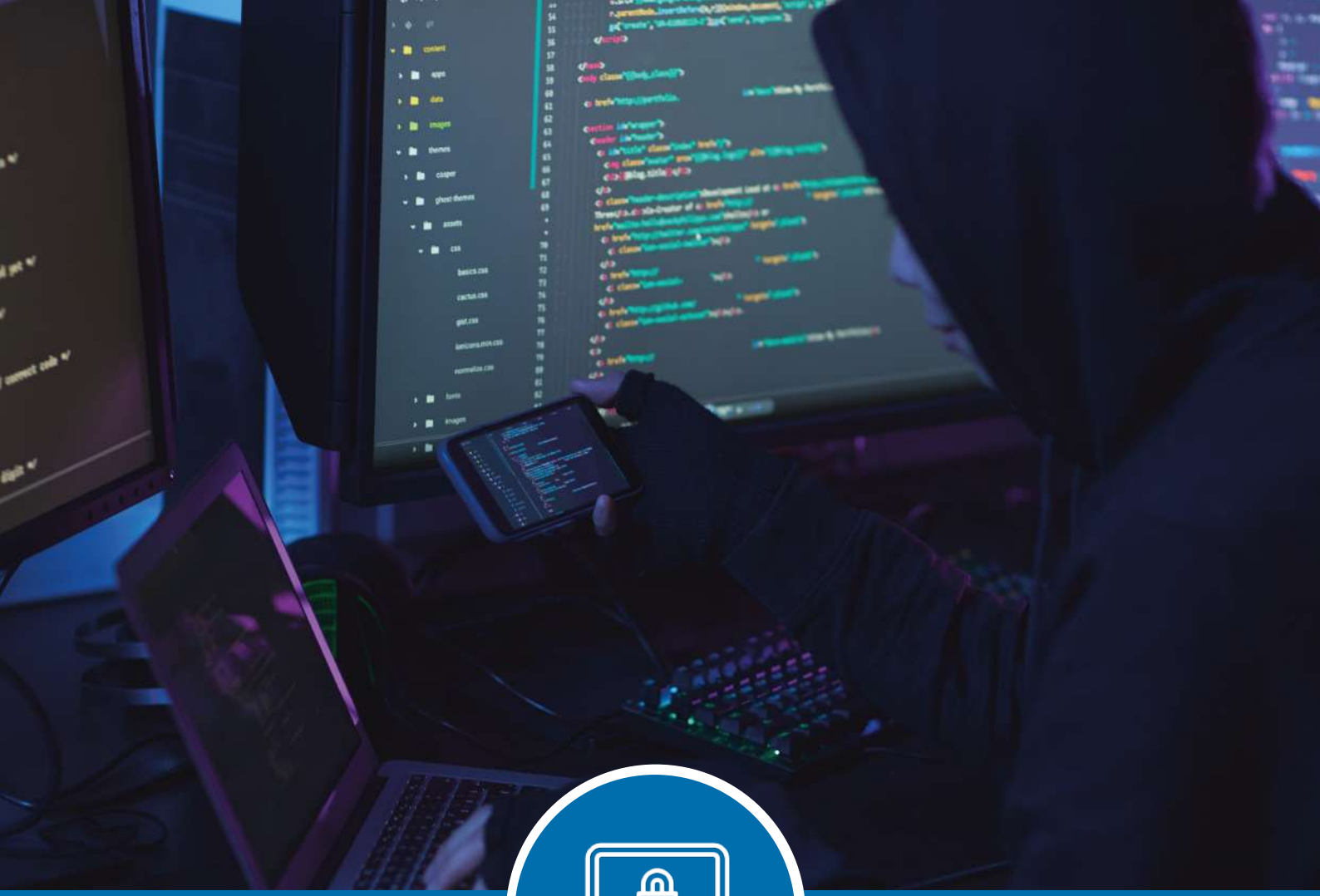

DELITOS
INFORMÁTICOS

Autor:
Percy Huaroc Llaja

DELITOS INFORMÁTICOS

Percy Huaroc Llaja[1]

SUMARIO

I. INTRODUCCIÓN.

Con fecha 03 de mayo del año en curso, fue publicado el Decreto Supremo N° 080-2020-PCM, mediante el cual el Gobierno aprueba el regreso de las actividades económicas progresivamente debido a la aún Emergencia Sanitaria por el COVID-19.

