses puramente económicos o incluso de orden político (como son, por ejemplo, los casos de cyberterrorismo).

Con relación al cybercrimen o los cyberdelitos, la Unión Europea, a través de la Comisión Europea – Sección de Trabajo contra el cybercrimen, define a este como todo acto criminal o delictivo que se comete de manera online empleando redes de comunicación electrónica y sistemas de información.

Dicha Comisión ha tipificado dichos actos en tres grandes categorías: I) Delitos específicos contra la Internet, tales como ataques contra sistemas informáticos o

phishing (suplantación de identidad); II) Fraude y falsificación online, siendo que tales crímenes a gran escala emplean conjuntamente el robo de identidad, phishing, spam así como códigos maliciosos; y, III) Contenido ilegal online, incluidos pornografía infantil, incitación al odio racial y actos terroristas, así como terrorismo, racismo y xenofobia.

A nivel normativo, uno de los textos más importantes en la materia es el Convenio Sobre Ciberdelincuencia de la Unión Europea, suscrito en Budapest en el 2001, el cual reconoce los siguientes delitos cibernéticos: I) Delitos contra la confidencialidad, la integridad y disponibilidad de los datos y sistemas informáticos (acceso ilícito, interceptación ilícita, ataque a la integridad de los datos, ataque a la integridad del sistema, abuso de los dispositivos); II) Delitos informáticos (falsificación informática y fraude informático); III) Delitos relacionados con el contenido (delitos relacionados con la pornografía infantil); y, IV) Delitos relacionados con infracciones con las infracciones de la propiedad intelectual y los derechos afines (delitos relacionados con infracciones de la propiedad intelectual y afines).

Toda vez que el presente comentario se centra en los ataques a los datos y a los sistemas informáticos, procedemos a dar un sucinto recuento de los tipos de ataques cibernético más comunes en la materia:

- El Malware
- El virus
- Los gusanos
- Los troyanos

- El spyware
- El ransomware
- El spoofing o phishing
- Denegación de servicio distribuido o DoS)
- El cryptojacking.

EXISTEN VACÍOS LEGALES QUE NO PUEDEN SANCIONARSE LOS DELITOS INFORMÁTICOS EN EL NUEVO CÓDIGO PENAL PERUANO

(Sequeiros, 2016)

Las tecnologías de la Información y Comunicaciones (TIC's) han evolucionado y creando nuevas métodos delictivos denominados delitos y fraudes informáticos. Estas nuevas formas de crimen en el Perú han producido nuevas leyes, cuya finalidad es prevenir y sancionar las conductas ilícitas que afectan a las personas, sistemas de información, entidades bancarias, a los secretos de comunicaciones y los demás bienes jurídicos que resulte afectado con esta modalidad delictiva como son el patrimonio, la fe pública y la libertad sexual.

La Ley N° 30096 "Ley de delitos informáticos" fue promulgada el 21 y publicado el 22 de octubre del 2013 en el diario oficial "El Peruano". Luego fue parcialmente modificada por la Ley N° 30171 "Ley que modifica la Ley 30096, Ley de delitos informáticos", promulgada el 9 y publicada el 10 de marzo del 2014.

Bajo este marco normativo se tipifican todos los actos delictivos informáticos, pero como la tecnología avanza cada día más rápido saliendo al mercado nuevos

dispositivos electrónicos que permiten que las personas y empresas adquieran y utilicen para sus procesos y transacciones diarias, hacen que las personas acostumbradas a delinquir se perfecciones y puedan crear nuevas formas de fraudes con el fin de afectar el patrimonio personal y jurídico, por ello nuestras leyes deben actualizarse y estar a la par con la tecnología, como por ejemplo el uso de los drones con cámaras de video incorporadas que en otros países ya los utilizan para delinquir realizando seguimientos espías, robando, utilizados para fraudes y otros métodos delictivos.

Al no actualizar nuestras leyes en delitos y fraudes informáticos va a seguir existiendo vacíos legales y que los delincuentes saben aprovechar para sacarle la vuelta a la ley.

.

2.4. COVID: “Impulsor de la Transformación Digital”

El estado peruano ha impulsado con llegar a ser un país de Gobierno electrónico con el fomento de la Ley de Transformación Digital, la pandemia del COVID-19 aceleró aún más el proceso de transformación digital, y la tecnología fue crucial, no solo para la continuidad de los negocios, sino también para posibilitar que los ciudadanos puedan tener conectividad en sus hogares y puedan interactuar con todas las aplicaciones que desarrolla el estado y la empresa privada, como trabajo remoto, tramites virtuales, asistencia médica y educación a distancia.

Nos encontramos en un momento único en el que las prioridades de las empresas se han diversificado, algunas cambian sus modelos de negocios y otros buscan optimizar procesos para ahorrar costos.

La pandemia fue y es una oportunidad de dinamizar la innovación mediante el aprovisionamiento y la modernización de aplicaciones y herramientas capaces de soportar nuevas plataformas ágiles. Dado el agresivo empuje de la oferta tecnológica, se vuelve favorable transitar un camino transformador que posicione mejor a la organización con miras a la fase de recuperación.

