SEMINARIO SAYÁN
ABOGADOS

LOS DELITOS INFORMÁTICOS EN LA ACTUALIDAD PERUANA

***Gustavo Seminario Sayán**
Socio Principal en Seminario Sayán Abogados

I. INTRODUCCIÓN.-

La época de aislamiento social dispuesta por el Gobierno en la emergencia sanitaria por el COVID-19 - Coronavirus, perfila un cambio en la forma de actuar de la sociedad. Antes, era normal tener entrevistas con magistrados y con funcionarios públicos a efectos de, en determinados horarios, explicar cualquier aspecto procesal o sustantivo relacionado con un caso bajo su competencia; con clientes, colegas y proveedores, a efectos de tratar temas relacionados con sus acuerdos comerciales; directores y accionistas de empresas, respecto al desarrollo comercial de éstas; profesores, alumnos y amigos, sobre temas académicos y/o personales; entre otros. Esta forma de reunión o audiencia ha cambiado. Durante la cuarentena, cualquier reunión o conferencia tiene que ser virtual. Lo que nos interesa es analizar lo que creemos sucederá en la época post confinamiento, en la que las personas, con la intención de mantener una distancia social prudente con los demás, evitarán tener reuniones y entrevistas en forma física, y las ejecutarán virtualmente. La información se transmitirá a través de las redes informáticas.

Si bien nos encontramos en la era de la digitalización, la coyuntura sanitaria ha acelerado y acrecentado el uso de la informática. Las empresas -aquellas que cuentan con las condiciones- han ingresado a un proceso intenso de informatización, al que se han visto forzadas por la situación de emergencia. Empresas grandes y pequeñas de todo rubro, Estudios de Abogados, Contadores, Ingenieros, Arquitectos, Constructores, Restaurantes, en general, en todos los sectores, formal e informal, están implementando con mayor intensidad la plataforma informática para seguir siendo competitivos. Lo mismo está ocurriendo en la administración pública.

Toda esta información, que se tratará, intercambiará y almacenará a través de las redes, es susceptible a actos delictivos – Delitos Informáticos-. Para las empresas y corporaciones, así como para las personas naturales, muchos de esos datos tienen valor, pues reflejan estrategias comerciales, toma de decisiones empresariales, niveles de inversión, planes tarifarios, relación de clientes, acciones legales, costos, además de información personal íntima / sensible y en muchos casos confidencial, que, en manos de delincuentes, podría ser de gran perjuicio económico o reputacional.

Dependiendo de la cantidad y calidad de la información, es de prever que los delincuentes desarrollarán métodos que les permitan tratar de vulnerar las medidas de seguridad informática de determinadas personas, naturales o jurídicas, con la finalidad de ingresar a sus sistemas y acceder a sus datos. No sólo nos referimos a acciones que vulneran sistemas informáticos o datos informáticos, sino, como lo reconoce la norma peruana, también a acciones que transgredan otra clase de bienes jurídicos, tales como la libertad e indemnidad sexual, patrimonio, intimidad, incluso bienes jurídicos como la libertad -en la prevención de secuestros, coacciones-, u otras conductas como extorsiones y chantajes.

Como indica RODRIGUEZ GOMEZ, el abaratamiento de los equipos informáticos, el perfeccionamiento de las infraestructuras de comunicación, la mejora en la formación de los usuarios y las mayores posibilidades ofrecidas por la tecnología han contribuido decisivamente a que internet se convierta en un medio de comunicación usual, en un vehículo de transmisión e intercambio de todo tipo de información. Su incorporación a la vida económica y social ofrece innumerables ventajas, como la mejora de la eficiencia empresarial, el incremento de las posibilidades de elección de los usuarios, la aparición de nuevas fuentes de empleo, un mayor acceso a la cultura, más rapidez en las comunicaciones, facilita las transacciones comerciales y la transmisión de información, en el campo de la educación, mejora las posibilidades de los consumidores, reduce los obstáculos para la creación y distribución de contenidos, ofrece un amplio acceso a fuente de información digital cada vez más ricas[1]; procesar datos en forma rápida y segura, almacenar información en grandes cantidades, realizar comunicaciones en tiempo real, contribuir en el aprendizaje a partir de la generación y publicación de información (contenidos) en Internet, aprendizaje interactivo, impulsar el trabajo desde casa, como el Teletrabajo[2]; transacciones comerciales, pagos electrónicos, gestión de negocios, control de procesos, transferencias de dinero, adquisición y venta de productos, etc. Pero, la implantación de Internet y de nuevas tecnologías trae consigo, también, numerosos inconvenientes y peligros.[3]

Por la coyuntura y viendo el nivel de exposición al riesgo que esto conlleva, es importante detenernos a estudiar "Los Delitos Informáticos en la actualidad Peruana". Estos delitos tienen una naturaleza particular y distinta de los convencionales, puesto que pueden ser cometidos por cualquier persona desde un ordenador, un celular, una Tablet, un reloj electrónico, u otro aparato electrónico, desde cualquier lugar del mundo; siendo nuestra labor analizar cuáles son las conductas sancionadas penalmente por el ordenamiento jurídico peruano y cuándo será necesaria la intervención de la justicia penal.

[1]RODRIGUEZ GOMEZ, Carmen – Universidad de Salamanca. "Criminalidad y Sistemas Informáticos". En: El sistema penal frente a los retos de la nueva sociedad, Coordinadores María Rosario Diego Díaz-Santos y Eduardo A. Fabián Caparrós. Edit. Colex. XV Congreso. España, 2003. Pág. 139.

