Los delitos informáticos y su relación con la criminalidad económica

Renzo Vinelli Vereau*
Universidad de Lima, Lima, Perú

Recibido: 22/3/2021 Aprobado: 29/3/2021
doi: https://doi.org/10.26439/iusetpraxis2021.n053.4995

RESUMEN. En los últimos meses se han consolidado las operaciones comerciales virtuales como las transferencias realizadas a través de los monederos digitales, lo que demuestra claramente una transformación sin retorno de nuestra convivencia socioeconómica común. Desde marzo del 2020 hasta la fecha, nos enfrentamos a un nuevo modo de adquisición de activos, pago de servicios e incluso formas de trabajo. Esta "evolución" hacia el mundo informático y virtual ha aportado muchos beneficios. Sin embargo, también ha generado innumerables dificultades. Uno de los problemas más relevantes y significativos son las actividades delictivas cometidas a través de los sistemas informáticos, las cuales han sido debidamente reguladas por nuestro legislador nacional en la Ley 30096, Ley de Delitos Informáticos, modificada por la Ley 30171. El presente artículo abordará los delitos de fraude informático y suplantación de identidad, que son los más frecuentes en esta nueva convivencia socioeconómica. Asimismo, se analizará la vinculación entre los delitos informáticos y la criminalidad económica.

PALABRAS CLAVE: delito informático / cibercrimen / pluriofensivo / fraude informático / suplantación de identidad / *pishing-pharming* / transnacional

INFORMATIC CRIMES AND THEIR RELATION TO ECONOMIC CRIME

ABSTRACT. In the past few months, virtual commercial operations have been consolidated. For example, transferences made though "digital purses", which clearly proves a transformation with no return of our common social-economic coexistence. Since March of 2020, we have faced a new form of assets acquisition, payment of services, and even new ways of working. This "evolution" to the virtual world has brought many benefits.

* Abogado por la Universidad de San Martín de Porres, Perú. Máster en Derecho Penal por la Universidad de Sevilla, España. Profesor de derecho penal de la Facultad de Derecho de la Universidad de Lima. Agradezco a mi asistente José Miguel Molina Cayo por su apoyo para la realización del presente trabajo.

However, it has also generated countless difficulties. One of the most relevant and significant problems are the criminal activities committed through computer systems, which have been properly regulated by our national legislator in the Law 30096 —Law of Informatic Crimes—, modified by the Law 30171. The present article will approach informatic fraud and identity theft, which are the most frequent crimes in this new social-economic coexistence. Likewise, we will analyze the link between informatic crimes and economic criminality.

KEYWORDS: informatic crimen / cybercrime / multioffensive / informatic fraude / identity theft / pishing-pharming / offshore

INTRODUCCIÓN

¿Cuántos hemos adquirido bienes y servicios a través de nuestros teléfonos móviles, *tablets* o computadoras a raíz de la pandemia generada por el COVID-19? ¿Cuántos hemos cancelado servicios básicos de nuestros domicilios a través de una aplicación en nuestros celulares? Estas preguntas no tendrían respuestas tan contundentes hace aproximadamente cinco años, cuando nuestra sociedad no confiaba y no se encontraba preparada para las operaciones comerciales virtuales, las transferencias bancarias y diversas operaciones realizadas a través de un sistema informático.

Ciertamente, según los datos del Banco Central de Reserva, los instrumentos de pagos distintos del efectivo ascendieron a 958 000 millones de soles y, de enero a mayo del 2020, se incrementaron en 18 % las operaciones efectuadas a través de la banca virtual (como se citó en "Transferencias electrónicas crecieron 13 % a mayo, mientras uso de tarjetas de crédito cayó 25 %", 2020). Es evidente que nos encontramos ante una nueva forma de convivencia económica en donde predomina el sistema informático. No obstante, esta "evolución" también conlleva la proliferación de una nueva criminalidad económica que sugiere que los operadores del derecho se encuentren plenamente capacitados para combatirla.

Pues bien, los medios de comunicación han permitido que la sociedad conozca de primera mano esta proliferación de nuevas organizaciones criminales dedicadas a la comisión de delitos informáticos. Solamente para tomar conciencia de la gravedad de estos ilícitos penales, resulta pertinente destacar algunas cifras: entre enero y la primera semana de agosto del 2020 se registraron 1 481 963 ataques de *pishing* en el Perú y un promedio de 7000 ataques diarios. Por otro lado, de enero a julio del 2020 se presentaron 1117 denuncias de fraude informático. De estas, 974 fueron por operaciones o transferencias electrónicas no autorizadas y 142 por compras fraudulentas en internet. No cabe la menor duda de que nuestra sociedad ha ingresado a un nuevo sistema de intercambios y de relaciones comerciales, y, por ende, también a una nueva forma de criminalidad.