En dicho Decreto Supremo se señala que las actividades correspondientes a la Fase 1 son las relacionadas al comercio electrónico de bienes destinados al hogar.

El comercio electrónico también es conocido como "E-commerce", y este brinda la facilidad de usar plataformas digitales para la actividad empresarial, ya sea vía internet, aplicativos u otra forma digital.

Como sabemos, el E-commerce ya era utilizado por muchos de nosotros, mucho antes del Estado de Emergencia; sin embargo, debido a la nueva "normalidad", personas que aún no tenían un alcance a él, deberán de acostumbrarse, ya que será una nueva forma de adquirir los bienes y servicios.

Toda esta situación nos lleva a la Ley N° 30096, "Ley de Delitos Informáticos", la misma que tipifica las condutas penales que de alguna u otra manera, afecten los sistemas y datos informáticos.

Dentro de los datos informáticos, nos podemos encontrar lo relacionado a la indemnidad y libertad sexual, la intimidad y el secreto de las comunicaciones, el patrimonio y la fe pública. En estos bienes jurídicos, el delincuente hace uso de la tecnología para cometer los diversos ilícitos penales ya normados por nuestro Código Penal.

En este artículo, comentaremos sobre los tipos penales mencionados en la Ley N° 30096, así como los fraudes informáticos relacionados al E-commerce y las recomendaciones a tomar para evitar ser víctima de un delito informático.

[1] Abogado por la Facultad de Derecho de la Universidad Nacional Mayor de San Marcos. Con estudios de post grado en Ciencias Penales. Jefe del área Penal de Torres y Torres Lara Abogados.

II. SOBRE LA LEY DE DELITOS INFORMÁTICOS.

Como es de conocimiento, la Ley Nº 30096, "Ley de Delitos Informáticos", fue publicada en el año 2013 y tuvo como principal objetivo evitar y sancionar las conductas típicas que causen un grave perjuicio al sistema y a los datos informáticos, la indemnidad y libertad sexual, la intimidad y el secreto de las comunicaciones, el patrimonio y la fe pública, en los cuales el delincuente, a través del uso de la tecnología, comete dichos actos ilícitos.

Dicha ley sufrió una modificación a través de la Ley N° 30171, la misma que fue publicada en el año 2014, en la cual se agregó los siguientes tipos penales:

> **Artículo 2°. Acceso ilícito**
> *"El que deliberada e ilegítimamente accede a todo o en parte de un sistema informático, siempre que se realice con vulneración de medidas de seguridad establecidas para impedirlo, será reprimido con pena privativa de libertad no menor de uno ni mayor de cuatro años y con treinta a noventa días-multa. Será reprimido con la misma pena, el que accede a un sistema informático excediendo lo autorizado."*
>
> **Artículo 3º. Atentado a la integridad de datos informáticos**
> *"El que deliberada e ilegítimamente daña, introduce, borra, deteriora, altera, suprime o hace inaccesibles datos informáticos, será reprimido con pena privativa de libertad no menor de tres ni mayor de seis años y con ochenta a ciento veinte días-multa."*
>
> **Artículo 4º. Atentado a la integridad de sistemas informáticos**
> *"El que deliberada e ilegítimamente inutiliza, total o parcialmente, un sistema informático, impide el acceso a este, entorpece o imposibilita su funcionamiento o la prestación de sus servicios, será reprimido con pena privativa de libertad no menor de tres ni mayor de seis años y con ochenta a ciento veinte días-multa."*
>
> **Artículo 7º. Interceptación de datos informáticos**
> *"El que deliberada e ilegítimamente intercepta datos informáticos en transmisiones no públicas, dirigidos a un sistema informático, originados en un sistema informático o efectuado dentro del mismo, incluidas las emisiones electromagnéticas provenientes de un sistema informático que transporte dichos datos informáticos, será reprimido con una pena privativa de libertad no menor de tres ni mayor de seis años.*
>
> *La pena privativa de libertad será no menor de cinco ni mayor de ocho años cuando el delito recaiga sobre información clasificada como secreta, reservada o confidencial de conformidad con la Ley 27806, Ley de Transparencia y Acceso a la Información Pública.*
>
> *La pena privativa de libertad será no menor de ocho ni mayor de diez cuando el delito comprometa la defensa, seguridad o soberanía nacionales.*
> *Si el agente comete el delito como integrante de una organización criminal, la pena se incrementa hasta en un tercio por encima del máximo legal previsto en los supuestos anteriores."*
>
> **Artículo 8º, Fraude informático**
> *"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."

