UNIVERSIDAD CÉSAR VALLEJO

ESCUELA DE POSGRADO

PROGRAMA ACADÉMICO DE MAESTRÍA EN DERECHO PENAL Y PROCESAL PENAL

Proliferación de la ciberdelincuencia como afectación al bien jurídico del derecho a la identidad, Callao 2022

TESIS PARA OBTENER EL GRADO ACADÉMICO DE:

Maestra en Derecho Penal y Procesal Penal

AUTORA:

Flores Rosario, Jessica Andrea (orcid.org/0009-0004-1055-0820)

ASESORES:

Dr. Neyra Villanueva, Javier Alejandrino (orcid.org/0000-0003-4644-5008)

Dra. Quiñones Li, Aura Elisa (orcid.org/0000-00002-5105-1188)

LÍNEA DE INVESTIGACIÓN:

Derecho Penal, Procesal Penal, Sistema de Penas, Causas y Formas del Fenómeno Criminal

LÍNEA DE RESPONSABILIDAD SOCIAL UNIVERSITARIA:

Fortalecimiento de la democracia, liderazgo y ciudadanía

LIMA – PERÚ

2023

DEDICATORIA

A mi hija Daniella Andrea, quien dio un sentido diferente a mi vida y es la razón que día a día me hace ser mejor persona y profesional.

A mi hermano Andrés Paúl que es mi ángel que me cuida desde el cielo.

AGRADECIMIENTO

A mis padres Sebilla y Andrés, por su apoyo incondicional y motivación a superarme cada día.

A Dany por impulsarme a conseguir esta meta y estar a mi lado en todo momento.

UNIVERSIDAD CÉSAR VALLEJO

ESCUELA DE POSGRADO

MAESTRÍA EN DERECHO PENAL Y PROCESAL PENAL

Declaratoria de Autenticidad del Asesor

Yo, NEYRA VILLANUEVA JAVIER ALEJANDRINO, docente de la ESCUELA DE POSGRADO MAESTRÍA EN DERECHO PENAL Y PROCESAL PENAL de la UNIVERSIDAD CÉSAR VALLEJO SAC - LIMA NORTE, asesor de Tesis titulada: "Proliferación de la ciberdelincuencia como afectación al bien jurídico del derecho a la identidad, Callao 2022", cuyo autor es FLORES ROSARIO JESSICA ANDREA, constato que la investigación tiene un índice de similitud de 17.00%, verificable en el reporte de originalidad del programa Turnitin, el cual ha sido realizado sin filtros, ni exclusiones.

He revisado dicho reporte y concluyo que cada una de las coincidencias detectadas no constituyen plagio. A mi leal saber y entender la Tesis cumple con todas las normas para el uso de citas y referencias establecidas por la Universidad César Vallejo.

En tal sentido, asumo la responsabilidad que corresponda ante cualquier falsedad, ocultamiento u omisión tanto de los documentos como de información aportada, por lo cual me someto a lo dispuesto en las normas académicas vigentes de la Universidad César Vallejo.

LIMA, 30 de Julio del 2023

Apellidos y Nombres del Asesor:	**Firma**
NEYRA VILLANUEVA JAVIER ALEJANDRINO **DNI:** 41440286 **ORCID:** 0000-0003-4644-5008	Firmado electrónicamente por: JNEYRAV el 05-08-2023 10:56:55

Código documento Trilce: TRI - 0627757

INVESTIGA UCV

ÍNDICE DE CONTENIDOS

ÍNDICE DE TABLAS

RESUMEN

El objeto de la presente investigación de analizar la manera en que la proliferación de la ciberdelincuencia afecta el bien jurídico del derecho a la identidad, Callao 2022. Se trata de una investigación que responde a una realidad actual en la cual los delitos a nivel cibernético van en incremento. En el aspecto metodológico es una investigación cualitativa, con diseño de teoría fundamentada, de nivel descriptivo y analítico, cuyo instrumento de recolección de datos fue la entrevista estructurada de acuerdo a los objetivos, categorías y subcategorías. En la recolección de datos participaron seis fiscales que laboran en el Distrito Fiscal del Callao. Los resultados de la investigación indican que la ciberdelincuencia es una realidad latente que afecta a la sociedad peruana. Las modalidades cada vez más son sofisticadas y la ciberseguridad no va de acuerdo a las demandas sociales, tampoco las leyes existentes surten los efectos esperados para proteger a la sociedad de los ataques cibernéticos que afectan al derecho a la identidad. Se concluye que, ante este tipo de realidad delictiva, es importante la acción preventiva y el uso responsable de los sistemas comunicación a fin de proteger los datos personales.