[2] https://www.consejosgratis.net/beneficios-de-la-informatica/

[3]RODRIGUEZ GOMEZ, Carmen – Universidad de Salamanca. "Criminalidad y Sistemas Informáticos". En: El sistema penal frente a los retos de la nueva sociedad, Coordinadores María Rosario Diego Díaz-Santos y Eduardo A. Fabián Caparrós. Edit. Colex. XV Congreso. España, 2003. Pág. 139.

Por ejemplo, durante el desarrollo de los Juegos Panamericanos y Parapanamericanos Lima 2019, se detectaron más de 43,000 incidencias de ataques cibernéticos, los cuales fueron bloqueados y reportados.[4] En julio de 2018 hackers atacaron a los bancos peruanos. La Asociación de Bancos del Perú (Asbanc) anunció que se activaron los protocolos de seguridad. En un comunicado, Asbanc confirmó una serie de ataques financieros que buscaba vulnerar la seguridad de los bancos.[5]

De acuerdo con lo publicado en el Diario Oficial El Peruano del 17 de enero 2020, cada mes hay más de 250 denuncias de delitos informáticos en el Perú. Durante el 2019 se registraron 3,012 de ellas a escala nacional; la mayor cantidad de denuncias se concentra en el delito contra el patrimonio. Los fraudes informáticos y sus subtipos alcanzaron 2,097 denuncias durante el 2019; del total, 1,641 denuncias se centran en transacciones no autorizadas vía internet. También hubo 431 casos de compras fraudulentas y 25 de clonación de tarjetas de crédito o débito; le siguen las denuncias en las que los atacantes emplearon herramientas digitales como redes sociales, software y otras plataformas en línea. En esta categoría hubo 268 denuncias en el 2019, mientras que el año previo tuvo 362 registros; el acoso sexual, las estafas en línea, amenazas desde mensajería o redes sociales o la extorsión agrupan la mayor cantidad de denuncias; la suplantación de identidad es otra amenaza digital frecuente en el Perú, con 247 casos en el 2019. Por otro lado, las proposiciones a niños, niñas y adolescentes con fines sexuales desde mecanismos digitales o las denuncias de pornografía infantil sumaron 237.

La incidencia de correos con información engañosa se ha incrementado en un 25% en la época de cuarentena.[6] Son varios los correos que circulan en internet que pretenden alertar a la comunidad sobre riesgos del COVID-19, bajo el nombre de alguna entidad gubernamental. Sin embargo, esta información puede ser una herramienta utilizada por cibercriminales para robar la información de quienes acceden a los archivos adjuntos enviados.[7]

En el 2019 el Perú se ha adherido a la Convención sobre Cibercriminalidad del Consejo de Europa o Convención de Budapest[8] (mediante Resolución Legislativa Nro. 30913 de febrero

[4] https://andina.pe/agencia/noticia-lima-2019-mas-43000-incidencias-ciberseguridad-fueron-bloqueadas-782219.aspx

[5] https://larepublica.pe/economia/1300366-asbanc-bancos-peru-sufrieron-ataques-ciberneticos/

[6] https://elcomercio.pe/economia/peru/covid-19-coronavirus-peru-como-evitar-ser-victima-de-ciberataques-teletrabajo-internet-pandemia-nndc-noticia/

[7] https://elcomercio.pe/tecnologia/tecnologia/coronavirus-los-crimenes-ciberneticos-que-se-propagan-con-el-virus-noticia/

[8] Este convenio nos establece las siguientes definiciones:

a) por "sistema informático" se entenderá todo dispositivo aislado o conjunto de dispositivos interconectados o relacionados entre sí, cuya función, o la de alguno de sus elementos, sea el tratamiento automatizado de datos en ejecución de un programa;

de 2019, ratificada a través del Decreto Supremo N° 10-2019-RE de marzo de 2019). El convenio es un mecanismo de cooperación judicial entre los estados miembros con la finalidad de proteger a la Sociedad frente a la ciberdelincuencia. La suscripción de este Convenio es coherente con una política de lucha contra la Delincuencia Informática, puesto que ayudará en las investigaciones a obtener cooperación internacional y ser más efectivos para prevenir y sancionar los actos que pongan en peligro la confidencialidad o integridad de los sistemas, redes o datos entre otros delitos informáticos.

II ACERCA DE LA INFORMÁTICA, SISTEMAS Y DATOS INFORMÁTICOS.-

La informática permite almacenar y alternar grandes cantidades de información, mientras las telecomunicaciones enlazan a personas situadas en lugares alejados entre sí, con sorprendente facilidad en breve tiempo.[9] Un Sistema Informático es un conjunto de partes interrelacionadas: hardware, software y personal informático, que permite almacenar y procesar información.

