Este artículo se encuentra disponible
en acceso abierto bajo la licencia Creative
Commons Attribution 4.0 International License

Ius Vocatio
Revista de Investigación de la Corte Superior de Justicia de Huánuco

Vol. 7, n.° 9, enero-junio, 2024, 91-115
Publicación semestral. Huánuco, Perú
ISSN: 2810-8043 (En línea)
DOI: 10.35292/iusVocatio.v7i9.928

La impunidad en los delitos informáticos. Una problemática de poco interés para legisladores, jueces y fiscales

Impunity in computer crimes. A problem of little interest to legislators, judges and prosecutors

Impunidade em crimes informáticos. Um problema de pouco interesse para legisladores, juízes e promotores

Catalina Tania Estrada Salvador Ramírez
Universidad de Huánuco
(Huánuco, Perú)
Contacto: 5201411140@udh.edu.pe
https://orcid.org/0009-0008-0313-5652

RESUMEN

El presente artículo se origina por el problema que se viene observando en la persecución y la sanción de los delitos informáticos, toda vez que muchos de estos casos delictivos suelen quedar impunes. En esa línea de ideas, a través del estudio referido, se identificarán plenamente los factores que contribuyen a la no sanción penal de los ciberdelincuentes. Uno de esos factores es la no individualización del ciberdelincuente, motivo por el cual el representante del Ministerio Público suele archivar el proceso penal, ello por una simple razón: la formalización de la investigación preparatoria exige la plena individualización del sujeto, en caso contrario,

no se podrá formalizar la investigación. A fin de evitar la impunidad de los delitos informáticos, esta investigación brindará determinadas soluciones que aportarán en la averiguación y la sanción de estos hechos delictivos.

Palabras clave: individualización; archivo; ciberdelincuente; investigación preparatoria; tecnología.

Términos de indización: derecho; administración de justicia; derecho del ciberespacio; derecho penal; derecho de la informática (Fuente: Tesauro Unesco).

ABSTRACT

This article originates from the problem that has been observed in the prosecution and punishment of computer crimes, since many of these criminal cases usually go unpunished. In this line of ideas, through the aforementioned study, the factors that contribute to the non-criminal punishment of cybercriminals will be fully identified. One of these factors is the non-individualization of the cybercriminal, which is why the representative of the Public Ministry usually files the criminal process, for a simple reason: the formalization of the preparatory investigation requires the full individualization of the subject, otherwise, the investigation cannot be formalized. In order to avoid impunity for computer crimes, this research will provide certain solutions that will contribute to the investigation and punishment of these criminal acts.

Key words: individualization; archive; cybercriminal; preparatory investigation; technology.

Indexing terms: law; justice administration; cyberspace law; criminal law; computer law (Source: Unesco Thesaurus).

RESUMO

Este artigo se origina do problema que foi observado na acusação e punição de crimes de computador, hoje em dia quando muitos desses casos criminais geralmente ficam impunes. Nesta linha de idéias, através do estudo acima

mencionado, os fatores que contribuem para a punição não criminal dos cibercriminosos serão totalmente identificados. Um desses fatores sendo a não individualização do cibercriminal, razão pela qual o representante do ministério público geralmente arquiva o processo criminal, por um motivo simples: a formalização da investigação preparatória requer a individualização completa do assunto; caso contrário, a investigação não pode ser formalizada. Para evitar impunidade por crimes de computador, esta investigação fornecerá certas soluções que contribuirão para a investigação e punição desses atos criminosos.

Palavras-chave: individualização; arquivo; criminal cibernética; investigação; tecnologia preparatória.

Termos de indexação: direito; administração da justiça; lei do ciberespaço; direito penal; lei de informática (Fonte: Unesco Thesaurus).

Recibido: 19/02/2024 **Revisado:** 03/05/2024
Aceptado: 10/05/2024 **Publicado en línea:** 30/06/2024

1. INTRODUCCIÓN

La globalización ha contribuido al progreso y al desarrollo de la tecnología al facilitar la creación de herramientas digitales que han transformado la manera en que se llevan a cabo diversas actividades. Este hecho, sin duda, ha obtenido mayor eficacia en las comunicaciones y ha permitido que las actividades se desarrollen con más prontitud; no obstante, también ha favorecido el riesgo de vulneración de los bienes jurídicos expuestos en el mundo digital. Es por eso que el desarrollo de la tecnología no solo ha traído consigo grandes ventajas, sino también nuevas formas y modalidades delictivas (Chavarría, 2023, p. 1).

De esta forma, año tras año, nuestras autoridades locales y nacionales vienen trabajando arduamente en la lucha contra los delitos cibernéticos; sin embargo, hasta la fecha, los resultados obtenidos han sido deficientes, toda vez que esta forma delictiva sigue en aumento, y ello se debe a diversos

factores: leyes inadecuadas, falta de formación de los profesionales del sistema judicial, carencia de recursos logísticos y tecnológicos para la persecución eficaz de dichos crímenes, entre otros.

La evolución constante de las tecnologías de la información y la comunicación (TIC) se convierte en un desafío para el ordenamiento jurídico, ya que genera cambios significativos en el derecho penal y la política criminal. Por tanto, conforme avanza la tecnología, la delincuencia también se adapta y se traslada cada vez más al espacio cibernético. En consecuencia, la transformación digital conlleva la necesidad de implementar un sistema legal y una política criminal que se ajusten de manera efectiva a las nuevas realidades que surgen en el entorno digital (Espinoza Prado, 2022, p. 19).

Es así que Villavicencio (2014), al analizar las ventajas y las desventajas de la tecnología, menciona que, a pesar de los beneficios que brinda la tecnología en los diversos ámbitos de interacción, también se incrementan los riesgos delictivos asociados al uso de tecnología informática y de comunicación. Razón por la cual el avance tecnológico no solo facilitó la fluidez en las interacciones, sino que también ha introducido nuevas formas delictivas, teniendo como medio los sistemas informáticos e internet (p. 285).