ANÁLISIS GENERAL DE LOS DELITOS INFORMÁTICOS

Definición de los delitos informáticos

Villavicencio Terreros (2014) refiere que los delitos informáticos o criminalidad informática:

> [...] 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 las TIC son el objetivo, el medio o el lugar de ejecución, aunque afecten a bienes jurídicos diversos; y que plantea problemas criminológicos y penales, originados por las características propias del lugar de comisión. (p. 286)

Por su parte, Rayón Ballesteros y Gómez Hernández (2014) explican que por ciberdelito o cibercrimen debe comprenderse:

> [...] cualquier infracción punible, ya sea delito o falta, en el que se involucra un equipo informático o internet y en el que el ordenador, teléfono, televisión, reproductor de audio o video o dispositivo electrónico, en general, puede ser usado para la comisión del delito o puede ser objeto del mismo delito. (p. 211)

Ahora bien, Davara (1993) define los delitos informáticos o *computer crimes* como "la realización de acciones que, reuniendo las características que delimitan el concepto del delito, son llevadas a cabo utilizando un elemento informático o vulnerando los derechos del titular del mismo, ya sea de *hardware* o de *software*" (p. 318). Adicionalmente, Morillas Fernández (2017) refiere que existen tres posiciones que definen el delito informático:

> La primera posición, denominada *concepción amplia*, destaca que la delincuencia informática se encuentra conformada por conductas novedosas para el derecho penal, cuya única característica especial radica en el empleo de la computadora, por lo que un buen número de figuras penales podría convertirse en delito informático en la medida en que se recurra a este medio para la consumación del hecho punible. La segunda posición, denominada *posición intermedia*, cuenta con los postulados del autor González Rus, quien señala que son hechos en los que el sistema informático o sus elementos son el objeto material del delito y aquellos otros en los que son el instrumento del mismo. La tercera posición ha sido denominada *concepción restringida* y concibe el delito informático como cualquier acto ilegal que requiere del conocimiento de la tecnología informática para su perpetración, investigación y persecución, de tal forma que el empleo mismo del medio informático caracterice a la conducta, brindándose así una valoración autónoma al delito informático que le permite su diferenciación respecto de un ilícito penal común que utilice como medio de comisión a la computadora. (pp. 27-28)

Nuestra postura se inclina a la concepción restringida del delito informático, toda vez que, como la gran mayoría de autores resaltan, la comisión de un delito a través de un medio tecnológico de *hardware* o *software* no configura *per se* un delito informático, sino que para ello resulta necesario que se establezcan ciertas características; de lo contrario, se estaría caracterizando un delito de manera inadecuada; por ejemplo, si una persona brinda ciertas declaraciones ofensivas a través de sus redes sociales, no se podría concluir que existe un delito contra el honor en concurso con un delito informático.

Morillas Fernández (2017) ha establecido ciertas características que deberán tener los hechos delictivos para tipificarlos como delitos informáticos:

- Son delitos cometidos a distancia, sin contacto físico entre agresor y víctima, en los que prima la separación temporal y espacial.
- Se trata de una tipología criminal transfronteriza. La propia esencia de internet o del ciberespacio la lleva implícita. Los delitos informáticos son cometidos cada vez en mayor medida por las redes de telecomunicación internacionales, por lo que se podría afirmar que este tipo de ilícitos penales complica las técnicas de investigación debido a su alta complejidad.
- Se vale del creciente número de usuarios y la facilidad de acceso al medio tecnológico para alterar datos o destruir sistemas informáticos. Otro factor determinante es la rápida difusión de información a través de este medio tecnológico a muy bajo costo, lo que permite a las organizaciones delictivas perpetrar delitos con mayor facilidad.
- La falta de jerarquía en la red, lo que dificulta la verificación de la información que circula por este medio.
- El anonimato del perjuicio protegido, la facilidad para encubrir el hecho y la disminución del riesgo de que el autor sea descubierto, gracias a la posibilidad de borrar todas las huellas, sin dejar rastro perceptible, una vez perpetrada la acción delictiva. Esto dificulta su percepción tras la comisión de un ilícito penal por este medio.
- Los autores poseen conocimientos informáticos avanzados.
- La indeterminación de las víctimas, toda vez que los destinatarios del delito son una pluralidad de personas. Puede ser que el victimario realice la acción ilícita sin siquiera conocer quiénes serán los destinatarios de esta, como ocurre en el *pishing*, que consiste en la búsqueda ilícita de datos personales del sujeto, como claves de acceso a servicios bancarios, suplantando la identidad de una entidad financiera, imitando o copiando su logo, con la finalidad de solicitar la introducción de claves de acceso, lo que permitiría la disposición de los activos de la víctima.