El software incluye al sistema operativo, firmware y aplicaciones, siendo especialmente importante los sistemas de gestión de bases de datos. Es un conjunto de programas, instrucciones y reglas informáticas que permiten ejecutar distintas tareas en una computadora; se considera que el software es el equipamiento lógico e intangible de un ordenador. El hardware es el conjunto de componentes físicos de los que está hecho el equipo[10]. Por su parte, la informática se refiere al procesamiento automático de información mediante dispositivos electrónicos y sistemas computacionales. Internet es una red informática de nivel mundial que utiliza la línea telefónica para transmitir información.[11]

Según Gonzales Rus, un sistema informático está formado tanto por elementos *lógicos* como por elementos *físicos*; expresiones que se utilizan aquí en sentido técnico estricto, sino como referencias genéricas inútiles para concretar los componentes u objetos que constituyen en cada caso el objeto de ataque de la conducta delictiva. Con la expresión "elementos lógicos" se alude al *software* en general y a los ficheros o archiveros en los que se recogen datos, información o documentos electrónicos, cualquiera que sea su contenido concreto.

b) por "datos informáticos" se entenderá toda representación de hechos, información o conceptos expresados de cualquier forma que se preste a tratamiento informático, incluidos los programas diseñados para que un sistema informático ejecute una función;
c) por "proveedor de servicios" se entenderá: i. toda entidad pública o privada que ofrezca a los usuarios de sus servicios la posibilidad de comunicar a través de un sistema informático, y ii. cualquier otra entidad que procese o almacene datos informáticos para dicho servicio de comunicación o para los usuarios del mismo;
d) por "datos relativos al tráfico" se entenderá todos los datos relativos a una comunicación realizada por medio de un sistema informático, generados por este último en tanto que elemento de la cadena de comunicación, y que indiquen el origen, el destino, la ruta, la hora, la fecha, el tamaño y la duración de la comunicación o el tipo de servicio subyacente

[9] En PÉREZ LÓPEZ, Jorge. Delitos regulados en Leyes especiales regulares. Gaceta Jurídica. Lima. 2009. P. 80. Haciendo referencia a: Suarez Tejera, Yoruaanys (2011). La estafa por informáticos en el Derecho Penal cubano. En Derecho Penal Contemporáneo. Revista Internacional Nro. 34. P.82.

[10] https://definicion.de/software/

[11] https://es.wikipedia.org/wiki/Internet

Dentro de la referencia quedan comprendidos, pues, los "datos, programas o documentos electrónicos". Con la locución "elementos físicos" hace referencia al *hardware* comprendido de los componentes mecánicos, eléctricos, radioeléctricos, electrónicos, magnéticos u ópticos que forman un ordenador o equipo informático. Por "sistema informático", en fin, se entiende el conjunto integrado de elementos lógicos y físicos que permiten el almacenamiento y tratamiento de la información. Dentro del término, pues, quedan comprendidos las "redes, soportes o sistemas informáticos".[12]

En tal sentido, el sistema informático está conformado por un componente inmaterial, constituido por los datos y programas informáticos que hay en el sistema (elementos lógicos), y otro material, que está compuesta por los objetos físicos, la PC, la lap top, etc, que son los que contienen y permiten el almacenaje y procesamiento de la información.

III. LOS DELITOS INFORMÁTICOS: ANÁLISIS DE LA LEY 30171.-

La lucha frente a la criminalidad informática desborda naturalmente el campo exclusivo del Derecho penal, pues se trata de un fenómeno cuyo control reclama además otros instrumentos más amplios y complejos (de tipo jurídico – no penal – de tipo técnico, formativo, así como educativo)[13]. El espectro de conductas calificables de delito informático es amplísimo. La cuestión fundamental es encontrar el criterio delimitador para esta categoría de comportamientos[14]

La Ley 30171 (en adelante la Ley de Delitos Informáticos o la Ley) define y regula los delitos informáticos en el Perú. Esta norma sanciona dos grupos de conductas: **1)** la intrusión o ataque a sistemas informáticos y datos informáticos, **2)** ataques a otros bienes jurídicos -tales como la libertad e indemnidad sexual, patrimonio, intimidad, secreto de las telecomunicaciones, interceptación de datos informáticos, abuso de mecanismos y datos informáticos-, siempre y cuando su vulneración se realice mediante tecnologías de la información y de la comunicación.

La Ley contempla como delitos informáticos conductas que atacan, manipulan, destruyen o inutilizan sistemas o datos informáticos (lo que, como veremos más adelante, se denomina "sabotaje informático"), y, también, conductas que afectan bienes jurídicos convencionales

[12] GONZALES RUS, Juan José. "Naturaleza y ámbito de aplicación del delito de daños en elementos informáticos (artículo 264.2 del Código Penal)". La Ciencia del Derecho Penal ante el Nuevo Siglo. Libro en homenaje al Profesor Doctor Don José Cerezo Mir. Madrid, España. Edit. Tecnos. 2002. Pág.1281.

[13] RICARDO MATA Y MARÍN. Universidad de Valladolid. En Actualidad Penal Nro. 37. "Criminalidad Informática: una introducción al cibercrimen". Doctrina XXXVI. 2003. Pág. 935.

[14] NURIA MATELLANES RODRÍGUEZ, Universidad de Salamanca. En: Hacia un derecho penal sin fronteras. "Algunas notas sobre las formas de delincuencia informática en el Código Penal". Coordinadores María Rosario Diego Díaz-Santos y Virginia Sánchez López. Edit. Cólex. 2000.

como la libertad e indemnidad sexual, el patrimonio, la intimidad, entre otros, cuando la conducta se haya realizado a través de las tecnologías de la informática y la comunicación.

Rodríguez Gómez afirma que podemos hablar de delitos cometidos por medio de sistemas informáticos, y delitos cometidos contra sistemas informáticos, en los primeros entrarían todo tipo de conductas convencionales, se trataría de delitos tradicionales pero que se lesionan ahora a través de este nuevo medio tecnológico. Nos referimos a la estafa, delitos contra la intimidad, propiedad, falsificación, etc. En los segundos, nos referimos a ataques al bien informático en si, por ejemplo, el software, la seguridad de un sistema, el hardware. Según sostiene, se añade un tercer un grupo de casos, en los que la tarea que desempeña un sistema informático a la hora de ejecución de un delito, además de las citadas, es la de ser instrumento del delito, por ejemplo, como simple soporte de la información cuyo interés para la justicia es meramente probatorio (por ejemplo, discos duros en donde una banda terrorista guarda información estratégica)[15].

