Lucerna Iuris Et Investigatio
n.º 1 - 2021, pp. 29 - 47
http://dx.doi.org/10.15381/lucerna.v0i1.18373

Print ISSN: XXXX-XXXX
Online ISSN: XXXX-XXXX
Facultad de Derecho y Ciencia Política UNMSM

INVESTIGACIONES NACIONALES

Estudio de los delitos informáticos y la problemática de su tipificación en el marco de los convenios internacionales

Study of computer crimes and the problem of your typification in the framework of the international agreement

Carmen Leyva Serrano[1]

Universidad Nacional Mayor de San Marcos

carmenleyvaserrano8@gmail.com

Presentado: 16/03/2019 - Aceptado: 25/09/2019 - Publicación: 12/04/2021

Resumen

Nuestra investigación, tiene por finalidad realizar un estudio dogmático doctrinario, que nos permita establecer la realidad jurídica, en armonía con la política criminal preventiva, protectora y garantista diseñada por nuestra Constitución; recomendamos reformular los fundamentos dogmáticos, en base a los delitos informáticos, los conocimientos que aportan la doctrina y la experiencia nacional actual.

Palabras clave: Tipificación de los delitos informáticos en el Perú.

Abstract

Our research aims to conduct a doctrinal dogmatic study, which allows us to establish the legal reality, in harmony with the preventive, protective and guarantee criminal policy designed by our Constitution; We recommend to reformulate the dogmatic foundations, based on computer crimes, the knowledge provided by the doctrine and current national experience.

Keywords: Typification of computer crimes in Peru.

1. Descripción de la realidad problemática

"Delitos informáticos", "Computerdelikte", "Computercrímenes" son sólo algunos de los rótulos utilizados en nuestra lengua dogmática para sintetizar el creciente fenómeno de la criminalidad informática e informatizada. Como expresa Sieber, la criminalidad informática y el derecho penal informático son manifestaciones relativamente recientes y su desarrollo histórico demuestra el proceso de una permanente adaptación de la criminalidad y el derecho a las nuevas tecnologías informáticas (cit. Abozo y Zapata 2006).

El fenómeno de la globalización caracterizado principalmente como un proceso socio – económico y cultural de tendencia mundial, junto a las tics, se han ido difundiendo de modo acelerado, desempeñando al día de hoy un factor preponderante en el desarrollo de la cultura. Las Tics, brindan una manera efectiva de procesar y almacenar datos en tiempo récord, simplificando tiempos en la comunicación e interacción digital. Medios de comunicación como el correo electrónico, messenger en sus inicios, facebook, twitter, entre otros, como producto del internet y por ende de la era global, se complementaron junto a las tecnologías de la información, generando una comunicación e interacción en tiempo real, superando todos los paradigmas jamás vistos y ello solo era el inicio. Estas herramientas, al día de hoy, vienen siendo implementadas como parte del gobierno electrónico, aplicado a diversos ámbitos de la gestión pública y en las diferentes instituciones, las mismas que en la búsqueda de efectivizar la administración pública, hacen uso de estas herramientas para poder llegar a los lugares más recónditos de la república y alcanzar objetivos gubernamentales en diversas materias como salud, educación y medio ambiente.

> Si bien los diversos ámbitos de interacción se ven favorecidos por la fluidez que le brinda esta nueva alternativa tecnológica, no obstante, se incrementan los riesgos relacionados a las tecnologías informáticas y de comunicación. El desarrollo de la tecnología también ha traído consigo nuevas formas delictuales que tienen por medio y/o finalidad los sistemas informáticos e internet. Las principales características de vulnerabilidad que presenta el mundo informático son las siguientes: a. La falta de jerarquía en la red, que permite establecer sistemas de control, lo que dificulta la verificación de la información que circula por este medio; b. El creciente número de usuarios, y la facilidad de acceso al medio tecnológico; c. El anonimato de los cibernautas que dificulta su persecución tras la comisión de un delito a través de este medio; d. La facilidad de acceso a la información para alterar datos, destruir sistemas informáticos. Otro factor determinante es la rápida difusión de información a través de este medio tecnológico a muy

> bajo costo que permite a las organizaciones delictivas perpetrar delitos con mayor facilidad[2].

Si bien es cierto, el sistema criminaliza determinadas conductas que trasgreden el orden social en el ámbito informático, no podemos dejar de mencionar las diversas ventajas que nos brindan las herramientas del sistema informático. Así, por ejemplo, en el campo de las comunicaciones y en el ámbito de la educación. Es importante mencionar un informe de las Naciones Unidas (12°), referido al delito y la justicia social, el mismo que establece los graves peligros que ha traído consigo la globalización y las nuevas tecnologías de la información, generando nuevas modalidades de comisión de delitos como la amplia e inmensa distribución de pornografía infantil y el fraude principalmente, también se vislumbran nuevos delitos a partir de la vulnerabilidad de las redes sociales o informáticas, envíos de correos no deseados con publicidad o fines criminales, como por ejemplo, la obtención de datos y contraseñas con el fin de acceder a cuentas bancarias o cuentas de redes sociales, la piratería también se constituye en una nueva modalidad y los ataques mediante virus se ha convertido en una actividad frecuente en el internet, todo ello, con el fin de obtener datos con información sensible.

Conforme a lo dicho, nuestra investigación pretende abordar este "novedoso" fenómeno criminal, vinculado con el uso abusivo de los ordenadores, los sistemas telemáticos y el almacenaje y procesamiento de datos. Sin dejar de lado el reconocimiento de los avances tecnológicos logrados por la humanidad en el siglo pasado, que configuran una nueva dimensión en cuanto al progreso de los lineamientos de vida de los particulares, ya que internet brinda una herramienta sumamente útil nunca antes vivenciada.