No se trata simplemente de una forma común de delincuencia, sino de una criminalidad arraigada y altamente evolucionada, con repercusiones más perjudiciales. Las víctimas bien pueden ser personas vulnerables, como ancianos, niños o individuos con un nivel de conocimiento informático bajo; por otro lado, suelen ser personas con gran capacidad económica bancaria, por tanto, ninguna persona está a salvo de esta forma delictiva tecnológica.

Por ello, la ciberdelincuencia representa un nuevo reto para nuestro sistema legal, así como también para aquellas instituciones encargadas de hacer cumplir la ley, incluyendo a la policía, la fiscalía y la autoridad judicial, pues estas entidades a menudo se ven superadas por los ciberdelincuentes que, en su mayoría, poseen conocimientos especializados en informática, mientras que los profesionales de nuestro sistema legal carecen de formación en esta área (Espinoza Calderón, 2022, p. 20).

Por tal razón, es imperativo que se asignen valores a los nuevos bienes jurídicos y se promulguen leyes que los protejan, para así abordar los vacíos legales presentes en nuestra normativa. Estas son cuestiones de urgencia que deben captar la atención de los legisladores; de lo contrario, persistirá un considerable grado de impunidad.

No cabe duda de que la llegada del internet ha incrementado las oportunidades para cometer nuevos delitos, que se ejecutan en lugares antes inimaginables en todo el mundo (Espinoza Prado, 2022, p. 8). Este fenómeno está en constante crecimiento y evolución, y representa un desafío significativo tanto para las fuerzas policiales como para las autoridades judiciales en su esfuerzo por combatir esta forma de criminalidad.

Sin duda alguna, los delitos informáticos han experimentado un crecimiento alarmante y han trascendido las fronteras tecnológicas. Los delincuentes aprovechan este cambio digital y utilizan las tecnologías disponibles para ejecutar ataques sofisticados contra las víctimas, lo que genera considerables consecuencias económicas (Anicama, 2023, p. 3). Es así que esta situación presenta un real desafío tanto para la seguridad cibernética como para la estabilidad económica global y, por ende, el ordenamiento jurídico debe estar a la altura para combatir esta forma delictiva.

2. CONCEPTO DE DELITO INFORMÁTICO

Sobre la base de lo señalado por Barrio (2017a), los ciberdelitos son aquellas transgresiones legales que ocurren en el ciberespacio, entendido como un entorno artificial creado a través de los medios informáticos (p. 300). Esta categoría no solo abarca los delitos que van dirigidos contra los equipos, los datos o los sistemas informáticos (que vulneran la integridad, la confidencialidad y la disponibilidad), sino que también comprende aquellos delitos tradicionales que se cometen a través de dispositivos electrónicos o digitales, como amenazas, coacciones y estafas. En otras palabras, los ciberdelitos engloban una variedad de acciones delictivas que tienen lugar en el entorno virtual e involucran tanto aspectos informáticos como conductas tradicionales llevadas a cabo mediante las tecnologías digitales.

Por su parte, Tobares y Castro (2010) nos brindan una definición similar a la anterior. Mencionan que el delito informático se refiere a cualquier infracción penal que involucra el uso de la informática o las técnicas relacionadas con ella. Este comportamiento delictivo puede materializarse cuando la computadora es utilizada como material o como objetivo de acción delictiva. Además, estos autores señalan que abarca cualquier conducta criminal que, en su ejecución, haga uso de la tecnología electrónica, ya sea como método, medio o propósito (p. 28). En un sentido más estricto, se considera delito informático a cualquier acto ilícito penal en el cual las computadoras, sus técnicas y sus funciones desempeñan un papel significativo (método, medio o fin de la acción delictiva). Cabe recordar que estos delitos están intrínsecamente relacionados con el uso de la tecnología informática en diferentes formas y contextos criminales.

Asimismo, Flores (2014) señala que los delitos informáticos pueden definirse como cualquier acción u omisión que está legalmente tipificada y sancionada con una pena, y son llevados a cabo por una persona en el ámbito de la informática, con la consecuencia de causar perjuicio a individuos específicos y proporcionar beneficios ilícitos al autor del delito. Además, destaca varios elementos claves que deben considerarse para identificar este tipo de delito, tal como se detalla a continuación:

i. El bien jurídico tutelado es la integridad técnica y la seguridad de los medios informáticos involucrados.
ii. El elemento subjetivo implica el dolo o la culpa con la que actúa la persona que comete el delito informático.
iii. El sujeto activo de estos delitos suele ser una persona con cierto nivel de inteligencia y educación, como programadores, analistas de sistemas, analistas de comunicaciones, supervisores, personal técnico y de mantenimiento, entre otros.
iv. El sujeto pasivo con mayor frecuencia son las entidades bancarias, que llevan a cabo transacciones mediante símbolos electrónicos (p. 132).

Según lo mencionado por dicho autor, los delitos informáticos a menudo son efectuados como parte de las actividades laborales, toda vez que los autores de estos delitos tienden a realizarlos mientras están en su lugar de trabajo, ya que son acciones que se caracterizan por ser oportunas, es por eso que el ciberdelincuente aprovecha situaciones propicias para cometer el acto delictivo. Además, estos delitos se caracterizan por generar considerables pérdidas económicas para las víctimas, al mismo tiempo generan beneficios para los perpetradores, a veces en cifras significativas de más de cinco dígitos. De igual forma, estas acciones son sencillamente fáciles de ejecutar en términos de tiempo y espacio, ya que pueden llevarse a cabo en un período mínimo, sin requerir la presencia física de los autores.

Asimismo, se menciona que, a pesar de la alta incidencia de estos delitos, muchos de ellos no son sancionados debido a las dificultades para su comprobación, atribuibles a su naturaleza técnica. La gran mayoría se caracterizan por ser dolosos e intencionales. La preocupante tendencia al aumento de estos delitos subraya la necesidad urgente de regulaciones a nivel nacional e internacional para combatir eficazmente este fenómeno en constante crecimiento.