No constituirá sabotaje informático la destrucción de elementos físicos de un equipo informático en los que no se contienen datos (monitor, impresora, disco de almacenamiento vacío, etc.), ni tampoco, en rigor, la simple alteración del funcionamiento del sistema informático que afecta al procesamiento de la información, pero que se produce afectando únicamente a los elementos físicos del equipo. Por eso, según GONZALES RUS, resulta más exacta la definición de sabotaje informático propuesta por ROMEO CASABONA: la destrucción o inutilización del elemento lógico o físico de un ordenador con el fin inmediato de imposibilitar la utilización de la información procesada o almacenada. Con este concepto se comprenden pues, los casos en que se destruyen elementos lógicos, tanto si ello se hace mediante la destrucción de sistemas informáticos completos mediante la específica de equipos datos, programas y documentos electrónicos. [16]

Lo relevante en la delincuencia informática referida al "sabotaje informático" lo constituye las funciones de procesamiento, transmisión y ejecución de programas propios del ordenador, con independencia de que la manipulación de estas funciones sea el medio o el objeto de la agresión ilegitima. Con ello, se elimina del ámbito de la delincuencia informática todas aquellas conductas que no afecten a alguna de las funciones citadas.[17]

La inutilización, manipulación u otra conducta en contra de los sistemas o datos informáticos propiamente dichos, puede efectuarse ingresando ilícitamente a los sistemas y redes

[15] RODRIGUEZ GOMEZ, Carmen – Universidad de Salamanca. "Criminalidad y Sistemas Informáticos". En: El sistema penal frente a los retos de la nueva sociedad, Coordinadores María Rosario Diego Díaz-Santos y Eduardo A. Fabián Caparrós. Edit. Colex. XV Congreso. España, 2003.

[16] GONZALES RUS, Juan José. "Naturaleza y ámbito de aplicación del delito de daños en elementos informáticos (artículo 264.2 del Código Penal)". La Ciencia del Derecho Penal ante el Nuevo Siglo. Libro en homenaje al Profesor Doctor Don José Cerezo Mir. Madrid, España. Edit. Tecnos. 2002.

[17] NURIA MATELLANES RODRÍGUEZ, Universidad de Salamanca. En: Hacia un derecho penal sin fronteras. "Algunas notas sobre las formas de delincuencia informática en el Código Penal". Coordinadores María Rosario Diego Díaz-Santos y Virginia Sánchez López. Edit. Cólex. 2000.

informáticas directamente en contra de éstos, o atacando los componentes y equipos físicos que los contienen (incluye cualquier dispositivo de comunicación, que abarca radio, televisión, teléfonos celulares, computadoras, laptop, USB, TV Smart, Tablet, sistemas satelitales, sistemas de GPS, u otro elemento del "hardware"), en los cuales se almacenen, desarrollen, soporten, estos sistemas o datos informáticos. Los delitos informáticos abarcan y sancionan penalmente todas estas conductas.[18]

Cuando la norma penal se refiere a la protección de bienes jurídicos convencionales, como la libertad e indemnidad sexual, el patrimonio, la intimidad, etc., establece que las conductas sancionables se deben ejecutar utilizando Tecnologías de la Información y la Comunicación (TIC). Las TIC están referidas a la integración de las telecomunicaciones (líneas telefónicas y señales inalámbricas) y las computadoras, así como el software necesario, el middleware (software que se sitúa entre un sistema operativo y las aplicaciones que se ejecutan en él), almacenamiento, sistemas audiovisuales, que permitan a los usuarios acceder, almacenar, transmitir y manipular información.[2]

La utilización ilegal de tecnologías de la comunicación e información puede permitir el acceso a sistemas informáticos o bases de datos de empresas o personas naturales, y obtener información como, por ejemplo, la tarifa en la que vende a sus clientes planes telefónicos, la relación de personas afiliadas a determinado servicio, planes estratégicos de expansión o fusión de empresas, montos de dinero que las empresas ofertarán en subastas o licitaciones, información íntima que lleve a extorsiones, secuestros; entre otros.

Pensemos en una empresa prestadora de servicios públicos, de luz, agua, de telecomunicaciones, de cable o internet, que tiene miles y millones de usuarios, cuyo sistema informático se vea vulnerado para manipular información relacionada con la deuda de sus usuarios, o para conocer información de los planes que tienen sus clientes y venderla a la competencia. Pensemos en una Universidad, en la que se manipulen los exámenes de ingreso que se analizan a través del sistema informático; en las entidades bancarias, educativas, de salud, notarías, etc. El problema se agrava si se trata de instituciones públicas, como, por ejemplo, la lista de requisitoriados registrados en el sistema de la Policía Nacional del Perú, en planes del Ministerio del Interior, datos de SUNAT, de los Registros Públicos, etc.