La información, el almacenaje de datos y su procesamiento adquieren en la actualidad un valor estratégico no sólo en el mercado, sino en el ámbito de la intimidad y demás derechos de las personas, que imprime la necesidad de adoptar medios legales para su correcta tutela. Siguiendo esta línea, la gran mayoría de los países han incorporado a su legislación penal una batería de normas que reprimen las actividades distorsivas en el uso de los sistemas informáticos. Al respecto, algunos autores como el profesor Vizcardo, ha establecido lo siguiente:

> Al efecto, es necesario partir de una diferenciación ampliamente aceptada de distinguir en el uso de los ordenadores y los sistemas telemáticos como medio o fin para la comisión de delitos. En una primera aproximación debe señalarse que el medio informático es empleado, por lo general, para cometer delitos contra el patrimonio, la intimidad, la libertad sexual, la fe pública, etc.; mientras que la información como objeto de tutela va ganando precisión de manera paulatina en su correcta materialización. Ya no puede discutirse

> seriamente que ella surge como un valor intrínseco digno de tutela jurídica en una sociedad cada vez más tecnificada y dependiente cibernéticamente. (Hugo Vizcardo 2010, p. 356).

En el caso peruano, nuestro país ha suscrito un importante convenio en materia de cibercriminalidad, el convenio de Budapest (2004), este convenio fue aceptado, contando la aprobación respectiva que figura en la Resolución legislativa N°30912, del 13 de febrero de 2019. Este tratado o convenio, pionero en la materia, tiene como principal objetivo, constituirse en una herramienta normativa internacional que permita erradicar los nuevos delitos asociados a internet o también llamados delitos informáticos a través de la adopción de normas internas, la efectividad en la investigación y la cooperación internacional. La aplicación de una "política penal común" que destaca en su preámbulo, constituye la piedra angular del mismo a fin de combatir el cibercrimen. Cuatro años de trabajo en cuanto al convenio, contando con la colaboración de diversos especialistas internacionales, ha brindado como fruto una lista de crímenes que los estados como parte de su compromiso, deben ser incluidos en el ordenamiento interno. Adicional a lo anteriormente mencionado, los estados firmantes, también se han comprometido a la colaboración en cuanto a la investigación y los procedimientos requeridos a fin de obtener datos que puedan configurar un ilícito penal de esta naturaleza.

Nuestro ordenamiento jurídico, especialmente en cuanto a los delitos informáticos, este tipo de delito estaba ubicado en el 186 del Código Penal. El principal problema al igual que en otros delitos, era la autonomía, la misma que se había configurado y tipificado como agravante del delito de hurto, conocido como "hurto electrónico". Esto sería corregido a través de la ley 27309, el mismo que fue expedido el 17 de julio del año 2009, ley que modificó el título V, del libro segundo del Código Penal, realizando la inserción de un capítulo nuevo (X), llamado "delitos informáticos", siendo insuficiente aún por su carácter netamente patrimonial, teniendo que nuevamente corregido y denominado "delitos informáticos patrimoniales". Mediante esa denominación es que se van a introducir los siguientes delitos: Intrusismo y fraude informático (Art. 207-A), sabotaje informático (Art. 207-B), circunstancias agravantes (Art. 207-C) y tráfico ilegal de datos (Art. 207-D). Todos los delitos anteriormente descritos, concretizaban el reproche penal hacia quienes, de manera indebida, accedía a bases de datos, sistemas o algún tipo de red computarizadas con fin de realizar un daño a través de alteraciones o la sustracción de la información.

En este contexto, fue promulgada la Ley N°30096, la misma que luego sería modificada mediante Ley N°30171, "Ley de delitos informáticos"; legislación que fue incorporada a nuestro sistema penal con el fin de adecuar nuestro ordenamiento jurídico interno a los estándares internacionales fijados a partir del "convenio de Budapest". Producto de ello se tipificaron:

"acceso ilícito, atentando a la integridad de datos informáticos, atentado a la integridad de sistemas informáticos, proposiciones a niños, niñas y adolescentes con fines sexuales por medios tecnológicos, interceptación de datos informáticos, fraudes informáticos y la suplantación de identidad y abuso de mecanismos y dispositivos informáticos". Estas modalidades descritas, también han sido tipificadas en diversos países de Europa como España, Alemania y Francia, países de Latinoamérica como Chile, Ecuador y Argentina y también en Estados Unidos.

El marco establecido, fundamenta los objetivos de nuestra investigación, la misma que pretende demostrar si la tipificación existente respecto a los delitos informáticos en el sistema penal peruano, ha sido diseñada en base a una técnica legislativa acorde y tomando en cuentas los estándares internacionales que se desprenden de los convenios internacionales de los cuales el Perú forma parte. También incidimos en un estudio dogmático pormenorizado en lo referente a los delitos informáticos en sus diversas modalidades básicas y formas agravadas; y, establecer de acuerdo a la investigación, si es que contamos con los fundamentos principales a fin de concretar la difícil labor de criminalización en cuanto a los "delitos informáticos", ya que estos, generan afectaciones en cuanto al tratamiento de datos sensibles, las comunicaciones y la reserva de las mismas y otros bienes jurídicos que contienen preeminencia penal – patrimonial. En cuanto a la afectación que pueden generar las nuevas tecnologías de la información, encontramos la fe pública, libertad sexual y otras de similar naturaleza. Se pretende mediante la presente investigación, identificar si la normativa es adecuada y de encontrar ciertas limitaciones, proponer mecanismos que permitan efectivizar la lucha contra la delincuencia informática. El último de los objetivos está referido a la determinación de los criterios por parte del legislador al momento de plantear y aprobar la criminalización referida a los delitos informáticos, proponiendo modificaciones legislativas que permitan mejorar el sistema.