Existe una elevada cifra negra de la criminalidad por las dificultades en la averiguación y en la comprobación del almacenamiento, procesamiento y transferencia de datos, y también por el desconocimiento o la ignorancia de haber sido víctima de un ataque informático (Morillas Fernández, 2017, pp. 32-34). Sobre este aspecto, Morón Lerma (2016) precisa que los hechos ilícitos pasan inadvertidos por la víctima. En la mayoría de las ocasiones, los incidentes son descubiertos aleatoriamente, debido a revisiones rutinarias, meses o incluso años después de que haya tenido lugar la intrusión original, o debido a controles realizados *ad hoc* al detectar rutinas extrañas. Además, en aquellos casos en los que se descubre el hecho, la víctima suele actuar con solidaridad criminosa, esto es, no reportando el incidente (p. 36).

Cabe señalar, de acuerdo con Morón Lerma (2016), que el "cibercrimen es un sector en el que todavía no se dispone de una terminología homogénea y uniforme". Agrega que "uno de los inconvenientes principales en el abordaje de la materia radica en la multivocidad de conceptos fundamentales, como pueden ser incidente informático o cibercrimen" (p. 37). Adicionalmente, la autora destaca que "existe una evidente continuidad en la vulnerabilidad de redes y sistemas, es decir, los ilícitos resultan cada vez más frecuentes, diversos y peligrosos. Los programas maliciosos son constantemente modificados para evitar ser detectados por herramientas de seguridad" (p. 39).

Bien jurídico

Los delitos informáticos son delitos considerados pluriofensivos, puesto que como bien jurídico principal (o más importante) tenemos la información almacenada, comprimida, transmitida a través de los sistemas informáticos (Villavicencio Terreros, 2014 p. 288); o la seguridad de la información contenida en las bases de datos, sistema o red de computadoras; o la seguridad en el tráfico jurídico de la información que transita en su interior (Peña Cabrera Freyre, 2008, p. 501). El segundo bien jurídico tutelado es el patrimonio o la intimidad. No obstante, es evidente que el bien jurídico principal son los que se encuentran plenamente vinculados a los sistemas informáticos.

Villavicencio Terreros (2014) refiere que en los delitos informáticos:

> No se puede establecer a la información como el único bien jurídico afectado, por ser el principal y el más importante, sino a un conjunto de bienes que son afectados, debido a la característica de la conducta típica en esa modalidad delictiva que colisiona con diversos intereses colectivos. (p. 288)

Bajo este argumento, coincidimos también con Pérez López (2019), quien agrega:

> La universalización de la tecnología ha generado a tal grado las oportunidades de la delincuencia informática que no es posible circunscribir a su autor a una tipología en particular, en una sociedad que ha ido superando las barreras sociales para su uso y democratizando día a día sus recursos y posibilidades. (p. 96)

REACCIÓN DEL ESTADO FRENTE A LOS DELITOS INFORMÁTICOS Y LA IMPLEMENTACIÓN DE HERRAMIENTAS NACIONALES Y TRANSNACIONALES

Como es de ineludible razonamiento, los Estados han reaccionado de forma indistinta o heterogénea frente a esta nueva criminalidad, lo que ha ocasionado que no exista una uniformidad en el tratamiento jurídico y sancionatorio.

Considero que no resulta del todo negativo que esta nueva forma de criminalidad se resuelva con numerosas fórmulas —heterogéneas entre sí—, toda vez que, como hemos indicado, el *modus operandi* de estos delitos suele evolucionar y transformarse

en el tiempo. Sobre el particular, Morón Lerma (2016) muestra cómo algunos Estados han adaptado sus legislaciones:

> En los casos de Perú y República Dominicana, la técnica legislativa ha sido incorporar una regulación específica para la cibercriminalidad a través de una ley especial. De forma contraria, en países como Colombia, Nicaragua o Panamá se decidió por integrar las previsiones sobre delitos cibernéticos en el Código Penal. En ocasiones, los cibercrímenes se concentran, bien en un título, destinado a proteger la seguridad jurídica de los medios electrónicos (como en Panamá) o a proteger la información y los datos (en Colombia), o bien en un capítulo referido a los delitos informáticos (caso de Guatemala o Costa Rica), pero otros países siguen un modelo de técnica legislativa más conservador, cifrado en crear "tipos de equivalencia"; es decir, se llevan a cabo modificaciones parciales en el Código, adaptando las figuras penales clásicas a fin de que resulte posible su aplicación para reprimir los delitos cibernéticos. En otras palabras, se prefiere introducir, en las correspondientes secciones en que se protegen bienes jurídicos tradicionales, las modalidades necesarias para afrontar estos nuevos riesgos (así, por ejemplo, en El Salvador, Nicaragua y Panamá). (p. 44)

Esta disparidad en los cuerpos normativos internacionales es una buena señal; sin embargo, también es cierto que mientras usemos más medios tecnológicos y sistemas informáticos, se necesitará que esta regulación sea ajustada a estos cambios y para ello es necesario contar con bases o herramientas generales.