Los primeros pasos se traducen en fomentar la cultura digital y entender que la transformación digital representa procesos. Por ello se debe empezar por identificar cuáles son las áreas que hay que transformar o intervenir con mayor urgencia, dependiendo del objetivo de negocio que se tiene.

Los primeros pasos para realizar transformación digital en las empresas es desarrollar una mentalidad digital; digitalizar procesos, datos y sensores; entender las oportunidades de digitalización; evaluar inversiones; y concentrarse en los clientes en vez de los productos o servicios.

Conclusiones

- Los delitos informáticos van a seguir aumentando si es que el estado, la empresa privada y todos los demás involucrados no tomen conciencia que la transformación digital no es un desafío tecnológico, sino un desafío de negocios y propio de cada persona.
- Los nuevos delitos informáticos van a seguir innovándose y acelerándose cada vez haya más penetración en el mercado de equipos tecnológicos y nuevas aplicaciones que lo soporten y sean más fáciles de utilizar por todas las personas, buscando una celeridad en sus procesos y no tener contacto con las personas por causa de la pandemia COVID-19.
- La transformación digital y gobierno digital ya no es un mito es una realidad que vivimos diariamente y estamos expuestos al igual que todas las actividades que hacemos a riesgos de robo, hurto, falsificación y todos los demás delitos tipificados en nuestra legislación peruana.
- Los factores claves de éxito en una transformación digital son el valor desde la gestión de la información; contar con los líderes correctos y expertos en tecnología digital; desarrollar capacidades para la fuerza laboral del futuro; empoderar a las personas para trabajar de nuevas maneras y adoptar una cultura colaborativa y con mentalidad digital.
- Nuestra legislación actual y el código penal en materia de fraudes y delitos informáticos como lo menciona (Sequeiros, 2016) existen vacíos legales que nuestros legisladores deben resolver y nuestro país no es excepto a esta limitación en materia legal, casi todos los países tiene este problema, debido al

rápido cambio tecnológico y la globalización, pero debemos estar actualizados y poder acortar la brecha de este “vacatio legis”

Aporte de la investigación

La creación de un comité de vigilancia tecnológica integrada por expertos en informática con el fin de estar a la vanguardia con las innovaciones

La creación de un verdadero Equipo de Respuesta a Incidentes de Seguridad (CSIRT) conformado por informáticos certificados en Ethical Hacking y no certificados (desconocidos) con el fin de proveer y anticiparse a los nuevos delitos y fraudes informáticos con el fin de estar preparados ante ilícitos penales.

La creación de tres (3) verdaderos Centro de Operaciones de Seguridad (SOC), uno por parte de la empresa privada, otro por el estado y el tercero por el comando conjunto de las fuerzas armadas del Perú, para velar por la seguridad nacional, ya que las guerras son ahora tecnológicas.

Recomendaciones

Actualizar nuestras leyes en materia de delitos informáticos en nuestro código penal con la finalidad que los que impartan justicia tenga todos los criterios establecidos en nuestra legislación.

Capacitar a los funcionarios que son los encargados de administrar justicia en cursos de delitos y fraudes informáticos, como son el Poder Judicial, Misterio Publico y Fiscalía de la Nación, Policía Nacional y Colegios de Abogados.

Difundir a la población en tener cuidado en el uso de las herramientas tecnologías que utilizan y puedan ser objetos de fraudes y delitos informáticos, tomando énfasis en la protección a los menores de edad.

Masificar el uso de internet brindando conectividad a todos los peruanos mediante enlaces de fibra óptica a nivel nacional – PERU CONECTADO.

Referencias bibliográficas

Sequeiros, I. (2016). VACÍOS LEGALES QUE IMPOSIBILITAN LA SANCIÓN DE LOS DELITOS INFORMÁTICOS EN EL NUEVO CÓDIGO PENAL PERUANO-2015 [Tesis, Universidad de Huánuco]. http://repositorio.udh.edu.pe/123456789/286

Cibercriminalidad y Derecho Penal ABOSO, Gustavo Eduardo y Z APATA, María Florencia (2006). Editorial IB de f. de Montevideo – Buenos Aires. Julio César Faira Editor. Buenos Aires.

Temas de derecho informático: Delitos informáticos, contratación electrónica, protección jurídica de programas informáticos ARBULU MARTÍNEZ, Víctor J. (2002).. CEPREDIM, Centro de Producción Editorial e Imprenta – UNMSM. Lima – Perú.

Los Delitos Informáticos en la Banca: El delito del milenio. Informática y Derecho Bancario.

BLOSSIERS MAZZINI, Juan José y CALDERON GARCÍA, Sylvia B. (2000). Editora R AO S.R.L. Lima – Perú.

El delito Informático en el Código Penal Peruano. Biblioteca de Derecho Contemporáneo.

BRAMONT – ARIAS TORRES, Luis Alberto (1997). Volumen 6. Pontificia Universidad Católica del Perú. Fondo Editorial. Lima – Perú.

ANEXO DE LECTURAS OBLIGATORIAS - CURSO: “DELITOS INFORMATICOS”