3. FACTORES QUE CONTRIBUYEN A LA DELINCUENCIA INFORMÁTICA

Según la perspectiva de Segrera y Cano (2010), uno de los problemas que presenta el sistema judicial para combatir los delitos informáticos es la falta de capacitación de los operadores de derecho, ya que no todos tienen un conocimiento amplio en la materia en cuestión; representa un desafío el trabajar en este aspecto a fin de que existan expertos legalmente calificados en esta área específica (p. 221).

Uno de los principios fundamentales de la gestión, tanto en el ámbito público como privado, es que la información es poder. Hay que entender que hoy en día existen diversas esferas sociales en donde la administración de la información se considera crucial para liderar de modo eficaz, especialmente aquellas organizaciones que están en constante cambio. Para los

directivos de la justicia penal, los avances recientes en tecnologías de la información y las comunicaciones brindan oportunidades para mejorar el control operativo, la toma de decisiones y la planificación estratégica, aspectos que son fundamentales para el éxito de las entidades de la administración de justicia, tales como la policía, los tribunales y los organismos correccionales.

Si recordamos, anteriormente, los problemas relacionados con la delincuencia informática solían resolverse mediante programas y controles informáticos, partiendo de la premisa de que la respuesta a la máquina residía en ella. No obstante, con la aparición de nuevos sistemas de prevención y protección, los ciberdelincuentes encuentran nuevas maneras de eludirlos. Por lo tanto, los profesionales del sector penal, conscientes de la complejidad de los crímenes de alta tecnología, necesitan poseer conocimientos especializados para llevar a cabo investigaciones y enjuiciamientos efectivos en este ámbito, ya que, a pesar de la creciente incidencia de los crímenes informáticos, existe una significativa escasez de operadores de justicia con el nivel adecuado de conocimientos para identificar, investigar y juzgar este tipo de delitos (Segrera y Cano, 2010, p. 222).

De esta forma, la complejidad y el dinamismo inherentes a los delitos informáticos subrayan la necesidad de personal especializado con habilidades y aptitudes basadas en una continua actualización en tecnologías de la información y las comunicaciones, *a contrario sensu*, la carencia de habilidades esenciales para investigar los crímenes informáticos obstaculiza su adecuado enjuiciamiento. Por tanto, la falta de educación y capacitación adecuada puede llevar a que los jueces pasen por alto o malinterpreten evidencia crucial en la resolución de casos que involucran sistemas informáticos.

Por ello, es imperativo brindar una formación inmediata a nuestros profesionales del derecho en este ámbito, puesto que los jueces, los fiscales, los policías y los abogados necesitan poseer un entendimiento adecuado para enfrentar eficazmente este tipo de delito; de lo contrario, podríamos enfrentar dificultades en el proceso de investigación.

Así, es esencial priorizar la actualización de los expertos legales en este campo, comenzando desde la etapa de formación universitaria, pues

se considera necesario que en la mayoría de las universidades el curso de Derecho Informático sea obligatorio como parte integral del plan de estudios, y que en él se abarque la enseñanza de conceptos fundamentales como comercio electrónico, firma digital, documentos electrónicos, delitos informáticos, prueba digital y otros conocimientos relacionados con estos ciberdelitos (Espinoza Calderón, 2022, p. 56).

De la misma forma, la instrucción sobre los delitos informáticos no debe limitarse exclusivamente a las fiscalías especializadas, sino que debe extenderse a todas las fiscalías, las comisarías, los juzgados y las demás instancias, ya que estos delitos pueden ocurrir en cualquier parte de nuestro país. Por ello, es esencial proporcionar formación a la población y realizar campañas de divulgación y prevención mediante charlas en escuelas, asociaciones, medios de comunicación, entre otros. En síntesis, se necesita fomentar una cultura digital que promueva el uso correcto y responsable de internet en toda la sociedad.

En relación con los desafíos encontrados en la investigación del ciberdelito, en el 12.º Congreso de las Naciones Unidas sobre Prevención del Delito y Justicia Penal (2010) se indicó que la colaboración pronta y efectiva entre autoridades de distintos países es crucial, especialmente en casos de delitos cibernéticos donde las pruebas tienden a eliminarse automáticamente en poco tiempo, toda vez que los procedimientos oficiales prolongados pueden representar un serio obstáculo para las investigaciones. Muchos acuerdos de asistencia judicial recíproca existentes todavía se basan en procesos oficiales complejos y a menudo excesivamente tardíos. Por tanto, se considera de suma importancia establecer procedimientos ágiles para responder rápidamente a incidentes y solicitudes de cooperación internacional. El capítulo III del Convenio sobre la Ciberdelincuencia del Consejo de Europa detalla principios para la creación de un marco legal de cooperación internacional en investigaciones de delitos cibernéticos. Este capítulo aborda la creciente importancia de la cooperación internacional y promueve el uso de medios de comunicación rápidos, como el fax y el correo electrónico. También, insta a las partes en el Convenio a designar un punto de contacto disponible las veinticuatro horas del día,

todos los días de la semana, con la finalidad de responder a solicitudes de asistencia de los Estados (artículo 35).

De acuerdo con Tejada (2017), para enfrentar estos actos delictivos se requiere contar con marcos legales que faciliten la investigación criminal y aprovechar al máximo las capacidades de las tecnologías para combatir eficazmente el delito (p. 34). Finalmente, es bueno señalar que a diario nos enfrentamos a una variedad de problemas, uno de los principales es la demora en obtener información de los proveedores de servicios de internet, pues estos carecen aún de enlaces web para procesar órdenes de conservación de datos u otros procedimientos; además, persiste una cierta resistencia por parte de los proveedores de internet a proporcionar información sobre sus usuarios.