Ahora, si bien es cierto que hemos aplaudido y felicitado que las legislaciones comparadas cuenten con una regulación específica para los delitos informáticos, también es importante recalcar que esta nueva forma de criminalidad trasciende los Estados. Como indicamos líneas atrás, una de las características de los delitos informáticos es su dimensión transnacional, motivo por el cual sí resulta indispensable la existencia de regulación internacional que brinde lineamientos generales y transversales para cada Estado.

Hasta ahora la mejor propuesta internacional para alinear criterios jurídicos respecto a los delitos informáticos ha sido el Convenio sobre la Ciberdelincuencia firmado el 23 de noviembre del 2001 en Budapest. No obstante, es bastante criticable que hayan transcurrido cerca de veinte años desde la suscripción de este convenio internacional y hasta la fecha no se pueda erigir un nuevo convenio de igual trascendencia. No cabe la menor duda de que en ese lapso de tiempo han aparecido innumerables formas de delitos informáticos y, además, hay otros que han evolucionado, lo que genera una mayor complejidad para su descubrimiento y posterior sanción. Este resulta un fundamento más que válido para concretar una nueva regulación internacional.

Solo para señalar brevemente la importancia de una regulación transnacional, es pertinente comentar algunos artículos del Convenio sobre la Ciberdelincuencia de Budapest.

En primer lugar, el capítulo II de este convenio introdujo los tipos penales de acceso ilícito (artículo 2), interceptación ilícita (artículo 3), ataques a la integridad de los datos (artículo 4), ataques a la integridad de sistema (artículo 5), abuso de los dispositivos (artículo 6), falsificación informática (artículo 7), fraude informático (artículo 8), delitos relacionados con la pornografía infantil (artículo 9) y delitos relacionados con infracciones de la propiedad intelectual y de los derechos afines (artículo 10).

En segundo lugar, este convenio también reguló ciertos aspectos procesales en la investigación de delitos informáticos, por ejemplo, obtención en tiempo real de datos relativos al tráfico (artículo 20), extradición (artículo 24), procedimientos relativos a las solicitudes de asistencia mutua en ausencia de acuerdos internacionales aplicables (artículo 27), conservación rápida de datos informáticos almacenados (artículo 29), entre otros artículos.

Por otro lado, es pertinente mencionar que los delitos informáticos o cibercrímenes también fueron parte de la agenda del Décimo Segundo Congreso de las Naciones Unidas sobre Prevención del Delito y Justicia Penal, llevado a cabo del 12 al 19 de abril del 2010 en la ciudad de Salvador en Brasil. En este congreso internacional se debatió la problemática de los delitos informáticos. Al respecto, se recalcó que el delito cibernético era uno de los mayores problemas que afrontaban los órganos de aplicación de la ley y se señaló que los Estados miembros habían exhortado a que se elaborara una convención internacional sobre la materia.

Este pronunciamiento inicial se condice con nuestra crítica, la cual hace hincapié en que resulta necesaria la formulación de un convenio internacional que disponga nuevos criterios y herramientas para la debida y adecuada investigación y sanción de los delitos informáticos.

Los Estados han reconocido que las diferencias entre los ordenamientos jurídicos y la insuficiente cooperación internacional obstaculizaban la investigación de los delitos cibernéticos y el enjuiciamiento de sus responsables. Bajo esta premisa, algunos Estados han destacado que para combatir los delitos informáticos han tenido que implementar y adoptar diversas medidas como, por ejemplo, la promulgación de la legislación penal y de normas contra el blanqueo de dinero, la reglamentación de los cibercafés, las campañas de sensibilización, el reforzamiento de los mecanismos para presentar denuncias y la protección de los grupos vulnerables, así como la creación de dependencias especializadas y la implementación de plataformas interinstitucionales para los órganos de represión.

Resulta alentador que se promuevan cooperaciones o comunidades transnacionales para combatir los delitos informáticos. Entre ellas figuran el Acuerdo de Cooperación de Shanghái, el Acuerdo de la Comunidad de Estados Independientes, el Acuerdo de la Liga de Países Árabes y, por último, el Acuerdo de la Unión Africana.