2. El delito informático

El paradigma clásico del poder a través del dominio de la información, ha tomado una nueva perspectiva, y, es que el paradigma actual se torna en el dominio de la información tal, como lo hemos podido percibir en distintos casos de connotación internacional, ahí tenemos el caso de los WikiLeaks por ejemplo, constituyéndose al día de hoy en el arma que arropa de poder a diversos países y personas que han logrado alcanzar significativos avances en el campo tecnológico de las aplicaciones como el caso del Mark Zuckerberg que al día de hoy es dueño de las redes sociales más importantes del mundo como whatsApp, facebook e Instagram, lo que le brinda un amplio margen de poder en las comunicaciones y la información que al día de hoy se difunde en gran porcentaje por las redes sociales mencionada. Ello, marca el desarrollo

y avance de cada país, siendo Estados Unidos al día de hoy el que mayor alcance ha generado, comprobando que la utilidad de máquinas y sistemas informáticos se han convertido en herramientas de incidencia desbordante en cuanto al grado de desarrollo de cada país.

Algunos autores, consideran han destacado de manera concreta y precisa, ciertas características respecto a los delitos informáticos, así, investigadores como Davara Rodríguez, contextualiza esta realidad de la siguiente manera:

> Esta realidad ha determinado, como contrapartida negativa, la aparición de actos vulnerantes o lesionantes contra los derechos que alrededor de la propiedad o utilización de los medios informáticos se han ido generando y que han fundamentado una nueva gama de bienes jurídicos a proteger. Aparece así la criminalidad por computadora o "delito informático" ("computer crime"), que es definido como la realización de una acción que, reuniendo las características que delimitan el concepto de delito, sea llevada a cabo utilizando un elemento informático o vulnerando los derechos del titular de un elemento informático, ya sea de hardware o de software. (Dávara 1993, p. 318)

Conforme lo plantea el profesor alemán, Klaus Tiedemann, "con la expresión <<criminalidad mediante computadoras>> se alude a todos los actos antijurídicos según la ley penal vigente (o socialmente perjudiciales y por eso penalizables en el futuro), realizados con el empleo de un equipo automático de procesamiento de datos" (1985, p. 122). Este tipo de delitos que son realizados mediante una computadora, constituyen delitos instrumentados. Al respecto, la "Organización para la Cooperación económica y el desarrollo, ha señalado que el "delito informático", representa un comportamiento ilícito, concretada mediante una acción antiética y sin autorización con el fin de procesar datos o transmitirlos" (Vizcardo, 2010, p.354)

Las definiciones de diversos autores respecto al delito informática, es variada, así, tomamos algunas citadas por el profesor Hugo Vizcardo con el fin de abordar de mejor manera la presente materia de investigación:

> "Autores como Camacho, han definido al delito informático como toda acción dolosa que provoca un perjuicio a persona o entidades, sin que necesariamente conlleve un beneficio material para su autor o que, por el contrario, produce un beneficio ilícito a su autor aun cuando no perjudique de forma directa o inmediata a la víctima y en cuya comisión interviene necesariamente de forma activa dispositivos habitualmente utilizados en las actividades informáticas". Por su parte, Fernández Calvo, abogado y consultor

> de sistemas de información, ha definido al delito informático como la concreción de un comportamiento con determinadas características que lo convierten en delito, mediante el uso básico de un elemento temático o informático que afecta tanto las libertades como los derechos de los ciudadanos" (citados por Vizcardo ob.Cit.p.354)

Otros autores, consideran que el concepto de delito informático aún no ha encontrado consenso en la doctrina, y también lo denominan computer crime o computerkriminalität, ello en razón que la delincuencia informática comprende una serie de comportamientos que es difícil reducir o agrupar en una sola definición. De manera general, "se puede definir el delito informático como aquél en el que para su comisión se emplea un sistema automático de procesamiento de datos o de transmisión de datos" (Bramont – Arias 1997, p. 27).

Regresando al estudio del Rodríguez Davara, se torna interesante su posición respecto al concepto de delito informático, afirmando con seguridad que "generalmente concurren determinadas características comunes a todas las conductas catalogadas como delitos informáticos, que nos permiten clasificarlas de acuerdo con la función y actividad que se realiza para cometerlos. Estos delitos poseen unas especialidades que les hacen, en ocasiones más difíciles de detectar y, en otras, aún detectados, no son denunciados por múltiples razones, y aun siendo denunciados son difíciles de perseguir. Todos ellos centran su principal actividad en el acceso y/o la manipulación de datos -que se encuentran en soportes informáticos- o de programas de ordenador utilizados en su procesamiento" (1993, p. 322).

Conforme lo señala Arbulú Martínez, (...) "el delito informático es todo comportamiento típico, antijurídico, culpable realizado a través de sistemas de procesamiento de datos, contra la información automatizada siempre en perjuicio de una persona natural o jurídica. Uno de los signos característicos del delito informático es que es pluriofensivo toda vez que puede ir contra el patrimonio, la intimidad, la seguridad pública, y la seguridad informática, esta última que puede ser considerada como un nuevo tipo de bien jurídico que debe ser tutelado penalmente" (2002, p. 21).