Palabras clave: ciberdelincuencia, derecho a la identidad, cibercrimen, delitos informáticos.

ABSTRACT

The purpose of this investigation is to analyze the way in which the proliferation of cybercrime affects the legal right to identity, Callao 2022. It is an investigation that responds to a current reality in which crimes at the cyber level are in increment. In the methodological aspect, it is a qualitative research, with a grounded theory design, at a descriptive and analytical level, whose data collection instrument was the interview structured according to the objectives, categories and auctions. Six prosecutors who work in the Callao Fiscal District participated in the data collection. The results of the investigation indicate that cybercrime is a latent reality that affects Peruvian society. The modalities are increasingly sophisticated and cybersecurity does not meet social demands, nor do existing laws have the expected effects to protect society from cyber-attacks that affect the right to identity. It is concluded that, in the face of this type of criminal reality, preventive action and the responsible use of communication systems are important in order to protect personal data.

Keywords: cybercrime, right to identity, cybercrime, computer crimes.

I. INTRODUCCIÓN

A nivel internacional, la ciberdelincuencia es una realidad alarmante por la incidencia que genera tanto en el entorno social como en la vida de las personas y las familias. Pues, según la evidencia científica aportada por Benites (2022), actualmente el 59,5% (4.660.000.000) de la población mundial tiene acceso a la red. Ello evidencia que, la sociedad se encuentra en constante comunicación por medios informáticos; lo cual puede desprenderse que su uso excesivo y no supervisado ha generado la aparición de ilícitos como el sabotaje informático, pornografía infantil, el acceso sin autorización a información privada, la piratería informática, entre otros. Ello ha expandido el campo de estudio pertinente a los juristas y con ello introducir nuevos retos a los que se debe enfrentar.

El desarrollo en las sociedades modernas, la evolución tecnológica, la globalización y con ello la especialización en las Tecnologías de Información y Comunicación, brindan un espacio amplio e indeterminado a los delincuentes para transgredir los derechos constitucionales de las personas: dignidad, intimidad e identidad (Zarate y Becerra,2021). Por lo que, la configuración de ciberdelito se refiere a aquella acción cometida a través de la red con fines ilícitos, que puede causar daño tanto a las redes comunicacionales como al patrimonio de un individuo (Fernández y Vargas, 2018).

La Corte Interamericana de Derechos Humano señala “el derecho a la identidad es el conjunto de atributos y características que permiten la individualización de la persona en sociedad” (Opinión Consultiva OC-24/17, 2017, fj. 90).

A nivel de América Latina, según refiere López (2022) el cibercrimen es un fenómeno que ha sido configurado por el uso desmedido del internet en los diferentes aspectos de la vida (en el trabajo, en la forma de comunicarse, entre otros). Así pues, cada vez más el ámbito social y personal del individuo pasa del espacio físico al virtual; poniendo en peligro los bienes jurídicos protegidos. Según Becerra (2022) en Latinoamérica en el año 2021 se incrementó los ciberataques en

un 4% en comparación al año 2020; y los países más afectados fueron México, Brasil y Perú. De acuerdo con el Índice de Inteligencia de Amenazas X-Force de IBM Security; el método más implementado por los ciberdelincuentes fue el “ransomware”; representando el 21% de los ataques en América Latina y el 29% a nivel mundial.

A nivel nacional, la afectación que genera la ciberdelincuencia en el “derecho a la identidad”, está referida al quebrantamiento de la proyección que tiene un sujeto sobre sí mismo (Díaz, 2020). Pues, el Artículo 2, de nuestra Constitución Política regula que: “Toda persona tiene derecho: 1. A la vida, a su identidad, a su integridad moral, psíquica y física y a su libre desarrollo y bienestar”.

Es así, que uno de los delitos cibernéticos principales que atentan contra el bien jurídico tutelado de la “identidad”, es la denominada “suplantación de identidad” cuya tipificación se encuentra en la Ley N.° 30096, que señala en su Artículo 9° sanción penal con privación de libertad por suplantación de identidad y de ello resulte un perjuicio. Este delito es cometido mediante el Hackeo, Sim Swapping, Deepfake o Spoofing; que radica en suplantar a una persona y extraer sus datos íntimos con finalidad delictivas (Rivera et al., 2022).

Desde esa óptica, la presente investigación tiene justificación a nivel teórico, metodológico, sociológico, jurídico y práctico. En el aspecto teórico, el trabajo se basa en el estudio de los trabajos académicos previos que están publicados en diferentes medios de soporte como bases de datos, revistas, libros. Además, tiene justificación de carácter social porque la problemática que se investiga forma parte de una realidad social permanente. Esta situación hace que la investigación tenga justificación jurídica porque busca regular y sancionar los comportamientos delictuosos que cada vez más resultan sofisticados que pueden quebrantar el derecho a la intimidad y privacidad, por lo tanto, presenta también una justificación práctica porque coadyuva al conocimiento y prevención de este tipo de delitos (Fernández, 2020). Finalmente tiene justificación metodológica toda vez que se

analizó la fuente documental, esto es trabajos previos realizados así como la normativa a nivel nacional e internacional.