En el hemisferio sur, se tienen dos pronunciamientos iberoamericanos interesantes: el primero es el Convenio Iberoamericano de Cooperación sobre Investigación, Aseguramiento y Obtención de Prueba en Materia de Ciberdelincuencia; y el segundo es la Recomendación de la Conferencia de Ministros de Justicia de los Países Iberoamericanos (COMJIB) relativa a la tipificación y sanción de la ciberdelincuencia, ambos del 28 de mayo del 2014. El primer instrumento internacional, en su artículo 2, señala que la ciberdelincuencia es "cualquier forma de criminalidad ejecutada en el ámbito de interacción social definido por el uso de las tecnologías y la comunicación". En su artículo 6 destaca las medidas de aseguramiento dentro de una investigación, y en su artículo 7 menciona las diligencias de investigación que se pueden llevar a cabo en un proceso por delito informático y también regula la cooperación internacional. Por su parte, el segundo instrumento transnacional es una recomendación que propone incorporar diversos tipos penales, por ejemplo, el acceso no autorizado a sistemas, daños informáticos o atentados contra la integridad de los datos, suplantación de identidad y estafa informática.

En buena cuenta, estas dos herramientas internacionales tienen el propósito de establecer criterios mínimos y comunes en la prevención y lucha contra los delitos informáticos, cibercrimen o ciberdelitos, sin menoscabar, conforme indicamos previamente, la postulación y promoción de cada legislación interna.

DELITOS INFORMÁTICOS

No es la finalidad de este trabajo analizar todos los delitos informáticos que se encuentran regulados en nuestro ordenamiento penal. Solamente se desarrollarán los delitos más frecuentes y de gran relevancia para la criminalidad económica, como son el fraude informático y la suplantación de identidad.

Delito de fraude informático

El delito de fraude informático se encuentra regulado en el artículo 8 de la Ley 30096, modificado a través de la Ley 30171:

> 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.

El Convenio sobre la Ciberdelincuencia regula en su artículo 8 el delito de fraude informático de la siguiente manera:

> Las Partes adoptarán las medidas legislativas o de otro tipo que resulten necesarias para tipificar como delito en su derecho interno los actos deliberados e ilegítimos que causan perjuicio patrimonial a otra persona mediante:
>
> a. la introducción, alteración, borrado o supresión de datos informáticos.
>
> b. cualquier interferencia en el funcionamiento de un sistema informático con la intención, dolosa o delictiva, de obtener de forma ilegítima un beneficio económico para uno mismo o para otra persona.

Al respecto, Pérez López (2019) refiere que en el delito informático:

> El agente, a través de las tecnologías de la información o de la comunicación, 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 manipulación en el funcionamiento de un sistema informático. (p. 159)

Sobre el particular, para la configuración de este tipo penal, se requiere necesariamente la manipulación de un sistema informático con la única finalidad de obtener un provecho económico. De esta descripción se puede inferir que este delito regula los supuestos en los cuales el agente transfiere fondos ajenos a una cuenta propia o de un tercero, así como también cuando el agente suprime datos económicos que terminan por alterar el estado financiero de una persona, o quien manipula el sistema informático de la empresa en donde trabaja modificando —dolosamente— la cantidad de pedidos requeridos con el objetivo de transferir el excedente de productos a un tercero.

De la lectura del tipo penal, se colige que para su configuración no se requiere de violencia o amenaza; es decir, esta conducta es necesariamente engañosa, motivo por el cual algunos autores la denominan *estafa informática*. Sin embargo, en mi opinión, se podría considerar que el fraude informático es una modalidad de estafa. De la misma manera, se debe deslindar categóricamente el delito de fraude informático del delito de hurto, toda vez que no existe un bien físico objeto de sustracción, sino una manipulación informática dolosa que ocasiona una transferencia económica.

Con respecto al elemento subjetivo, este delito es eminentemente doloso, por lo que no permite la modalidad culposa.

Una de las modalidades típicas que advertimos en el Perú es la de *trashing*, que consiste en que el agente busca que el agraviado "muerda el anzuelo" con el objetivo de obtener información privada para utilizarla en actividades delictivas. Esto puede darse a través de las redes sociales y programas informáticos, entre otros.

Delito de suplantación de identidad

El delito de suplantación de identidad se encuentra regulado en el artículo 9 de la Ley 30096:

> El que, mediante las tecnologías de la información o de la comunicación suplanta la identidad de una persona natural o jurídica, siempre que de dicha conducta resulte algún perjuicio, material o moral, será reprimido con pena privativa de libertad no menor ni mayor de cinco años.

El Convenio sobre la Ciberdelincuencia regula en su artículo 7 el delito de falsificación informática de la siguiente manera:

> La introducción, alteración, borrado o supresión deliberados e ilegítimos de datos informáticos que generan datos no auténticos con la intención de que sean tomados o utilizados a efectos legales como auténticos, con independencia de que los datos sean legibles e inteligibles directamente.