Respecto a la tipificación de los delitos informáticos, cabe resaltar su difícil tarea en cuanto a los mismos, ello, debido a su amplitud y crecientes modalidades que día a día se van develando. Una de los mayores retos es poder precisar cada característica en cuanto a la criminalización de este tipo de conductas y señalar el bien jurídico afectado en virtud de la sistematización. Otro tema que aún deja sombras sobre la materia es el referido a la prueba y sobre ello, autores como Núñez, han señalado que la amplia problemática

sobre la prueba en este tipo de delitos, debería ser encuadrada de manera que se logre sanciones y se efectivice el sistema" (1964, p.253)

En esas circunstancias, cabe precisar que:

> contemporáneamente el uso de las computadoras y su interconexión, ha dado lugar a un fenómeno de nuevas dimensiones: el delito instrumentado mediante el uso del computador (denominado "delito informático", <<delito electrónico>>, <<delito relacionado con las computadoras>>, <<crímenes por computadora>> o <<delincuencia relacionada con el ordenador>>. Y, aunque al día de hoy no se tiene una cuantificación precisa sobre este tipo de delitos, es preciso mencionar que la comisión de los mismos se irá expandiendo conforme el uso de computadores, redes sociales y otros medios de cualquier naturaleza se siga acentuando en el mundo actual. Ya los tipos penales tradicionales han fracasado en el intento de poder contenerlos, tomando cada vez mayor importancia no solo a nivel de nuestro ordenamiento legal interno, sino también a nivel internacional, debido a la afectación de diversos ordenamientos nacionales. (Correa y otros, 1987, p.295).

Por su parte, el profesor Klaus Tiedemann, considera respecto a la tarea del derecho, que, "la misma no puede mantenerse en base a categorías producto de teorías antiquísimas, que al día de hoy no responde a las formas de delito, específicamente, los delitos informáticos, por ello, se tiene que prevenir y brindar protección a la sociedad, en base a nuevas formas, revisando constantemente el derecho y proponiendo a través de un estudio sistematizado, alternativas de solución que superen lagunas legales (1999, p.334).

Consideramos, como punto importante de la investigación, que la prevención frente a este tipo de delitos, debería tomar en cuenta la no aceptación de errores en calidad de no intencionados o involuntarios, ya que para los fines que se hace uso, se necesita contar con cierta pericia, la misma que es producto de un largo proceso de preparación y entrenamiento, la familiaridad de este tipo de conducta relacionadas al delito, es frecuente y recurrente en tanto en cuanto, en su mayoría suele contratarse personas con amplia experiencia o practicado por las mismas personas que gozan del manejo de redes informáticas y similares.

Por ello, es que consideramos que una de los desafíos más importantes del derecho penal al día de hoy, implica evitar todo tipo de manipulación en cuanto a sistemas informáticos que pueda afectar la convivencia social, teniendo en consideración, como ya hemos dicho, que, la globalización y desarrollo informático actual, han traído consigo, diversas herramientas

útiles para los seres humanos, pero también, diversas modalidades nuevas de comisión de delitos que se torna mayormente difíciles en cuanto a su persecución e investigación por la naturaleza y especialidad de su accionar.

3. Concepción clásica del Derecho penal y el delito informático

Como ya hemos tenido la oportunidad de fundamentar, el "fenómeno informático", se ha convertido en una realidad con la cual convivimos y que apareció entre nosotros y se ha instalado de manera irreversible en nuestra realidad social y económica. Ello determinó, en su momento, la aparición de una serie de derechos que giran alrededor de su implementación y utilización, que reclaman la protección del sistema legal. Por ello, el problema primordial actual se implica la búsqueda de reformas efectivas de control y regulación penal efectivas, ya que los modelos punitivos tradicionales no eran suficientes para su protección.

Sin embargo, no podemos dejar de mencionar la importancia que implica tomar en cuenta el principio de última ratio, tal como lo establece el profesor Bramont:

> "Nadie duda que el fenómeno informático produce en distintas ramas del ordenamiento jurídico (Derecho civil, Derecho Procesal, derecho Mercantil, etc.) un cierto trastorno a la hora de enfrentar tales hechos. Tal es la problemática generada por este fenómeno que ha motivado en la actualidad la necesidad de recurrir al derecho Penal a fin de disuadir del uso abusivo al que lleva el empleo de computadoras, lo cual se ha plasmado ye en varias legislaciones extranjeras. No obstante, ante estas situaciones no puede olvidarse el principio del derecho Penal como ultima ratio, lo cual significa que la intervención penal solo está justificada cuando otras ramas del ordenamiento jurídico ya no pueden resolver los problemas que genera el fenómeno informático en la sociedad, de ahí que el derecho penal actúe como última instancia de control social" (Bramont Arias 1997, p. 17 – 18)

Es indudable que la computadora, desde la perspectiva de su constitución física, puede ser el medio para la comisión de diversos ilícitos penales, como, por ejemplo, un delito de lesiones contra la persona a la que se le agrede arrojándole una computadora o cuando se la destruye en el sentido de daños a la propiedad. Pero no es este al caso ya que aquí analizaremos los supuestos en que la computadora es utilizada en su función propia, en cuanto permite el procesamiento de datos, la confección o utilización de programas para ello.

Tal como lo hemos descrito en líneas anteriores, las figuras o tipos penales comunes y tradicionales, específicamente los referidos a delitos patrimoniales, han sido los utilizados en los inicios de del fenómeno informático con el fin de contener esta nueva forma de criminalidad, sin embargo, como se desprende de diversas posturas analizadas, no ha sido suficiente, teniendo que acudir a la creación de tipos penales especiales en cuanto a los delitos informáticos. En el caso peruano, tal como lo hemos descrito, formaba parte del artículo 186°, inciso 3, segundo párrafo del Código Penal de 1991, no siendo efectiva su aplicación debido a la carencia de autonomía como delito, sino como agravante de otro tipo relacionado a delitos patrimoniales clásicos. Por ello, se introduce a través de la ley 27309 del 17 de julio del 2000, el título V, referido a "Delitos Informáticos", pero con un matiz patrimonial, siendo incompleta la figura, cambiándose posteriormente por "delitos informáticos patrimoniales", al advertir el error.