Los sistemas informáticos deben tener sistemas y códigos de seguridad acordes a la magnitud y dimensión de cada uno, sin embargo, siempre estarán los ciberdelincuentes tratando de vulnerarlos con la finalidad de hacerse de beneficios ilícitos sin ser detectados. Esto nos lleva a la pregunta, ¿si la empresa instala un código de seguridad de muy fácil vulneración y éste es vulnerado, estaremos ante un delito informático? La respuesta es sí, estaremos ante la comisión de un delito informático, pues la vulneración de cualquier código de seguridad, de cualquier manera, configura delito.

[18] GONZALES RUS. Ob. Cit.

Las conductas prohibidas por la Ley de Delitos Informáticos son:

A. RESPECTO DEL SISTEMA INFORMÁTICO[19] Y DATOS INFORMÁTICOS[20]:

- Acceder ilícitamente a un sistema informático, sin autorización y vulnerando medidas de seguridad; y acceder a un sistema informático excediendo lo autorizado.

- Dañar, introducir, borrar, deteriorar, alterar, eliminar o volver inaccesibles datos informáticos.

- Inutilizar total o parcialmente, entorpecer o imposibilitar el funcionamiento o la prestación del servicio de un sistema informático.

- Impedir el acceso a un sistema informático, a través de tecnologías de la información o comunicación.

Según Tellez Valdez, los delitos informáticos deben comprender las siguientes acciones: Acceso no autorizado, uso ilegítimo de passwords, la entrada a un sistema informático sin la autorización del propietario; destrucción de datos; infracción a los derechos de autor de base de datos, uso no autorizado de información almacenada en una base de datos; Intervención de e-mail, lectura de un mensaje electrónico ajeno; fraudes electrónicos; transferencia de fondos; spamming o envío masivo de correos electrónicos en forma deliberada, con el propósito de bloquear un sistema; espionaje; terrorismo[21] [22].

[19] Sistema informático: *Todo dispositivo aislado o conjunto de dispositivos interconectados o interrelacionados entre sí, cuya función, o de alguno de sus elementos, sea el tratamiento automatizado de datos en ejercicio de un programa.*

[20] Datos informáticos: *Toda representación de hechos, información o conceptos expresados de cualquier forma que se preste a tratamiento informático, incluido los programas diseñados para que un sistema informático ejecute una función.*

[21] TELLEZ VALDEZ, Julio. Instituto Tecnológico y de Estudios Superiores de Monterrey, Campus Estado de México. "Derecho Informático". Tercera Edición.

[22] A continuación pasaremos a señalar algunas de estas conductas, como se verá algunos encajan en algunos de los tipos del Código Penal y otras no tienen ninguna relevancia desde el punto de vista penal. 1. Intrusismo Informático. Podríamos entender por intrusismo informático la entrada en un sistema o en un ordenador sin consentimiento, como una especie de allanamiento de morada. El denominado hacking "blanco", sin animo especial alguno, simplemente por curiosidad o de paseo por placer (joyring) y de reto constante a modo de desafío intelectual del intruso para descubrir la vulnerabilidad del sistema, pero, sin intentar explorar en beneficio propio los puntos débiles del sistema (hackito ergo sum). Su tratamiento varía de los ordenamientos jurídicos; 2 Espionaje Informático: Debemos entender la obtención, sin autorización, de datos almacenados en fichero informático. El Código penal contempla esta acción en distintos artículos, diferenciando a) La obtención, sin el consentimiento del titular de datos personales que violen secretos o vulneren la intimidad. b) Y entre la obtención de datos, cuya finalidad sea descubrir secretos de una empresa, mediante la utilización de documentos escritos o electrónicos, soportes informáticos u otros objetos que conlleve un perjuicio a la misma recogida. 3) Sabotaje informático (delito de daños): Se trataría de interferencias en el funcionamiento adecuado del sistema, mediante la inserción, transmisión, alteración, daño o supresión de datos informáticos. El daño informático puede producirse tanto a la parte física del ordenador (hardware) como a la parte lógica del mismo (software). Los daños al software pueden producirse a través de elementos electromagnéticos, la introducción de virus o una bomba lógica que destruya, altere o inutilice los programas, datos o documentos electrónicos almacenados en el sistema informático.

De acuerdo a la Ley, las conductas descritas deben realizarse ilegal y deliberadamente. Esto significa que quien realiza la conducta no debe tener autorización del titular, y debe actuar dolosamente. Si tales conductas se realizan con la autorización del titular del sistema informático, no estaremos ante una conducta delictiva. El titular de un sistema informático puede instalar -o pedir que instalen- un virus en el mismo que se active si es que algún intruso quiere ingresar ilícitamente en sus redes; o un desarrollador de sistemas puede preferir destruir determinado sistema construido en vez de permitir que su competencia lo conozca. Ello no configuraría delito. La norma penal establece como necesaria la ilegitimidad de la conducta, la cual se ve reflejada en la falta de autorización de parte del titular.

B. RESPECTO DE LOS OTROS BIENES JURÍDICOS PROTEGIDOS POR LOS DELITOS INFORMÁTICOS.-

La Ley de Delitos Informáticos también protege otros bienes jurídicos como la indemnidad y libertad sexual, intimidad, el patrimonio, la interceptación de datos informáticos, entre otros, siempre y cuando estos delitos se hayan cometido a través de tecnologías de la información o de la comunicación. Las conductas prohibidas por la norma son:

- Indemnidad y libertad sexual: Contactar a menores de 14 años para solicitar u obtener de él material pornográfico, o para llevar a cabo actividad sexual; y cuando la víctima tiene entre 14 y 18 años y medió engaño.