El comportamiento de este ilícito penal se configura cuando el agente sustituye la identidad de una persona natural o jurídica, con la finalidad de generar un perjuicio (en sentido extenso). Ciertamente, la configuración del tipo penal requiere que la suplantación sea real y consistente; además, cabe señalar que la conducta es completamente dolosa, no considerándose la modalidad culposa.

Un punto que se tiene que tomar en consideración es que el perjuicio debe ser interpretado en un sentido amplio; es decir, no solamente se comprenderá el perjuicio económico, sino que también se incluirá un perjuicio moral o ético.

Este tipo penal contiene una modalidad denominada *pishing* que ha tenido bastante relevancia y exposición en estos últimos meses. A través de esa modalidad los agentes buscan acceder a información personal o confidencial (financiera o económica) mediante la remisión de correos falsos o adulterados, de tal manera que una vez que reciben la información verdadera ingresan a las cuentas bancarias de los agraviados (personas naturales o jurídicas) y sustraen o transfieren el dinero, con la finalidad de aprovecharse económicamente de ello.

Por otro lado, la modalidad del *pharming* es un mecanismo para llegar a las cuentas bancarias o información financiera de los agraviados a través de la creación de páginas web falsas, las mismas que suplantan —casi a la perfección— a las páginas originales de las entidades públicas o privadas.

SOBRE LA CRIMINALIDAD ECONÓMICA

Terradillos Basoco (2015), en la introducción a su exposición sobre el derecho penal económico, indica:

> La globalización económica, más allá de los juicios valorativos a los que se haga acreedora, constituye una realidad de implantación amplia, que trasciende las fronteras nacionales. Y, en cuanto homogeneiza las condiciones en que se desarrolla la actividad mercantil, genera también formas comunes de delincuencia, susceptibles, a su vez, de respuestas institucionales internacionalmente aceptadas. (p. 8)

Evidentemente, estas palabras nos permiten ingresar a analizar el desarrollo de esta nueva forma de criminalidad económica, que se encuentra "vinculada a estructuras de la globalización y financiación de la economía, que genera ingentes costes económicos, entre los que deben contarse, junto a los perjuicios directos, los derivados de los efectos resaca y espiral" (Terradillos Basoco, 2015, p. 14).

Los delitos informáticos tienen gran repercusión en la criminalidad económica actual porque colisionan con una economía globalizada y que emplea sistemas financieros, operaciones comerciales, transacciones bancarias virtuales, así como sistemas informáticos. Ahora bien, esta nueva forma de criminalidad posee ciertas características que le son inherentes y que Caro Coria y Reyna Alfaro (2016) han señalado:

> – Multiplicidad de sujetos activos: al ser empresas entes de carácter colectivo, sus actividades se desarrollan mediante la participación de múltiples sujetos que actúan para proteger los intereses del ente colectivo, lo que genera dificultades en la determinación de responsabilidad penal, sobre todo en empresas con complejos sistemas de distribución de funciones.
>
> – Afectación de bienes jurídicos colectivos: resulta evidente que las conductas en el seno de las agrupaciones tienden a afectar bienes jurídicos de carácter colectivo o macrosocial, ligados al propio funcionamiento del sistema social.
>
> – Diversidad de nexos causales y problemas en la determinación de responsabilidades: los procesos de producción, distribución y venta de bienes y servicios generan una serie de problemas en la determinación de la participación, hecho que es característico en las sociedades posmodernas. (p. 45)

Después de esbozar brevemente algunas ideas respecto a la criminalidad económica, podemos asegurar que los delitos informáticos deben ser incluidos en esta nueva gama de ilícitos penales, toda vez que las características de los delitos informáticos se adecúan perfectamente a la estructura y características de este nuevo sistema.

Considero que no resulta debatible afirmar que los delitos informáticos cuentan con una multiplicidad de agentes; peor aún, algunos se mantienen en la clandestinidad y se desconoce sus identidades y ubicaciones, lo cual genera y agrava su impunidad. Su actuación delictiva no se restringe a un solo agente, sino que por la complejidad de los hechos es indispensable que exista una distribución de roles y, más grave aún, existen organizaciones criminales cuyos agentes no son nacionales, sino que trascienden a un Estado, lo cual perjudica más la correcta investigación.