4. Aspectos Criminológicos de la delincuencia informática

"La criminología tradicional, por su raigambre positivista, potenció al máximo el protagonismo de la persona del delincuente, creyendo poder encontrar en una supuesta diversidad del mismo, patológica (teoría de la diversidad), la explicación científica del comportamiento criminal. Por el contrario, en la moderna Criminología -de corte prioritariamente sociológico- el examen y significado de la persona del delincuente pasa a un segundo plano, desplazándose el centro de interés de las investigaciones sobre la persona del infractor hacia la conducta delictiva misma, la víctima y el control social. En todo caso, el delincuente se contempla <<en sus interdependencias sociales>>, como unidad <<biopsicosocial>>, y no desde una perspectiva biopsicopatológica, como sucediera con tantas biografías criminales <<clásicas>> orientadas por el espíritu <<correccionalista>> e <<individualistas>> de la Criminología tradicional" (García-Pablos de Molina, Antonio 1999, p. 73).

La delincuencia informática, es relativamente moderna y en ello, coincidimos con el profesor Arbulú Martínez, quien sostiene que:

> La criminalidad informática es de reciente aparición. Comenzó a manifestarse con los llamados "Computer Hackers", personas especialmente hábiles en el manejo de la informática, quienes, en un inicio, hicieron sonar la alarma en orden a la necesidad de reforzar la seguridad en los sistemas informatizados. A esto se une el continuo desarrollo tecnológico de los diversos países, el cual se ve potenciado cada vez más gracias al incremento de redes internacionales de comunicación electrónica de datos. La posibilidad de introducirse en tales redes es de puntos muy remotos de países extranjeros,

agravan los problemas de descubrimiento y persecución de estas conductas. (Cfrme. Arbulú Martínez 2002, p. 20).

Conforme lo precisa Bramont Arias, en el fenómeno informático es necesario resaltar los siguientes aspectos criminológicos:

1. Un primer aspecto es el riesgo que gira en torno a la "información" que los nuevos sistemas informáticos potencian, desarrollan y revalúan. No constituye ninguna novedad afirmar que actualmente las computadoras almacenan una gran información, del más variado contenido. El peligro surge con la utilización abusiva de la información relativa a los ciudadanos, circunstancia que muchos casos puede colisionar con el sistema de garantías fundamentales del ciudadano, propio de un sistema de derecho. Desde este punto de vista, "Información" significa "Poder", en la medida en que aumenta la capacidad de control sobre los individuos. La informática se ha constituido en una herramienta que permite articular ese poder, el cual se torna peligroso en una sociedad que cree ampliamente en el libre mercado o en el monopolio estatal (ambas variantes son peligrosas). Así, la informática multiplica el poder de quien se vale de la información, pero, al mismo tiempo, crea y acentúa las desigualdades y pone en entredicho los derechos y garantías individuales que deben existir en un estado social y democrático de derecho.

2. En la generalidad de los casos, la condición de un delito informático se detecta de manera casual. Y cuando ello ocurre, sobre todo si la victima resulta ser una persona jurídica, no se presenta la correspondiente denuncia debido tanto a la publicidad que se puede generar y manchar su reputación, como a la misma desconfianza existente en la eficacia de los órganos jurisdiccionales. Así la denuncia de la ejecución, realizada dolosamente, por ejemplo, de una transferencia de dinero de una cuenta corriente a otra en una institución bancaria de reconocido prestigio, unida a la publicidad que pudiera hacerse del caso, puede motivar a muchos clientes de dicha institución al cierre de sus cuentas o bien disuade a otros futuros clientes de la apertura de nuevas cuentas por la desconfianza que provoca su sistema de seguridad.

3. Es importante también indicar que este tipo de delincuencia informática normalmente produce un gran daño a la víctima, sobre todo de carácter económico. Esto trae como consecuencia lo siguiente:

   3.1. Si denuncian los agraviados por estos delitos, no es con la finalidad de recuperar el dinero por el daño causado, sobre todo

si se tiene en cuenta que, en el proceso judicial, el monto de la reparación suele ser inferior al efectivo daño causado y porque, al ser condenado este sujeto a una pena privativa de libertad, deja de trabajar, por lo que con mayor razón carecerá del dinero necesario para reparar el daño causado. De ahí que el motivo de la denuncia de estos hechos, ante todo, es castigar al sujeto con una pena.

3.2. Por otro lado, y por lo que respecta al daño o perjuicio ocasionado por estos delincuentes, estos son de tal magnitud que crean una mayor alarma en los miembros de la sociedad (1997, p. 20 – 22).

La sociedad ha confeccionado su propio estereotipo de los autores de la delincuencia informática, a saber, éste es representado generalmente por un adolescente con orígenes de clase media que le ha permitido acceder a una formación en el manejo de dispositivos informáticos, inofensivo, ignorante respecto a la negatividad de su actuar, hábil y por lo general varón. Sumado a ello, una inteligencia avanzada y bastante inmiscuido en el mundo informático. Excluyéndose con ese estereotipo a personas que bien no encajarían en esas características pero que sí cometen el delito. Es posible que, en algunos casos, el sujeto o agente no maneje temas informáticos, sin embargo, de igual forma hace uso de medios informáticos para cometer el ilícito. Por ello, en la actualidad, podemos concluir que los delitos informáticos no solo lo pueden cometer personas con manejo profundo en informática y amplia habilidad e inteligencia.