4. EL ANONIMATO DEL CIBERDELINCUENTE

En principio, cabe destacar que el numeral 1 del artículo 336 del Código Procesal Penal a la letra dice:

> Si de la denuncia, del Informe Policial o de las Diligencias Preliminares que realizó, aparecen indicios reveladores de la existencia de un delito, que la acción penal no ha prescrito, que se ha individualizado al imputado y que, si fuera el caso, se han satisfecho los requisitos de procedibilidad, dispondrá la formalización y la continuación de la Investigación Preparatoria.

Por tanto, según el artículo *in comento*, se podrá formalizar y continuar con la investigación siempre y cuando se haya individualizado al sujeto involucrado en el hecho delictivo, entre otras exigencias.

Así, una de las estrategias prevalentes en la actualidad que coadyuva y/o facilita a la creación o el aprovechamiento de circunstancias que propician a la delincuencia informática es el anonimato, toda vez que estos hechos ilícitos se caracterizan por la ocultación de la identidad real de los ciberdelincuentes o la ubicación donde se conectan (Defensoría del Pueblo, 2023, p. 15).

Cada dispositivo digital cuenta con un identificador único al conectarse a internet, conocido como dirección de protocolo IP o dirección IP; sin embargo, existen diversas formas de ocultar este identificador e incluso simular la conexión desde otro punto (lugar de ubicación), propiciando así el anonimato del ciberdelincuente, lo que se convierte en un desafío agobiante en la tarea de los operadores de justicia en la detección y la persecución de las actividades delictivas en el ciberespacio.

Desde la perspectiva de Barrio (2017b), la lucha contra la ciberdelincuencia enfrenta una serie de obstáculos provenientes de diversos factores técnicos que complican la identificación y la persecución de los delitos cometidos a través de internet, ello contribuye significativamente al incremento de la ciberdelincuencia. En ese sentido, señala que el anonimato viene a constituirse como uno de esos factores (p. 43), toda vez que brinda a los ciberdelincuentes una capa de protección que impide su identificación, lo que complica los esfuerzos de las autoridades para rastrear y procesar a aquellos que cometen delitos en el ciberespacio.

En esa línea de ideas, este autor señala dos factores elementales que dificultan o imposibilitan la lucha contra la ciberdelincuencia: el principal factor es el anonimato del autor y, además, la ejecución del delito a distancia. Con relación al anonimato, es significativo mencionar que muchas veces resulta desafiante poder esclarecer la perpetración de un delito realizado a través de las redes digitales. De esta forma, la plena identificación del autor detrás de un presunto ciberdelito puede ser una tarea complicada.

Para ello, se debe tener en cuenta que cada dispositivo conectado a internet posee una dirección IP, que funciona como el «DNI electrónico» del terminal. En muchos casos, la detección y seguimiento de esta dirección IP no parece ser compleja inicialmente, ya que es un dato público y de carácter personal; sin embargo, existen técnicas para enmascarar o manipular esta asignación, dentro de las cuales se incluye la posibilidad de conectarse a través de redes wifi abiertas, el uso de proxies o redes privadas virtuales (VPN), así como la creación de redes botnet (Barrio, 2017b, p. 43).

Por tanto, el anonimato de los ciberdelincuentes se constituye en la principal dificultad para los fiscales y las autoridades policiales en la investigación penal. Por ejemplo, en casos de fraudes informáticos, aunque se identifique la identidad del titular de la cuenta receptora de aquellos fondos provenientes de transferencias no autorizadas desde la cuenta de la víctima, no siempre se puede considerar a esta persona como el sujeto activo, pues quien recibe el dinero no necesariamente es el responsable de las operaciones fraudulentas (Espinoza Calderón, 2022, p. 47).

Existen diversos casos en los que es común observar que la cuenta beneficiada de aquellas transferencias fraudulentas suele pertenecer a otra víctima más. En ocasiones, los delincuentes incluso llegan a apropiarse de diversas cuentas y las utilizan con propósitos ilícitos, esto es, como cuentas receptoras. Para tales fines ilícitos, los ciberdelincuentes se las ingenian para que las víctimas proporcionen de forma culposa toda la información necesaria para sustraerles todo su dinero.

Así, los ciberdelincuentes suelen crear páginas falsas del Banco de la Nación, en las que supuestamente se puede tramitar y solicitar la clave token de forma digital, donde piden el número de tarjeta, la clave, entre otra información personal que normalmente no es solicitada por el banco; es suficiente que la víctima introduzca tal información en dicha página falsa para que estos sujetos puedan sustraer todo el dinero de su cuenta bancaria.

En síntesis, según Villavicencio (2014), las principales características de vulnerabilidad presentes en el entorno informático vendrían a ser las siguientes:

i. La ausencia de una jerarquía en la red que permita establecer sistemas de control, lo que genera complicaciones al momento de verificar la información que circula por este medio.
ii. El constante aumento del número de usuarios sin conocimiento sobre los riesgos de la tecnología.
iii. El anonimato de los cibernautas, que dificulta la ubicación posterior a la comisión del ciberdelito.

iv. La facilidad de acceso a la información, lo que posibilita la manipulación de datos y la destrucción de sistemas informáticos (p. 285).

Además de lo mencionado, es propicio resaltar, como lo señaló la Defensoría del Pueblo (2023), que la Interpol, una institución gubernamental que reúne a ciento noventa y cuatro cuerpos policiales a nivel mundial, ha indicado adicionalmente seis factores que contribuyen a la ciberdelincuencia:

i. La creciente conectividad, ya que cada vez son más las personas que se conectan en línea con un bajo nivel de conciencia e información sobre seguridad digital y esparcen información personal.
ii. La movilidad, ya que genera más transacciones, comunicaciones y negocios en línea sin las debidas medidas de seguridad necesarias.
iii. La interconexión, que contribuye a la ampliación del número de dispositivos digitales potencialmente vulnerables, debido a la rápida expansión de ciudades y hogares inteligentes.
iv. La sofisticación, la constante evolución de las habilidades y las tácticas de aquellos expertos en cibernética, que ofrecen sus servicios a quienes estén dispuestos a pagar por ellos sin importar que se trate de servicios ilícitos.
v. La falta de información sobre la magnitud, el alcance y el funcionamiento de este fenómeno criminal, ligada a la renuencia de las víctimas a denunciar por desconocimiento, por la creencia de que no vale la pena, por vergüenza u otras razones.
vi. Las complejas y transfronterizas investigaciones que implican el esclarecimiento de los hechos por parte de las autoridades judiciales (p. 16).