Artículo 10º, Abuso de mecanismos y dispositivos informáticos
El que deliberada e ilegítimamente fabrica, diseña, desarrolla, vende, facilita, distribuye, importa u obtiene para su utilización, uno o más mecanismos, programas informáticos, dispositivos, contraseñas, códigos de acceso o cualquier otro dato informático, específicamente diseñados para la comisión de los delitos previstos en la presente Ley, o el que ofrece o presta servicio que contribuya a ese propósito, será reprimido con pena privativa de libertad no menor de uno ni mayor de cuatro años y con treinta a noventa días-multa."

Y modifica:

Artículo 5°, Proposiciones a niños, niñas y adolescentes con fines sexuales por medios tecnológicos
"El que a través de internet u otro medio análogo contacta con un menor de catorce años para solicitar u obtener de él material pornográfico, o para llevar a cabo actividades sexuales con él, será reprimido con una pena privativa de libertad no menor de cuatro ni mayor de ocho años e inhabilitación conforme a los numerales 1, 2 y 4 del artículo 36 del Código Penal.
Cuando la víctima tiene entre catorce y menos de dieciocho años y medie engaño, la pena será no menor de tres ni mayor de seis años e inhabilitación conforme a los numerales 1, 2 y 4 del artículo 36 del Código Penal."

En la mayoría de los artículos se incorpora los términos "deliberada e ilegítimamente", señalando que dichos tipos penales se cometen de manera dolosa; por tanto, no cabe la culpa en ello. El agente o delincuente debe tener la conciencia y voluntad de diseñar, introducir, alterar, borrar, suprimir, clonar, interferir o manipular de forma ilegítima el funcionamiento de un sistema informático.

Por delitos informáticos, se entiende que son *"aquellas conductas dirigidas a burlar los sistemas de dispositivos de seguridad, esto es, invasiones a computadoras, correos o sistemas de datas mediante una clave de acceso; conductas típicas que únicamente pueden ser cometidas a través de la tecnología. En un sentido amplio, comprende a todas aquellas conductas en las que la Tecnología de la Información y Comunicación (TIC) son el objetivo, el medio o el lugar de ejecución, aunque afecten a bienes jurídicos diversos (...)"*[2]

Respecto al bien jurídico se protege "(...) *la información, pero está considerada de diferentes formas, ya sea como un valor económico, como un valor intrínseco a la persona, por su fluidez y tráfico jurídico, y finalmente por los sistemas que la procesan o automatizan"*[3]

[2] VILLAVICENCIO TERREROS, Felipe. Delitos Informáticos. Revista IUS ET VERITAS. Lima, 2014, N° 49, pp. 286-287.
[3] ACURIO DEL PINO, Santiago. Delitos Informáticos. Generalidades. pp. 20-21.

En ese sentido, es necesario también proteger los bienes jurídicos comunes que afectan, tales como el patrimonio, la fe pública, la indemnidad sexual y otros. Por tanto, nos encontramos ante un delito pluriofensivo, ya que afecta varios bienes jurídicos.

III. DELITO DE FRAUDE INFORMÁTICO.

3.1 Del Tipo penal y los sujetos activo y pasivo.

El fraude informático es un tipo penal de resultado; es decir que no es suficiente realizar las conductas típicas relatadas, sino que es necesario que ese comportamiento cause un perjuicio económico.

El sujeto activo de este este ilícito puede ser cualquier persona, quien actúa en contra de cualquier persona natural o jurídica (sujeto pasivo).

Este delito también se clasifica como un delito de resultado y también es válido únicamente de forma dolosa; ya que, el delincuente debe tener la conciencia y voluntad de suplantar la identidad de una persona natural o jurídica, ocasionando un perjuicio económico.

3.2 De las modalidades.

A fin de evitar ser víctima de fraude informático, es necesario conocer las modalidades:

- ***Clonación de tarjetas de crédito:*** Conducta delictiva cometida *"mediante aparatos electrónicos de lectura de bandas magnéticas (skimmer) donde malos empleados de restaurantes, gasolineras y otros locales extraen los datos de la tarjeta de crédito. Luego, son copiados a una computadora portátil o personal y, finalmente, copiados a otra tarjeta clonada con los mismos datos personales de la tarjeta original."*[4]

- ***Phishing:*** Conducta delictiva *"diseñada con la finalidad de robarle la identidad al sujeto pasivo. El delito consiste en obtener información tal como números de tarjetas de crédito, contraseñas, información de cuentas u otros datos personales por medio de engaños."*[5]

- ***Spear Phishing o Phishing segmentado:*** Conducta delictiva muy parecida al Phishing; sin embargo, esta modalidad tiene como sujeto pasivo a grupos vulnerables como por ejemplo a adultos mayores.