El profesor Bramont Arias, sostiene:

> De otro lado, hay que reconocer que los primeros delitos informáticos recayeron en un sistema de gran importancia: La NASA y, el Departamento de Defensa de los EE.UU. Dado estos actos y los avances de la tecnología, cada vez se da más importancia al tema de la "seguridad" dentro de los sistemas informáticos, lo cual hace más difícil el acceso a los distintos programas. Sin embargo, últimamente también se habla de un delincuente profesional dentro del ámbito informático en la medida que los comportamientos de estas personas están relacionados con el crimen organizado, relativo sobre todo al espionaje internacional. Las personas que realizan este tipo de delitos, por lo general suelen ser personas que cuentan con alguna conexión a las empresas, conocen las características y la seguridad del sistema y aprovecha de ello para vulnerar el sistema informático (Bramont Arias 1997, p. 23).

5. La víctima en el delito informático

Cada vez hay más autores que plantean que hay que considerar el papel de la víctima en el Derecho Penal, circunstancia que ha sido posible a través del desarrollo de la Criminología, sobre todo de la victimología. En tal sentido, se entiende por victima a la persona afectada por el comportamiento del autor del delito. "Para la victimología, víctima es el ser humano que padece daño en los bienes jurídicamente protegidos por la normativa penal: vida, salud, propiedad, honor, honestidad, etc., por el hecho de otro…" (Matos Quezada, Julio 2016, p. 81).

García Pablos, ha establecido lo siguientes respecto al concepto de víctima:

> La doctrina se ha basado en el binomio o duplicidad víctima – delincuente a fin de poder brindar una definición a partir de la interacción entre ambos. Siendo la persona humana la que es víctima. "Los primeros estudios trataron de poner de relieve que aquélla no es un mero objeto, pasivo y fungible, sino un sujeto; un sujeto que configura el hecho criminal, el autor del mismo y contribuye a su propia victimización. De este concepto de víctima como sinónimo de persona natural que experimenta subjetivamente con malestar o dolor una lesión objetiva de bienes jurídicos. Pero es una acepción restrictiva que dejaría fuera de toda consideración victimológica una rica y grave gama de comportamientos criminales dirigidos contra personas jurídicas o intereses supraindividuales. Una vez superado, además, el microscópico ámbito de la pareja criminal y los prejuicios psicologicistas de los primeros estudios victimológicos, evidenció su insuficiencia, su estrechez" (García, 1999, p. 122).

Desde antiguo. Se ha destacado cómo en el Derecho Penal hay una interrelación entre delincuente y víctima. Así, por ejemplo, en el delito de estafa, es muy frecuente que el delincuente se aproveche del afán de lucro de su propia víctima, como sucede, por ejemplo, con el cuento del billete de lotería premiado. En los últimos tiempos se ha destacado que la víctima asume, desde el principio, el riesgo como medio de aumentar la seducción de la oferta en un sistema de alta competitividad, como por ejemplo el caso de los supermercados en que todo está al alcance inmediato de los clientes, que eventualmente podrían tomarlos y constituir un hurto. Es por ello que esta asunción del riesgo hay que tenerla en cuenta también desde una perspectiva penal. En base a esto, algunos autores pretenden encontrar en el comportamiento de la víctima, una categoría de carácter formativo que actué como un principio a tenerse en cuenta dentro de la sistemática del delito. De ahí surge el concepto de autorresponsabilidad. "Significa que la víctima ha de tomar todas las precauciones que sean del caso para evitar que sea su comportamiento la causa del delito, en otros términos,

quien no toma las precauciones correspondientes a su responsabilidad respecto de sus bienes jurídicos carecerá de protección frente a estos" (Blossiers Hüme 2005, p. 367).

> La existencia de autorresponsabilidad implica la imposibilidad de atribuir ese hecho al tipo legal; estaría ante una causa de atipicidad. Siguiendo esta idea, la victima que deja un saco, su cartera o su maletín sumamente costosos en el asiento trasero de su carro descapotable mientras va a hacer unas compras, los cuales ya no encuentra al regresar, seria autor responsable de ese hecho. En el ámbito de los delitos informáticos, también es posible aplicar estos razonamientos: Normalmente las empresas, con el desarrollo continuo de la sociedad en una economía de mercado, siempre tienden a que su oferta llegue al público; el instrumento para conseguir esto son las computadoras, las cuales facilitan y aceleran este proceso. Es por esto que las victimas más frecuentes de los delitos informáticos son personas jurídicas, con un cierto potencial económico. Esta característica corresponde con las notas propias de la delincuencia de cuello blanco o socioeconómico donde también se cuadra la delincuencia informática (Bramont Arias 1997, p. 25).

6. El bien jurídico protegido

En cuanto al bien jurídico, es importante resaltar la importancia de la concepción sobre el Derecho Penal, como un instrumento que va a facilitar la vida organizada o en comunidad, teniendo como objetivo principal, brindar garantía en cuanto a la evolución y el funcionamiento del sistema social. Por ello, al referirnos al concepto de "bien jurídico", este debe estar necesariamente asociado a la "realidad social", lo cual no puede representar la voluntad de quien legisla, ya que es anterior a esa voluntad y contiene límites respecto a su actividad.