Por tanto, si el Ministerio Público no logra identificar y/o individualizar a estos ciberdelincuentes, no podrá continuar con la investigación y, por ende, tendrá que archivar el proceso. En consecuencia, la razón primordial para que los delitos informáticos queden en total impunidad se debe mayormente a la falta de individualización del sujeto activo, pues el

numeral 1 del artículo 336 del Código Procesal Penal señala que la formalización de la investigación procederá, entre otras razones, cuando el sujeto haya sido individualizado.

5. ANÁLISIS DEL ACUERDO PLENARIO N.º 7-2006/CJ-116

El Acuerdo Plenario n.º 7-2006/CJ-116 versa sobre cuestión previa e identificación del imputado y surge para analizar la problemática que se generaba ante la falta de individualización del sujeto por parte de la fiscalía. De esta forma, muchos de los juzgados penales del país, de manera oficiosa, disponían una cuestión previa; por tanto, anulaban todo lo actuado y se daba por no presentada la denuncia. En esa línea de ideas, antes de la emisión del mencionado acuerdo plenario, muchos de los procesos eran resueltos de oficio como cuestión previa. Ello significaba que diversas formalizaciones de denuncias fueran archivadas. En este acuerdo plenario se determinó que, para la individualización, se exige únicamente la identificación del presunto responsable con sus nombres y sus apellidos.

En principio, se debe tener en claro que la continuidad del proceso penal está supeditada a la individualización del sujeto, que debe estar claramente identificado, debe proporcionar sus nombres y sus apellidos completos, así como su documento de identidad. Además, se deben proporcionar otros datos personales adicionales que lo distingan y lo hagan único, como su edad (para saber su capacidad legal), su lugar de nacimiento, los nombres de sus padres, su situación familiar, su dirección, su nivel educativo, su ocupación y sus características físicas (Viza, 2018, «La individualización como presupuesto para la apertura de instrucción», párr. 1).

Es así que identificar de manera plena a la persona a la que se le imputa la comisión de un delito es de suma importancia, esto con la finalidad de garantizar que el proceso judicial se dirija contra la persona correcta y no contra alguien que no esté relacionado con los hechos. Asimismo, la identificación individualizadora del sujeto es determinante para la emisión y la ejecución de órdenes de detención, las cuales deben contener la información necesaria del individuo que está siendo perseguido por la justicia, con el fin de evitar confusiones o casos de homonimia.

En ese sentido, uno de los presupuestos para dar inicio a un proceso judicial es precisamente la correcta identificación del imputado, ya que simplemente no basta con conocer la existencia del acusado e identificarlo por su nombre y su apellido; sino que también es necesario determinar con precisión quién es esta persona, para ello se proporcionan sus datos adicionales. Por lo tanto, el juez debe analizar si la identificación del sujeto bajo investigación se ha realizado correctamente. Esta exigencia garantiza proteger contra posibles actos arbitrarios o errores, asegurando que el Estado siempre dirija sus acciones contra la persona que verdaderamente ha cometido el hecho ilícito.

Asimismo, debemos señalar lo que establece el fundamento 7 del Acuerdo Plenario n.º 7-2006/CJ-116, en el cual se establece que para iniciar una acción penal y abrir un proceso judicial contra una persona, es necesario identificar al imputado con sus nombres y sus apellidos completos. En tal sentido, a fin de proseguir con el proceso penal basta que se cumpla dicha referencia (apellidos y nombres), y se da por concretado el mencionado requisito de admisibilidad. De igual forma, la Corte Suprema ha determinado que estos son los únicos datos requeridos para el inicio del proceso penal, sin hacer referencia a la necesidad de información adicional.

En la actualidad, nuestro Código Procesal Penal utiliza el término individualizar, que implica singularizar y particularizar completamente al imputado con los datos que lo distinguen como una persona única e inconfundible. La plena individualización del sujeto cumple determinados objetivos:

i. Asegurar que el proceso se dirija contra una persona específica y verificada, para así evitar acciones legales contra individuos no relacionados con los hechos o posibles homónimos.
ii. Facilitar la solicitud y, si es necesario, la imposición de medidas de coerción personal de acuerdo a ley.
iii. Individuar adecuadamente al imputado le permite garantizar su derecho fundamental de defensa a fin de que pueda plantear las acciones legales que le favorezcan. (Viza, 2018, «Respecto a la individualización del imputado», párr. 4)

Tal como ha mencionado la Corte Suprema, los únicos datos necesarios para identificar al imputado son sus nombres y sus apellidos. Sin embargo, al emitir una orden de captura contra alguien, lo que implica una restricción de su libertad, se necesitan otros datos adicionales con la finalidad de evitar detenciones arbitrarias debido a posibles coincidencias de nombres.

Por esa razón, la Corte Suprema, en el fundamento 8 del Acuerdo Plenario n.º 7-2006/CJ-116, ha determinado que la orden de detención emitida por el órgano jurisdiccional debe contener los siguientes datos esenciales para identificar al presunto autor: nombres y apellidos completos, edad, sexo y características físicas, incluyendo talla y contextura. En caso de que falte alguno de estos en la orden de captura, la policía tiene la autoridad para pedir que el órgano judicial correspondiente aclare la situación.

Es así que el Tribunal Constitucional, en referencia a la individualización en la detención, ha adoptado la siguiente postura: la orden de detención emitida por el órgano jurisdiccional debe incluir, con carácter obligatorio y bajo responsabilidad, los siguientes datos para identificar al presunto autor: (a) nombres y apellidos completos, (b) edad, (c) sexo, y (d) características físicas, altura y contextura (Expediente n.º 07395-2006-PHC/TC).