- ***Transferencias electrónicas fraudulentas:*** Conducta delictiva "*mediante la modalidad del "phishing", donde el timador busca que alguien revele información confidencial personal que puede ser usada para robarle su dinero, luego de obtener la información*

[4] ACURIO DEL PINO, Santiago. Delitos Informáticos. Generalidades. pp. 24-25.
[5] AMERICAN BAR ASSOCIATION (ABA)-Rule of Law Initiative. Proyecto de Apoyo al Sector Justicia. Taller de Investigación Criminal y Litigación Oral Especializado en Delitos Informáticos - Cybercrime (diapositiva).

necesaria para acceder a la cuenta del banco y procedan a efectuar operaciones fraudulentas por internet."[6]

- ***Compras por internet mediante información de tarjetas de crédito o débito***: Esta conducta delictiva se comete cuando el delincuente observa a su víctima realizar una compra vía wifi y aprovecha en sustraer la información de la tarjeta para posteriormente realizar compras en cualquier página de internet.

- ***Vishing:*** Conducta delictiva "*en la cual el sujeto activo envía un SMS haciéndose pasar por una entidad bancaria, pidiendo bajo alguna excusa que te comuniques con algún teléfono falso o respondas el SMS con información confidencial (número de tarjeta o clave secreta)."*[7]

- ***Ransomware:*** Conducta delictiva *"que utiliza un tipo de malware (software malintencionado) que los criminales instalan en las PC sin consentimiento y bloquean el equipo desde una ubicación remota (…) a fin de que el ordenador se bloquee."*[8]

- ***Smishing:*** Aquella conducta en la que el delincuente utiliza los mensajes de texto para enmascarar el número de teléfono y, muestra en el contenido del mensaje, un texto de instituciones.

De acuerdo con la División de Alta Tecnología (DIVINDAT) de la Policía, en el año 2019, se han registrado un promedio de 3100 denuncias de fraude electrónico, pornografía infantil, suplantación de identidad y otros.

La mayoría de los casos se centra en delitos contra el patrimonio, tales como fraudes informáticos, estafas, etc., como lo son las transacciones no autorizadas o no seguras vía internet (pagos, cobros y transferencias) a través de compras fraudulentas o clonación de tarjetas. Es recomendable verificar la veracidad de la tienda virtual en la que están realizando la compra.

También encontramos las denuncias en las que se hace uso de las redes sociales, las que usualmente nos solicitan hagamos transferencias a cuentas de otro.

Asimismo, encontramos también dentro de esos, el acoso sexual, amenazas desde mensajes o redes sociales, también denominadas extorsión.

Finalmente, encontramos lo que es la suplantación de identidad, lo cual es usado generalmente para un acercamiento a menores de edad, ello con fines sexuales, lo que nos lleva a denuncias de pornografía infantil.

[6, 7 y 8] AMERICAN BAR ASSOCIATION (ABA)-Rule of Law Initiative. Proyecto de Apoyo al Sector Justicia. Taller de Investigación Criminal y Litigación Oral Especializado en Delitos Informáticos- Cybercrime (diapositiva). Consulta: 20 de mayo de 2020.

IV.RECOMENDACIONES.

Se recomienda evitar acceder a plataformas digitales o páginas web que nos solicite datos bancarios, esto es, el PHISHING, ya que el delincuente buscará la manera de que su víctima le brinde información sobre sus cuentas con engaños, ya sea enviando enlaces o con enlaces de páginas web falsas que aparentemente parecieran ser sitios web de entidades bancarias. En este caso, es necesario señalar que ninguna entidad bancaria solicita usuario o contraseña.

Finalmente, otra situación que suele pasar y debe evitarse es guardar las claves de nuestra banca móvil en los teléfonos celulares, en la billetera o en los bolsos; esta es una conducta negligente ya que el delincuente tendrá los datos necesarios para llevar a cabo sus ilícitos, lo que afectará gravemente el patrimonio del sujeto pasivo.