Por lo dicho, en virtud del principio de última ratio, el Derecho penal solo puede intervenir en determinadas conductas que garanticen el orden social. Tal es así, que el profesor Polaino Navarrete, ha referido al respecto lo siguiente:

> "La opinión mayoritaria en la dogmática penal sostiene que el Derecho penal cumple una función de protección de bienes jurídicos, esto es, de los bienes y valores que son consubstanciales a la convivencia humana y se consideran imprescindibles para la vida social. Esta función tutelar es, en su esencia, una función de garantía, que en cuanto a tal, a su vez, implica una función de prevención de futuros delitos, porque los comportamientos

> delictivos inciden sobre los objetos jurídicos de tutela penal. Protección y prevención constituyen un binomio inseparable y mantienen una relación de medio a fin. El Derecho penal protege bienes jurídicos (esto es, les concede garantía normativa), con el objetivo de la prevención de la lesión de los mismos (o sea, de la evitación de futuros delitos). La protección de bienes jurídicos es el contenido de la función, y la prevención de delitos es el objetivo final de la misma. Desde esta perspectiva, el bien jurídico, es tanto objeto de protección típica, se convierte en un concepto esencial del Derecho penal, consubstancial a su propia existencia" (Polaino, 2005, p. 95 - 96)

A decir de Bramont Arias, "es innegable que el bien jurídico protegido es punto de referencia obligado para la determinación del tipo penal del delito informático, puesto que determina el marco dentro del cual pueden realizarse las conductas delictivas. No hay unanimidad en orden al contenido del bien jurídico protegido en el delito informático. La mayoría de legislaciones establecen que estos delitos afectan al patrimonio, pero, de lege ferenda, también hay autores que afirman que el bien jurídico protegido es bien el orden económico, bien la intimidad de las personas" (1997, p. 51).

Al efecto, nos dice Durand Valladares, "las diferentes conductas nocivas que se concretan a través de sistemas informáticos y en internet pueden ocasionar diversas lesiones a diferentes bienes jurídicos protegidos, tales como la intimidad, el patrimonio y nuevos objetos jurídicos de protección que adquieren autonomía e identidad propias en la red. Algunos autores han llegado a establecer al patrimonio como el bien jurídico protegido y además, a la intimidad de la persona. Sin embargo, creemos que, si bien estos bienes jurídicos pueden verse afectados mediante el uso de sistemas informáticos, principalmente debido a la expansión de la tecnología, no constituyen bienes jurídicos propios de los delitos informáticos, ya que se trata de objetos de protección penal que están más allá del uso de los sistemas informáticos y que, en consecuencia, no se han originado producto de la tecnología (2002, p. 156).

De las definiciones aportadas por la doctrina, y que hemos tenido la oportunidad de apreciar, el delito informático tiene como característica el de realizarse a través de sistemas de procesamientos de datos, contra información automatizada en perjuicio de personales naturales o jurídicas; siendo en consecuencia que lo que se pretende proteger es la seguridad informática, que en la actualidad se constituye en un nuevo tipo de bien jurídico que debe ser tutelado penalmente. Nuevo tipo de bien jurídico que consideramos se inserta en el contexto de los delitos informáticos, mediante los cuales se protegen los intereses socio económicos.

En el delito informático, nos refiere Arbulú Martínez, "el objeto de la acción típica es la información; pero no cualquier tipo de información sino aquellas que revisten la forma de representaciones codificadas expresadas en magnitudes físicas variables, tales como señales típicas, impulsos electromagnéticos, etc., susceptibles de registro, proceso y transmisión, que ofrecen una vulnerabilidad especial, debido a la facilidad de acceder a ellas y utilizarlas. Y más aún ahora que estando en caminos a ser una sociedad informatizada; la información trasmitida por medios magnéticos adquiere una categoría de objeto protegible de la acción antijurídica" (2002, p. 22).

7. Valoración de la tipificación de los delitos informáticos en el Perú

La presente investigación encuentra su justificación en su aspecto dogmático, ya que, en un sistema democrático de derecho, la persona humana es el fin supremo tal como lo establece nuestra Carta Constitucional, por ello, es necesario el aseguramiento de sus derechos fundamentales, como aquellos relacionados a sistemas informáticos, bases de datos, las comunicaciones y la reserva de las mismas y otros bienes jurídicos que contengan relevancia e importancia penal – patrimonial. Debemos tomar en cuenta, que también puede vulnerarse la libertad sexual y la fe pública. ante ello, el Estado debe reaccionar brindando las garantías normativas necesarias y adecuadas para la prevención y protección.

Y es justamente en este marco que radica el fundamento y los objetivos de nuestra investigación, que pretende demostrar si la tipificación realizada respecto a los delitos informáticos, han sido desarrollados tomando en cuenta la técnica legislativa adecuada y si la estructura mediante la cual ha sido construida, es acorde a los estándares establecidos en los convenios internacionales firmados por el Perú. El estudio dogmático respecto a los delitos informáticos, también justifican la investigación, ya que se han diversificado las modalidades básicas y agravadas. Por otro lado, tomar en cuenta los fundamentos que permitan abordar la criminalización, se torna indispensable. Encontrar mecanismos correctos y eficaces para contener esta nueva modalidad de delitos, es el desafío mayor y nuestro aporte, va en esa línea, enfocados a la propuesta de las modificaciones legislativas necesarias.

En este sentido, la investigación en cuanto a su justificación, tiene como base primigenia, un amplio estudio dogmático que tiene como principales aristas, señalar las distintas modalidades, la naturaleza de los delitos informáticos, principales características, los elementos relevantes que los componen y su regulación normativa tanto a nivel interna como internacional.

7.1.Valoración práctica

Abordar el tema de los delitos informáticos, también contiene un carácter práctico, ya que se enfoca un análisis complementario al análisis dogmático y los casos reales se han convertido en casos comunes, aunque no en la misma magnitud. Las ventajas y desventajas de la era global, nos impele al estudio de estas nuevas formas de criminalidad. Al respecto, el profesor Villavicencio, tomando en cuenta la vulnerabilidad a la que nos vemos expuestos en el mundo cibernético, establece como principales características: "La falta de un sistema de control, agregando de nuestra parte, que dicho sistema de control, no menoscabe derechos fundamentales; la cantidad de usuarios y su fácil acceso; la no identificación de quienes utilizan los medios informáticos, ya que por general, ello genera mayores complicaciones en cuanto a la persecución del autor del delito; la alteración de datos para generar desinformación y la rapidez con la que fluye la información, llegando a miles de personas a un costo bastante bajo y sin corroborar la veracidad[3].