Por lo tanto, en casos específicos, si se emitiese una orden de arresto sin una individualización completa del imputado, el Tribunal Constitucional determinaría que se transgredió el derecho a la libertad personal del recurrente homónimo de manera injustificada.

La Corte Suprema ha determinado que la presentación de una cuestión previa procede solo en situaciones donde no sea posible identificar plenamente los nombres y los apellidos de una persona, o cuando se confirme que se ha utilizado una identidad falsa o inexistente. Sin embargo, en el fundamento 10 del Acuerdo Plenario n.º 7-2006/CJ-116 se estableció que si se plantea una cuestión previa basada únicamente en la falta de inscripción del imputado en el Registro Nacional de Identificación y Estado Civil (Reniec), o en la omisión del número de su documento nacional de

identidad (DNI), dicho planteamiento no tiene la relevancia o el fundamento necesario para ser aceptado. Además, el juez penal no podrá rechazar la denuncia fiscal solo por este motivo.

Para entender la cuestión previa, se puede señalar que esta tiene como propósito cuestionar la validez de una relación jurídica procesal, y se destaca la ausencia de un requisito o una declaración extrapenal necesaria para iniciar la acción penal. En otras palabras, es un recurso de defensa técnica que se presenta contra la acción penal por la falta de cumplimiento de los requisitos previos que condicionan su ejercicio. Es importante tener en cuenta que esto no implica que tenga efectos de cosa juzgada, ya que el proceso se suspende hasta que se subsane o se obtenga el requisito previo necesario; luego, la denuncia prosigue su curso.

6. ALTERNATIVAS DE SOLUCIÓN EN LOS DELITOS INFORMÁTICOS

6.1. Creación de herramientas tecnológicas

Es menester mencionar que, durante el 12.º Congreso de las Naciones Unidas sobre Prevención del Delito y Justicia Penal, se abordaron algunos mecanismos y recursos legales muy importantes que deben ser tomados en cuenta. En ese sentido, debemos señalar que existe la necesidad de requerir la presencia de instrumentos legales, toda vez que la efectividad de la aplicación de la ley se encuentra fuertemente ligada a la disponibilidad de herramientas de investigación, por ejemplo, aquellos programas informáticos forenses que sirven para poder recopilar pruebas, registrar pulsaciones del teclado y recuperar archivos eliminados. Asimismo, es esencial contar con programas informáticos y bases de datos para gestionar investigaciones, e incorporar características como «hash» para imágenes de pornografía infantil (Espinoza Calderón, 2022, p. 58).

Es así que en los últimos años se ha trabajado en el desarrollo continuo de estas herramientas. Por ejemplo, en el Colegio Universitario de Dublín, se viene elaborando un proyecto de investigación llamado «Reconstrucción Automática de Eventos para el Análisis Forense Digital y

de Intrusiones». Además, en los Estados Unidos, se implementó una nueva tecnología llamada Photo DNA con la finalidad de poder ubicar o rastrear la pornografía infantil. A pesar de estos avances, sigue siendo crucial abordar la coordinación en el desarrollo de estas herramientas para evitar duplicaciones. Esto se extiende a la necesidad de coordinar los esfuerzos de las redes de puntos de contacto, como las del Grupo de los Ocho, Interpol y la red asociada al Convenio sobre la Ciberdelincuencia.

Los delitos informáticos son perpetrados mediante el empleo de herramientas digitales avanzadas, por lo que las personas o, en este caso, los investigadores encargados de abordar estos delitos deben poseer, como mínimo, las mismas herramientas utilizadas por los delincuentes, e incluso deben contar con recursos superiores, como *software* y *hardware* actualizado, toda vez que va a permitir realizar una lucha efectiva contra la ciberdelincuencia, razón por la cual la adquisición de estas herramientas se vuelve imperativa y urgente para enfrentar este tipo de delito de manera eficaz.

6.2. Fomento de la capacitación

Asimismo, se estableció que el problema del delito cibernético no se limita a los países desarrollados, sino que también afecta a las naciones en desarrollo. En ese sentido, según el reporte realizado por la Development Gateway Foundation, existían más usuarios que utilizaban internet en los países en desarrollo que en las naciones industrializadas.

Es por ello que la Asamblea General, mediante la Resolución 64/179, enfocada en fortalecer el Programa de las Naciones Unidas en materia de prevención del delito y justicia penal, destacó nuevas cuestiones de política como la piratería, el delito cibernético, la explotación sexual de niños y la delincuencia urbana, e instó a la Oficina de las Naciones Unidas contra la Droga y el Delito (UNODC) a abordar estas situaciones según su mandato. La investigación y el enjuiciamiento de delitos cibernéticos resulta desafiante para todas las instituciones involucradas debido a la complejidad del tema y al constante avance tecnológico. La capacitación continua de todas las autoridades involucradas sigue siendo un aspecto crucial. El

grupo de expertos pertenecientes a la UNODC comentaron sobre el delito cibernético y señalaron que el fortalecimiento de la capacidad institucional y la sostenibilidad a largo plazo eran factores clave para evaluar el éxito de futuras iniciativas (Espinoza Calderón, 2022, p. 59).

Además, es imperativo fortalecer las instituciones dedicadas a combatir la ciberdelincuencia, lo cual implica la emisión de directivas y protocolos, así como la realización de modificaciones y adiciones a la legislación procesal y a las leyes especializadas que faciliten la lucha contra los delitos informáticos. De manera similar, este fortalecimiento debería incluir la formación del personal y la provisión de la logística esencial.