Como segundo punto, los delitos informáticos o cibercrímenes protegen bienes jurídicos supraindividuales, como la seguridad de la información contenida en las bases de datos, sistemas o redes de computadoras, o la seguridad en el tráfico jurídico de la información. En buena cuenta, estos bienes jurídicos involucran necesariamente la afectación de una colectividad o el funcionamiento de un bien de interés social. Además,

estos delitos son pluriofensivos, por lo que no solamente se salvaguarda el sistema de información o la seguridad en el tráfico de información, sino también otros bienes jurídicos "clásicos" como, por ejemplo, el patrimonio o la intimidad.

En tercer lugar, resulta necesario puntualizar que los delitos informáticos contienen una estructuración compleja, es decir, su *modus operandi* entraña diversidad de conductas y sujetos. Se convierte así en un delito que tiene como principal característica la complejidad en su investigación y posterior sanción.

Estas características de los delitos informáticos nos llevan a concluir que revisten presupuestos inherentes a la criminalidad económica, para lo cual debemos contar con instrumentos jurídicos idóneos que permitan su correcta investigación. A lo que Pérez López (2019) añade que "existe un consenso en aceptar a la categoría de los delitos informáticos como el reflejo de una nueva forma de criminalidad que se relaciona directamente con el uso o la intermediación de un elemento o dato informatizado" (p. 159).

No cabe la menor duda de que el 2020 fue el año de las compras por internet (en abril, el comercio electrónico constituyó el 49,1 % del consumo total de bienes y servicios). La coyuntura de las restricciones por la pandemia del COVID-19 condujo a que el *e-commerce* sea utilizado por miles de personas. Solamente para comprender la importancia de la correcta regulación de los delitos informáticos, es importante conocer ciertas cifras:

- Diez millones de latinos han comprado bienes de consumo masivo a través del comercio electrónico (Kantar, 2020).
- En México, el gasto en comercio electrónico se multiplicó por 10 durante la cuarentena con un incremento en valor del 123 % (Kantar, 2020).
- En Estados Unidos, la penetración del comercio electrónico ha crecido un 70 % en los primeros meses del 2020 (IPMARK, 2020).
- En el Perú, entre enero y mayo del 2020, el valor de las transacciones del público a través de los instrumentos de pagos distintos al efectivo ascendió a 958 000 millones de soles, según el Banco Central de Reserva (como se citó en "Transferencias electrónicas crecieron 13 % a mayo, mientras uso de tarjetas de crédito cayó 25 %", 2020).
- En el Perú, entre enero y mayo del 2020, se incrementó en 18 % las operaciones efectuadas a través de la banca virtual, de acuerdo con el Banco Central de Reserva (como se citó en "Transferencias electrónicas crecieron 13 % a mayo, mientras uso de tarjetas de crédito cayó 25 %", 2020).
- En España, en el 2019, se cometieron 218 302 ciberdelitos. De ellos, 192 375 fueron fraudes informáticos y 4275 constituyeron falsificación informática (Observatorio Español de Delitos Informáticos, s. f.).

- En el Perú, entre enero y junio del 2020, se registraron 1412 denuncias de delitos informáticos (División Policial de Alta Tecnología, como se citó en Pichihua, 2020).
- En el Perú, entre enero y julio del 2020, se registraron 1117 denuncias de fraude informático, de las cuales 974 fueron por operaciones o transferencias electrónicas no autorizadas y 142 por compras fraudulentas en internet (División Policial de Alta Tecnología, como se citó en Pichihua, 2020).
- En el Perú, entre enero y julio del 2020, se detuvo a 171 personas por la presunta comisión de delitos informáticos (División Policial de Alta Tecnología, como se citó en Pichihua, 2020).
- En el Perú, se estima que solamente el 15 % de las víctimas de delitos informáticos denuncian (División Policial de Alta Tecnología, como se citó en Alva Olivera y Collave García, s. f.).
- En el Perú, entre enero y la primera semana de agosto del 2020, se registraron 1 481 963 ataques de *pishing* y un promedio de 7000 ataques diarios (División Policial de Alta Tecnología, como se citó en Alva Olivera y Collave García, s. f.).
- A nivel mundial, los delitos informáticos ocasionan pérdidas de 12 500 millones de dólares cada año (División Policial de Alta Tecnología, como se citó en Alva Olivera y Collave García, s. f.).

Las cifras mencionadas demuestran que nunca antes habíamos empleado los sistemas informáticos con tanta normalidad en nuestra vida diaria, por lo que las organizaciones criminales dedicadas a cometer este tipo de delitos han encontrado en este *modus vivendi* una zona liberada que vienen aprovechando sin contemplaciones. No obstante, es en este contexto donde nuestras herramientas jurídicas tienen que estar completamente alineadas. Además, el Estado debe promover políticas de prevención por parte de instituciones públicas y privadas; e, igualmente, impulsar la suscripción de convenios internacionales para combatir los delitos informáticos, toda vez que estos tienen como características principales ser transnacionales y contar con una estructura compleja. En consecuencia, resulta necesario contar con mejores herramientas para investigar y sancionar adecuadamente a las organizaciones criminales.