Conforme lo expuesto, nuestra investigación pretende abordar este "novedoso" fenómeno criminal, vinculado con el uso indiscriminado de los ordenadores, los sistemas telemáticos y el almacenaje y procesamiento de datos. Sin dejar de lado el reconocimiento de los avances tecnológicos logrados por la humanidad en el siglo pasado, que configuran una nueva dimensión que facilitan la vida de muchas personas, constituyéndose en una herramienta sumamente positiva, nunca antes vivenciada.

Este enfoque teórico – práctico, será de suma utilidad en cuanto a la comprobación respecto a la aplicación de los fundamentos de la tipificación e imputación de los delitos informáticos, y sin con ello se resguarda la seguridad jurídica y la vigencia del debido proceso.

La opinión de especialistas en la materia, se torna indispensable en este tipo de investigaciones, los operadores de justicia también juegan un rol importante, ya que estos últimos pueden identificar con mayor facilidad debido a su practica diaria, posibles problemas, deficiencias o vacíos de nuestro ordenamiento legal.

8. Conclusiones y propuestas de solución proyectada

Como ya dejamos expresado, nuestra investigación, tiene por finalidad realizar un estudio de tipo dogmático doctrinario, que nos permita establecer la realidad jurídica de la protección que en nuestro sistema penal se hace de los datos informativos, el secreto de las comunicaciones y otros. Por ello, se debe profundizar el estudio dogmático y reorientar la evolución y realidad actual de la protección, que en nuestro país se hace de tales bienes jurídicos, desde la perspectiva constitucional basada en los más modernos principios penales orientados a la protección de la persona humana, ello, con el fin de guiar la actividad que desarrollan nuestros legisladores, docentes en aulas,

los jueces a través de la interpretación tanto desde la doctrina como desde el ámbito judicial.

Por ello, los beneficios que aporta nuestra propuesta están directamente relacionados a contribuir con la labor docente y operativo-judicial, brindando un espacio de deliberación y de necesario debate jurídico, a fin de perfeccionar la legislación a partir de nuevos conocimientos doctrinarios y del aporte también del derecho comparado.

Por eso, es que teniendo en perspectiva nuestro objetivo general y habiendo identificado ya que en el Perú existe un clima de gran convulsión social e inseguridad ciudadana; y que al efecto no contamos con una criminalización técnica e integral de las conductas que lesionan los intereses informáticos, proponemos recomendaciones, relacionadas a las acciones que el Estado deberá realizar en relación a su marco institucional y las necesarias modificaciones legislativas, ya que nuestro trabajo pretende propender una mejora de la legislación en armonía con la política criminal preventiva, protectora y garantista diseñada por nuestra Constitución, por lo que en general, siendo que se encuentra ad portas la implementación de un nuevo Código Penal, recomendamos en principio reformular los fundamentos dogmáticos de los delitos informáticos y sobre la base de los nuevos conocimientos que aporta la doctrina y la experiencia nacional, se proceda a reformular el universo de estos delitos informáticos.

Referencias

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

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

Los Delitos Informáticos en la Banca: El delito del milenio. Informática y Derecho Bancario. BLOSSIERS MAZZINI, Juan José y CALDERON GARCÍA, Sylvia B. (2000). Editora RAO S.R.L. Lima – Perú.

El delito Informático en el Código Penal Peruano. Biblioteca de Derecho Contemporáneo. BRAMONT – ARIAS TORRES, Luis Alberto (1997). Volumen 6. Pontificia Universidad Católica del Perú. Fondo Editorial. Lima – Perú.

Derecho Informático. CORREA, Carlos M. y Otros (1987). Ediciones Jurídicas De palma. Buenos Aires - Argentina.

Derecho Informático DAVARA, Miguel Ángel (1993). Editorial Aranzandi. Barcelona – España.

Cyber Delito o Delitos de Ordenadores, Sistema Bancario Nacional. DURAND VALLADARES, Raúl (2002). Gráfica Net. Imprenta. Lima – Perú.

Virus en las Computadoras. FERREYRA CORTEZ, Gonzalo (1990). Editorial Macrobit. México.

Delitos Contra el Patrimonio. HUGO VIZCARDO, Silfredo (2010). Pro Derecho Perú Investigaciones Jurídicas. Lima – Perú.

Derecho Penal, Sociedad y nuevas tecnologías. ZUÑIGA RODRIGUEZ, Laura/ MÉNDEZ RODRÍGUEZ, Cristina/ DIEGO DIAZ-SANTOS, Rosario (coordinadoras) (2001). Editorial COLEX. Madrid – España.

Notas al final

1 Biografía: Abogada miembro de la orden del Colegio de Abogados del Callao, Directora Administrativa de la Facultad de Ingeniería de Sistemas e Informática de la Universidad Nacional Mayor de San Marcos, Alumna de la Maestría de Derecho y Ciencias Penales de la UNMSM.

2 Al respecto, el doctor y docente universitario, Felipe Villavicencio Terreros, ha desarrollado uno de los pocos trabajos sobre la materia que puede verificarse en el siguiente enlace: http://revistas.pucp.edu.pe/index.php/iusetveritas/article/view/13630/14253

3 https://www.academia.edu/32884244/Felipe_Villavicencio_Terreros_Delitos_Informaticos_Ley30096_su_modificacion.