Así, con la finalidad de llevar a cabo eficientemente la investigación y el proceso legal del ciberdelito, es esencial que los profesionales judiciales reciban una formación especializada. En ese contexto, el 12.º Congreso de las Naciones Unidas sobre Prevención del Delito y Justicia Penal aborda la necesidad de capacitar a los operadores de justicia debido a las complicaciones inherentes a la investigación y el enjuiciamiento de delitos cibernéticos, por lo que resulta crucial proporcionar capacitaciones a los agentes encargados de hacer cumplir la ley, fiscales y jueces. En la reunión del grupo de expertos de la UNODC sobre delito cibernético en Viena, se resaltó que la mayoría de las organizaciones internacionales y regionales involucradas en este tema han tomado medidas para incentivar a los expertos que participan en la investigación de delitos cibernéticos y para desarrollar material educativo.

En ese sentido, podemos recalcar la importancia fundamental de proporcionar formación al personal, tanto en organismos especializados como en otras instituciones, con el objetivo de que, desde sus respectivas funciones, contribuyan a la eficacia de la prevención del ciberdelito. En el caso de los profesionales de la justicia involucrados en la lucha contra el ciberdelito, la capacitación debe ser continua y rigurosa.

6.3. Apoyo de la UNODC

Conforme a lo indicado en el 12.º Congreso de las Naciones sobre la Prevención del Delito y Justicia Penal, la UNODC se posiciona como el

«organismo responsable de establecer estándares en materia de prevención del delito y justicia penal» y brinda apoyo, principalmente, a los países en desarrollo. Además, añade que la oficina continuará adoptando un enfoque integral, multidisciplinario y colaborativo, combinando sus conocimientos probados en los campos jurídico, técnico y de aplicación de la ley para enfrentar las actividades delictivas.

Asimismo, la UNODC tiende a colaborar con expertos y suele utilizar herramientas apropiadas, incluyendo aquellas provenientes del sector privado, proveedores de servicios de internet, para abordar el problema en países o regiones específicas. Además, se brinda prioridad a la provisión de asistencia técnica a los Estados miembros que lo requieran, con el objetivo de superar las deficiencias en capacidad y competencia técnica, para así asegurar la sostenibilidad a largo plazo en la lucha contra los delitos informáticos.

De la misma forma, la UNODC prioriza la ayuda a los Estados miembros en la implementación de una legislación que sea eficaz en la investigación de los delitos informáticos y de esa forma lograr el enjuiciamiento de los responsables. Ello requiere, necesariamente, mejorar la competencia operativa y técnica de jueces, fiscales y agentes del orden en asuntos relacionados con el delito cibernético, mediante capacitación, adaptación o creación de material didáctico sobre la investigación y el enjuiciamiento a los autores de los delitos informáticos. Asimismo, brinda capacitación a las autoridades encargadas de hacer cumplir la ley en el uso efectivo de mecanismos de cooperación internacional contra el delito cibernético; por otro lado, incentiva a las autoridades para que colaboren en la prevención y el combate de los delitos cibernéticos (Espinoza Calderón, 2022, p. 61).

La colaboración y la asistencia técnica proporcionadas por la UNODC son altamente valoradas, ya que esta institución se ha convertido en un valioso aliado para la formación de nuestros profesionales legales. Asimismo, la Unidad de Cooperación Judicial Internacional y de Extradiciones del Ministerio Público desempeña una función crucial al manejar solicitudes de asistencia judicial dirigidas a proveedores de servicios de

internet; además, suele brindar directrices sobre la autogestión de información a través de plataformas de redes sociales y aplicaciones.

Nuestra legislación no fue ajena a la problemática que acarrean los delitos informáticos. Ante ello, hubo esfuerzos normativos para combatir la ciberdelincuencia. De esta forma, en el ámbito probatorio respecto a los delitos informáticos, la Ley n.º 30096, Ley de Delitos Informáticos, reguló tres aspectos esenciales para la averiguación de los hechos sobre los ciberdelitos. En primer lugar, estableció que la facultad proporcionada a los jueces de controlar y conocer las comunicaciones también será extendida a las personas que son sujetos de investigación por la comisión de algún delito informático. En segundo lugar, se aprobó que cuando se trata de delitos informáticos se podrá aplicar la colaboración eficaz, a fin de facilitar el rol investigador del Ministerio Público. Finalmente, se estableció que los procedimientos relativos a la investigación, el juzgamiento y la sanción de los delitos dados dentro de una organización criminal también son compatibles con los delitos informáticos.

A fines del año 2020, el Ministerio Público organizó una comisión competente para evaluar técnicamente la creación de un plan piloto de fiscalía u organismo especializado en delitos informáticos. Este organismo estuvo conformado por diversos fiscales y funcionarios de dicha institución, y también contó con el apoyo técnico de la Embajada de los Estados Unidos; de esta forma, se crea la Unidad Fiscal Especializada en Ciberdelincuencia del Ministerio Público. Dicha unidad fiscal tiene como principales roles: dictar los lineamientos, unificar criterios de aplicación de las normas y acompañar técnicamente las investigaciones fiscales de los delitos informáticos. El rol que tiene el Ministerio Público en realizar las investigaciones correspondientes en estos tipos de delitos se dificulta por la falta de respuesta cabal y oportuna de parte de las instituciones bancarias y financieras, y de aquellas empresas que realizan actividades de telecomunicaciones. En esa línea de ideas, la eficacia de combatir los delitos informáticos no solo está en manos de los operadores del derecho, sino de todas las instituciones, al facilitar la información que requieren las entidades del Poder Judicial, el Ministerio Público y la Policía Nacional del Perú.

7. CONCLUSIONES

Los delitos informáticos se constituyen como aquellos actos ilícitos existentes en la tecnología, que transgreden a la propiedad privada intelectual, económica y la privacidad de las personas, las organizaciones y del propio Estado. Cada día se puede observar que este tipo de delito sigue en un aumento alarmante. Un factor contribuyente al problema es el desconocimiento y el uso negligente de los usuarios, lo que facilita la tarea de los ciberdelincuentes, ya que encuentran oportunidades para atentar contra ellos.