- Contra la intimidad y el secreto de las telecomunicaciones: Crear, ingresar o utilizar indebidamente una base de datos de una persona -natural o jurídica-, para comercializar, traficar, vender, promover, favorecer, facilitar información relativa al ámbito personal, familiar, patrimonial, laboral, financiero o de otra naturaleza. Es indiferente para la norma si dicha conducta crea o no un perjuicio.

- Interceptación de datos informáticos en transmisiones privadas, secretas, reservadas o confidenciales (no públicas dice la norma) dirigidas a un sistema informático, originadas en un sistema informático, o efectuadas dentro de un sistema informático.

4) Cyberterrorismo (como subespecie del sabotaje). El descubrimiento y análisis de los modos de convergencia entre el mundo real y el mundo virtual es el primer paso para determinar qué tipos de actos terroristas pueden ser realizados. Un ejemplo de estos modos, donde tenemos convergencia entre realidad y virtualidad, es el sistema de control aéreo de un país desarrollado; otros serían el control de subterráneos y trenes, sistemas de distribución de energía eléctrica y gas, sistemas de comunicación, sistemas bancarios y financieros, el sistema informático de un sistema de un hospital. Todos estos nodos son susceptibles de ser atacados y perturbados por medio de la intrusión al sistema, infectándolo con el virus, bombas lógicas o troyanos (caballo de Troya) simplemente cambiando información o programas. La otra forma de atacar la infraestructura de información es destruyendo físicamente las computadoras por medio de las armas silenciosas, las armas del pulso electromagnético ya descritas. Los efectos físicos (de pérdidas humanas y materiales) de estos ataques pueden ser incalculables, pero fundamentalmente el objetivo del atentado cyber-terrorista será minar la confianza de los habitantes en la sociedad en la que viven, transmitir un mensaje claro: nadie está a salvo, y todo es posible de ser infiltrado, trastocado, corrompido y desestabilizado. RODRIGUEZ GOMEZ, Carmen – Universidad de Salamanca. "Criminalidad y Sistemas Informáticos". En: El sistema penal frente a los retos de la nueva sociedad, Coordinadores María Rosario Diego Díaz-Santos y Eduardo A. Fabián Caparrós. Edit. Colex. XV Congreso. España, 2003. Pág. 139.

- Se incluyen las transmisiones electromagnéticas provenientes de un sistema informático que transporte datos informáticos.

- Se agrava la pena si el delito compromete la seguridad, defensa o soberanía nacional.

- Patrimonio: Diseñar, introducir, alterar, borrar, suprimir o clonar datos informáticos con la finalidad de generar un provecho ilícito, en perjuicio de tercero.
  Interferir o manipular el funcionamiento de un sistema informático con la finalidad de generar un provecho ilícito, en perjuicio de tercero.

- Se agrava la pena cuando el patrimonio afectado es del Estado, destinado a fines asistenciales o programas de apoyo social.

- Abuso de mecanismos y dispositivos informáticos: Fabricar, diseñar, desarrollar, vender, facilitar, distribuir, importar u obtener, mecanismos, programas informáticos, dispositivos, contraseñas, códigos de acceso o cualquier otro dato informático diseñado y que sea utilizado para cometer delitos.

Existe una agravante que eleva la pena hasta en un tercio, cuando el agente forma parte de una organización criminal; comete abuso de la posición especial de acceso a la data o información reservada, o accede a ésta por el cargo o función que ejerce; busca un beneficio económico no estipulado en la norma específica; o cuando el delito compromete fines asistenciales, de seguridad o de soberanía nacional.

La norma precisa que el Fiscal, atendiendo a la naturaleza y gravedad del delito, puede autorizar la participación de agentes encubiertos para fines de la investigación, o de cualquier delito que se cometa mediante la utilización de tecnologías de la comunicación, no siendo necesario que forme parte de una organización criminal.

Entonces, tenemos que cualquier conducta que vulnere sistemas informáticos o datos informáticos en forma ilegal, mediante tecnologías de la información y comunicación, para utilizarlos, manipularlos, copiarlos, eliminarlos, sin autorización del titular, será un delito informático. Las diferencias que presentan estos ilícitos con los delitos comunes reafirman la necesidad de detenernos a estudiar esta materia. Tenemos la posibilidad de su comisión a distancia; las dificultades probatorias; la reticencia de las empresas afectadas a denunciar el hecho por miedo a desprestigiarse; la posibilidad de programar su ejecución automática para determinada fecha y en general su inadecuación a las normas penales vigentes.[23]

Un tema relevante es el nivel probatorio que requiere un delito de esta naturaleza. El Juez o el Fiscal, por más especializados que sean, son abogados de formación, no técnicos o ingenieros informáticos. Siempre deberán actuar sobre la base de elementos objetivos, como

[23] PALAZZI, Pablo Andrés. "Delitos Informáticos". Primera Edición. 2000. Buenos Aires. Argentina.

los informes periciales informáticos. Se trata de informes emitidos por (profesionales o instituciones) técnicos especializados, quienes, luego de estudiar los elementos relacionados con lo que se investiga, podrán indicar, por ejemplo, si hubo o no una intrusión al sistema, cuándo se dio, cómo, desde qué ordenador, etc. Al igual que en un delito de homicidio se requiere de un Informe de necropsia, en el delito de Lavado de Activos o Estafa un informe contable, o en una falsificación de firmas o de documentos un informe pericial grafotécnico, en los delitos informáticos se requerirá de un Informe Pericial Informático, emitido por un (profesional o institución) técnico especializado, que explique si se cometió la conducta y cómo.