CONCLUSIONES

Los presupuestos especiales de los delitos informáticos permiten establecer una relación directa con la criminalidad económica, que no solamente se circunscribe a delitos patrimoniales, sino que también engloba tipos penales que cuentan con una importante repercusión en el sistema informático y, accesoriamente, en el sistema económico.

Para combatir los delitos informáticos o cibercrímenes resulta necesaria la convocatoria de diversos Estados para suscribir un nuevo convenio internacional que contenga nuevas herramientas, debido a que las modalidades delictivas y organizaciones criminales evolucionan y se perfeccionan.

REFERENCIAS

Alva Olivera, G., y Collave García, Y. (s. f.). Si ganaste un premio por actualizar tus datos desde el celular, te acaban de estafar. *El Comercio.* https://especiales.elcomercio.pe/?q=especiales/estafas-electronicas-ecpm/index.html

Caro Coria, C., y Reyna Alfaro, L. (2016). *Derecho penal económico. Parte general* (t. I). Jurista Editores.

Convenio sobre la Ciberdelincuencia. 23 de noviembre del 2001. Budapest. https://normas-apa.org/referencias/citar-leyes-documentos-legales/

Davara, M. A. (1993). *Derecho informático.* Aranzadi.

Kantar. (30 de septiembre del 2020). *10 millones de latinos compraron FMCG en e-commerce.* https://www.kantar.com/latin-america/inspiracion/retail/10-millones-de-latinos-compraron-fmcg-en-e-commerce?par=pe/Noticias/10-millones-de-latinos-compraron-FMCG-en-Ecommerce

Ley 30096 del 2013. Ley de Delitos Informáticos. 21 de octubre del 2013. https://www2.congreso.gob.pe/sicr/cendocbib/con5_uibd.nsf/C5F98BB564E5CCCF05258316006064AB/$FILE/6_Ley_30096.pdf

Ley 30171 del 2014. Ley que modifica la Ley 30096, Ley de Delitos Informáticos. 9 de marzo del 2014. https://www.leyes.congreso.gob.pe/Documentos/Leyes/30171.pdf

Morillas Fernández, D. (2017). *Delitos informáticos. Material de la Maestría en Derecho Penal Económico Internacional.* Universidad de Granada.

Morón Lerma, E. (2016). Nuevas tecnologías e instrumentos internacionales. Consecuencias penales. En F. Velásquez Velásquez, R. Vargas Lozano y J. D. Jaramillo Restrepo (Comps.), *Derecho penal y nuevas tecnologías. A propósito del título VII bis del Código Penal* (pp. 33-54). Universidad Sergio Arboleda.

Observatorio Ecommerce & Transformación Digital. (s. f.). *Son tiempos de e-commerce.* Recuperado el 17 de marzo del 2021 de https://observatorioecommerce.com/son-tiempos-de-ecommerce/

Observatorio Español de Delitos Informáticos. (s. f.). *Estadísticas. Reporte de ciberdelitos en España.* Recuperado el 17 de marzo del 2021 de https://oedi.es/estadisticas/

Peña Cabrera Freyre, A. R. (2008). *Derecho penal. Parte especial*. IDEMSA.

Pérez López, J. (2019). *Delitos regulados en leyes penales especiales.* Gaceta Jurídica.

Pichihua, S. (8 de agosto del 2020). *Fraudes en línea son los delitos informáticos más frecuentes en el 2020.* Andina. Agencia Peruana de Noticias. https://andina.pe/agencia/noticia-fraudes-linea-son-los-delitos-informaticos-mas-frecuentes-el-2020-809048.aspx

Rayón Ballesteros, M., y Gómez Hernández, J. (2014). Cibercrimen: particularidades en su investigación y enjuiciamiento. *Anuario Jurídico y Económico Escurialense*, *XLVII*, 209-234.

Terradillos Basoco, J. M. (2015). Derecho penal económico. Lineamientos de política penal. *Revista del Instituto de Ciencias Jurídicas de Puebla*, *25*, 7-38.

Transferencias electrónicas crecieron 13 % a mayo, mientras uso de tarjetas de crédito cayó 25 %. (7 de julio del 2020). *El Comercio*. https://elcomercio.pe/economia/negocios/plin-yape-tunki-lukita-transferencias-electronicas-crecieron-a-mayo-mientras-uso-de-tarjetas-de-credito-cayo-25-nndc-noticia/?ref=ecr

Villavicencio Terreros, F. (2014). Delitos informáticos. *Ius et Veritas*, *24*(49), 284-304.