Ante la presencia de esta nueva modalidad delictiva, no cabe duda alguna de que el ordenamiento jurídico también debe adaptarse a la delincuencia tecnológica, en caso contrario, no podrá combatir y sancionar tales actos. Si bien diferentes países como el nuestro se esforzaron para regular legislativamente esta forma delictiva, hasta el día de hoy existen diversos vacíos legales que, de cierta forma, contribuyen a la impunidad de los delitos informáticos.

Sin miedo a equivocarnos, podemos decir que, actualmente, la delincuencia informática está un paso por delante del ordenamiento jurídico. Ello se observa y se contrasta en los diversos casos de delitos informáticos archivados en sede preliminar por el representante del Ministerio Público, toda vez que no logra identificar al auto del delito informático. En consecuencia, el Estado peruano debe prontamente ejecutar las políticas criminales necesarias para hacer frente a los delitos informáticos, ya que sus efectos son tremendamente perjudiciales para la sociedad y para el Estado.

REFERENCIAS

Animaca, Y. A. (2023). *Delitos informáticos y la ciberdelincuencia con el uso de las nuevas tecnologías en Lima Centro 2022* [Tesis de maestría, Universidad César Vallejo]. https://repositorio.ucv.edu.pe/bitstream/handle/20.500.12692/122811/Anicama_AYA-SD.pdf?sequence=1&isAllowed=y

Barrio, M. (2017a). *Ciberdelitos. Amenazas criminales del ciberespcio.* Reus.

Barrio, M. (2017b). *Fundamentos del derecho de internet.* Centro de Estudios Políticos y Constitucionales.

Chavarría, G. R. (2023). *Delitos informáticos y la implementación de la Unidad Fiscal Especializada en Ciberdelincuencia del Ministerio Público en el Perú* [Tesis de maestría, Universidad César Vallejo]. https://repositorio.ucv.edu.pe/handle/20.500.12692/129744

Defensoría del Pueblo (2023). *La ciberdelincuencia en el Perú: estrategias y retos del Estado.* Informe Defensorial n.º 001-2023-DP/ADHPD. https://www.defensoria.gob.pe/wp-content/uploads/2023/05/INFORME-DEF-001-2023-DP-ADHPD-Ciberdelincuencia.pdf

Espinoza Calderón, V. R. (2022). *Delitos informáticos y nuevas modalidades delictivas.* Instituto Pacífico.

Espinoza Prado, V. (2022). *Análisis de los delitos informáticos y el valor probatorio de la evidencia digital en la Corte Superior de Justicia de Lima - 2021* [Tesis de licenciatura, Universidad César Vallejo]. https://repositorio.ucv.edu.pe/bitstream/handle/20.500.12692/90185/Espinoza_PV-SD.pdf?sequence=1

Flores, L. L. (2014). *Derecho informático.* Patria.

Segrera, M. L. y Cano, J. J. (2010). La formación de los jueces en temas de delito informático y la evidencia digital en el contexto internacional y sus implicaciones en la administración de justicia en Colombia. En J. J. Cano (coord.), *El peritaje informático y la evidencia digital en Colombia. Conceptos, retos y propuestas* (pp. 179-236). Universidad de los Andes.

Tejada, E. (2017). Novedades en la tipificación de determinados delitos vinculados a la criminalidad informática en el Código Penal español: evolución legislativa y adaptación a la normativa internacional. En D. Dupuy (dir.) y M. Kiefer (coord.), *Cibercrimen. Aspectos de derecho penal y procesal penal. Cooperación internacional. Recolección de evidencia digital. Responsabilidad de los proveedores de servicio de internet* (pp. 33-57). BdeF.

Tobares, G. H. y Castro, M. J. (2010). *Delitos informáticos.* Advocatus.

Villavicencio, F. (2014). Delitos informáticos. *Ius et Veritas*, (49), 284-304. https://revistas.pucp.edu.pe/index.php/iusetveritas/article/view/13630

Viza, J. H. (2018). Análisis del Acuerdo Plenario 7-2006/CJ-116. Cuestión previa e identificación del imputado. *LP Pasión por el Derecho.* https://lpderecho.pe/acuerdo-plenario-7-2006-cuestion-previa-identificacion-imputado/#_ftn5

Fuentes normativas y jurisprudenciales

Acuerdo Plenario n.º 7-2006/CJ-116 (2006). Corte Suprema de Justicia de la República (13 de octubre de 2006). https://www.pj.gob.pe/wps/wcm/connect/2d16b9804075bac9b71ff799ab657107/acuerdo_plenario_07-2006_CJ_116.pdf?MOD=AJPERES&CACHEID=2d16b9804075bac9b71ff799ab657107

Expediente n.º 07395-2006-PHC/TC (2007). Tribunal Constitucional (27 de junio de 2007). https://tc.gob.pe/jurisprudencia/2007/07395-2006-HC.pdf

Informe del 12.º Congreso de las Naciones Unidas sobre Prevención del Delito y Justicia Penal (2010). https://www.unodc.org/documents/crime-congress/12th-Crime-Congress/Documents/A_CONF.213_18/V1053831s.pdf

Financiamiento
Autofinanciado.

Conflicto de intereses
La autora declara no tener conflicto de intereses.

Contribución de autoría
La autora ha participado en el desarrollo del proceso de investigación, en la elaboración y en la redacción del artículo, así como en la aprobación final de la versión que se publicará.

Agradecimientos
La autora agradece los alcances brindados por los jueces penales respecto a sus inquietudes y sus observaciones sobre el tema en comento, que dieron origen a esta publicación. Asimismo, agradece el apoyo en la recolección de datos del colega Edgar Johan Cantaro Sanchez.

Biografía de la autora
Catalina Tania Estrada Salvador Ramírez, abogada graduada y titulada en la Universidad de Huánuco. Se encuentra cursando la maestría en Derecho Penal en la mencionada casa de estudios. Se ha desempeñado por más de cuatro años como asistente de juez superior en la Corte Superior de Justicia de Huánuco, y, en la actualidad, labora como secretaria administrativa de Presidencia.

Correspondencia
cestradas@pj.gob.pe