En una investigación, cada parte podrá designar un perito - técnico informático, y la Policía, Fiscalía o Juzgado podrán designar un perito oficial. El valor que el funcionario público dará a cada informe dependerá de su solidez, de los argumentos objetivos, así como de la solvencia del perito o de los peritos que lo emiten. Ese es un tema de valoración probatoria.

IV. LA COMPETENCIA TERRITORIAL EN LOS DELITOS INFORMÁTICOS.-

En la investigación de los delitos informáticos, será importante delimitar la competencia territorial. Suele ocurrir que, con la finalidad de evitar ser detectados o dificultar las investigaciones, los delincuentes actúan a través de una PC ubicada en otro país, o incluso en forma remota desde un tercer país, produciéndose los daños en el Perú.

Este tema lo trata ABOSO, poniendo un caso como ejemplo del razonamiento que deberá realizarse en este tipo de situaciones. El 20 de noviembre de 2000, el Tribunal de Gran Instancia de Paris afirmó su jurisdicción para asumir competencia en una denuncia formulada por las asociaciones "Unión de Estudiante Judíos de Francia", al considerar ilegal que la empresa de informática "Yahoo! Inc.", y su filial "Yahoo Francia", ofrezcan para la venta, en su sitio web "Auctions", artículos relacionados con la cultura nacional socialista imperante en Alemania durante el régimen de III Reich-, los libros de "Mein Kampf" de Adolf Hitler y "Los Protocolos de los sabios de Sion"; además de diversos artículos centrados en la negación del Holocausto y de los campos de concentración. Según los denunciantes, ello favorecía la propagación del antisemitismo. Más allá de la conclusión de fondo, en lo que se refiere a la competencia, el Tribunal sostuvo que si bien la conducta de ofertar esos productos se decidió y ejecutó fuera de Francia, los tribunales franceses eran competentes puesto el daño ocurrió en Francia, por tanto, el hecho se cometió en territorio francés,.[24].

En nuestra legislación, el Código Penal en su artículo 1 estatuye que la Ley Penal peruana se aplica a todo el que comete un hecho punible en el territorio de la República; mientras que en el artículo 5 precisa que el lugar de la comisión de un delito es aquel en el cual el autor o partícipe ha actuado u omitido la obligación de actuar, o en el que se producen sus efectos.

[24] Gustavo Eduardo ABOSO y María Florencia ZAPATA. "Cibercriminalidad y derecho penal". Edit. Julio César Faira. 2006. Buenos Aires, Argentina.

En tal sentido, si tenemos, por ejemplo, que la acción de intrusión en el sistema informático de una empresa peruana se realiza desde un ordenador ubicado en Estados Unidos, la jurisdicción penal Peruana es competente debido a que, al haberse producido los efectos en el Perú, el delito se considera cometido en el Perú.

V. RECOMENDACIONES. MEDIDAS PREVENTIVAS QUE PUEDEN ADOPTARSE.-

Como sostiene MATELLANES RODRÍGUEZ, es un hecho que solo una pequeña parte de los ilícitos informáticos se descubren, y cuando ello ocurre, suele ser de una manera fortuita y usualmente no se denuncian, siendo la cifra negra de la criminalidad informática excepcionalmente alta. Según ella, las causas que contribuyen a explicar por qué se da de esa manera son diversas, entre ellas la complejidad técnica de los sistemas informáticos; el desconocimiento de las altas tecnologías por los propios directivos de las empresas, que les obliga a abandonarse en manos de técnicos y especialistas; la centralización de elementos del sistema, así como la falta de documentos escritos de las operaciones realizadas, lo cual facilita que no se "dejen huellas"; la confianza "mítica" en la infalibilidad del ordenador; la insuficiencia de medidas de seguridad incorporadas a los equipos por los fabricantes[25].

Para prevenir ser víctima de la comisión de Delitos Informáticos, es necesario adoptar algunas acciones, como: ***a)*** no abrir correos de cuentas desconocidas o que claramente parezcan un spam, ***b)*** no abrir datos adjuntos a correos que no tengan relación alguna con el trabajo, ***c)*** en horario de trabajo únicamente utilizar correos de trabajo, para evitar que se filtre algún virus a través del correo personal del trabajador, ***d)*** cláusulas contractuales muy específicas y claras al respecto, ***f)*** publicar internamente el código de ética de la empresa y el "*compliance informático*", ***g)*** que el área de seguridad informática de la empresa tenga personal debidamente capacitado, ***h)*** verificar que el programa de seguridad que utilice sea el adecuado, ***i)*** que el área de seguridad informática de la empresa mantenga un control de los accesos***, j)*** que verifique que los códigos cambien cada cierto tiempo, para evitar la acción de trabajadores que se fueron descontentos y pudieron conocer información, ***k)*** que el área de seguridad informática haga un seguimiento al nivel de acceso de conformidad con los códigos asignados, ***l)*** que se realice una capacitación permanente del personal de la empresa encargado de la seguridad informática, entre otros.

En el Diario Gestión se publicó una entrevista a uno de los Socios de la firma Deloitte Perú, denominada "*Ciberataques: cinco claves para evitar ser una víctima en época de cuarentena*"[26], en la que da algunas recomendaciones interesantes para evitar ser víctima de

[25] NURIA MATELLANES RODRÍGUEZ, Universidad de Salamanca. En: Hacia un derecho penal sin fronteras. "Algunas notas sobre las formas de delincuencia informática en el Código Penal". Coordinadores María Rosario Diego Díaz-Santos y Virginia Sánchez López. Edit. Cólex. 2000.

[26] https://gestion.pe/tendencias/ciberataques-cinco-claves-para-evitar-ser-una-victima-en-epoca-de-cuarentena-noticia/

ataques informáticos. Por lo específico de sus indicaciones, las detallaremos textualmente: ***1)*** los riesgos cibernéticos aumentan al realizar trabajo remoto o desde casa (home office), por lo que las empresas deben identificar y clasificar los requisitos de conexión remota, reconociendo los riegos relacionados y confirmando rápidamente el umbral de seguridad del negocio permitido bajo esta situación. ***2)*** Gestión de permisos y accesos. Es clave tener una visión integral de las identidades privilegiadas dentro de sus entornos de Tecnologías de la Información, incluido un procedimiento para detectar, prevenir o eliminar cuentas huérfanas; refinar la granularidad del monitoreo de seguridad y enriquecer el monitoreo en escenarios de operación remota; asimismo, se debe dar seguimiento a la operación de las funciones de gestión de ciberseguridad e identificar cuáles de éstas puedan llegar a estar fuera de servicio y los retrasos que se presenten en la respuesta de seguridad. En cuanto a la protección de datos privados de los empleados, las empresas deben controlar el acceso, transmisión y uso de dichos datos en el proceso de estadísticas de información de salud y gestión de empleados; finalmente, deben establecer el nivel de protección de datos clínicos y médicos, evitando el uso de plataformas de terceros para su almacenamiento o transmisión. ***3)*** Cuidado con difundir noticias falsas. Ante las constantes amenazas, se debe tener cuidado al manejar cualquier correo electrónico con asunto, archivo adjunto o hipervínculo relacionado con COVID-19; además, se debe utilizar fuentes confiables, como sitios web legítimos del gobierno para obtener información actualizada y basadas en hechos sobre COVID-19 (esto se debe replicar a cualquier asunto). También se recomienda no revelar información personal o financiera en el correo electrónico y no responder a solicitudes de correo para esta información. ***4)*** Herramientas seguras para la colaboración en línea. Para las empresas que no han implementado soluciones de colaboración y acceso remoto y no cuentan con oficinas remotas a gran escala, deberán evaluar el alcance y modelo de colaboración empresarial remota en función del tamaño de la compañía y las características de la industria. Seleccionar herramientas de colaboración razonables; clarificar el alcance del acceso a servicios de oficina; y mejorar el monitoreo de seguridad y protección de los servicios y sistemas de información de la empresa. ***5)*** Capacitaciones en línea sobre seguridad informática. Para empresas con acceso remoto flexible y soluciones de colaboración ya implementadas, deben llevar a cabo actividades de concienciación y entrenamiento de seguridad de la información y ciberseguridad; además, es clave realizar seguimiento oportuno de accesos sospechosos y situaciones anormales; centrar la atención en garantizar instalaciones de servicio que proporcionen acceso remoto y colaboración de forma segura.

En otra nota publicada por el Diario Gestión, denominada "*Correos con información engañosa aumentó 25% en cuarentena, según EY Perú*"[27], en la que se realiza una entrevista a uno de los socios de la firma EY Perú, proporciona las siguientes recomendaciones: actualizar con la última versión de anti-malware las máquinas del personal y de los servidores de aplicación en las empresas; tener un antivirus instalado y actualizado en el computador, celular o Tablet; revisar siempre la fuente la información; confiar únicamente en fuentes

[27] https://gestion.pe/economia/correos-con-informacion-enganosa-aumento-25-en-cuarentena-segun-ey-peru-nndc-noticia/

oficiales; evitar a toda costa las fuentes de información que solicitan ingresar a un link o a una página específica, mucho menos si piden alguna información a cambio (datos personales, contraseñas o datos bancarios); revisar el remitente, normalmente los correos maliciosos vienen de remitentes similares a los ya conocidos; evitar abrir correos que obliguen a tomar una acción determinada en un corto período de tiempo; evitar a toda costa correos que a cambio de una información ofrezcan recompensa; evitar replicar mensajes de dudosa procedencia, entre otros.

Asimismo, en la publicación del Diario Oficial El Peruano del 17 de enero 2020, se precisa que, para evitar fraudes electrónicos, no se debe proporcionar datos personales en internet, no ingresar a correos electrónicos con contenido sospechoso o no visitar webs peligrosas. Las entidades bancarias no piden en línea información privada. Sólo hacer compras en internet desde tiendas virtuales que tengan un certificado de seguridad, casos en los cuales la dirección web empieza con "HTTPS", y se muestra un candado en la barra de navegación. Al crear un usuario, colocar una contraseña que incluya caracteres especiales, letras en mayúscula y minúscula, así como números. Cambiar la clave frecuentemente y evitar repetirla en más de un servicio; entre otros.

Nuestra recomendación es que las empresas, corporaciones, o personas naturales, insertadas al mundo de la informática, implementen lo que se denomina un "*compliance informático*"; el cual consiste en el desarrollo de protocolos técnico-informáticos y legales, la implementación de una política de mantenimiento de los estándares de seguridad y el perfeccionamiento y supervisión del cumplimiento efectivo de las acciones diseñadas.

Estos datos pueden ayudarnos prevenir, a título personal o corporativo, ser víctima de Delitos Informáticos.

Para consultas y mayor información comunicarse al 9999-69815 y/o al correo electrónico estudio@ss-abogados.com.