Por lo tanto, esta investigación tiene relevancia social por cuanto vislumbra una realidad alarmante que afecta a la sociedad en general y por lo mismo, resulta relevante a nivel profesional, toda vez que, como agentes activos y operadores del derecho, no se puede estar al margen de esta situación, sino coadyuvar en la búsqueda de los mecanismos de solución.

Por ende, la pregunta general de la investigación es: ¿De qué manera la proliferación de la ciberdelincuencia afecta el bien jurídico del derecho a la identidad, Callao 2022? Las preguntas específicas son: 1. ¿De qué modo la caracterización actual de la ciberdelincuencia repercute en el derecho a la identidad? 2. De qué forma las sanciones penales ante la ciberdelincuencia incide en la mitigación de la misma? 3. ¿De qué manera la legislación peruana favorece a la ciberseguridad como antídoto a los delitos cibernéticos?

Por ello, el objetivo general de la investigación consiste en analizar cómo la proliferación de la ciberdelincuencia afecta el bien jurídico del derecho a la identidad, Callao 2022. Los objetivos específicos son: 1. Describir el modo en que la caracterización actual de la ciberdelincuencia repercute en el derecho a la identidad. 2. Analizar la forma en que los fines de la pena ante la ciberdelincuencia incide en la mitigación de la misma. 3. Delimitar la manera en que la legislación peruana favorece a la ciberseguridad como antídoto a los delitos cibernéticos.

II. MARCO TEÓRICO

A nivel internacional, Rodríguez (2018) en su investigación planteó como objetivo determinar la clasificación de delitos informáticos cometidos por redes sociales tipificados según la Ley de Ecuador. Implementó una metodología de tipo exploratorio y descriptivo, método inductivo mediante el análisis documental. Los resultados indicaron que según la normativa ecuatoriana existen los siguientes delitos cibernéticos: Pharming, suplantación de identidad, violación a la intimidad, child grooming, entre otros. Concluyó que, los usuarios de las distintas redes sociales -Facebook, Twitter e Instagram- son potenciales víctimas de vulneración a su identidad, ya que al consignar datos íntimos en su perfil (nombre, gustos, ubicación, intereses, etc.) facilitan la duplicidad de este que podría facilitar la actividad delincuencial a nivel cibernético.

Zelada (2018) en su tesis estableció como objetivo determinar si ante el robo de identidad se vulnera la seguridad jurídica de la persona. La metodología que se aplicó fue el enfoque cualitativo, de tipo analítico y deductivo. Se determinó como resultado que el gobierno tiene el deber de resguardar tanto la identidad legal como la biológica con el propósito de brindar a todo ciudadano un componente que lo diferencie del resto de habitantes. Concluyó que el robo de identidad se da cuando se arrebata información personal a través de la red para ejecutar un fraude o delinquir, vulnerando con ello la seguridad jurídica del usuario.

Aquino (2020) en su trabajo de investigación planteó como objetivo comparar las regulaciones jurídicas sobre la prevención del robo de identidad entre México y Argentina. Aplicó una metodología de enfoque cualitativo, tipo documental y método comparativo. Como resultado se determinó que la identidad digital aparece como producto del internet, ya que se almacena en las plataformas digitales datos personales como direcciones, números de tarjetas, claves de acceso a cuentas bancarias, entre otros, los cuales pueden ser extraídos mediante virus (malware o

phishing) con un fin delictivo. Concluyó que el robo de identidad se da cuando un individuo transfiere, obtiene o posee sin autorización datos íntimos como números de licencia, números de tarjetas de crédito, nombres de usuario y contraseña que favorece al ciberdelincuente cometer un acto delictivo.

Tobón (2020) en su tesis estableció como propósito plantear estrategias de ciberseguridad que protejan a los usuarios y los datos que los identifican como seres humanos. Utilizó una metodología de enfoque cualitativo, de tipo básico y análisis documental. Se obtuvo como resultado que el modelo de Blockchain coadyuva a la protección de datos contenidos en cualquier plataforma digital. Concluyó que la protección de la identidad digital es un reto en constante evolución; pues, los delincuentes cada vez más perfeccionan sus técnicas de robo de información haciendo difícil la identificación de estos.

Utreras (2021) en su trabajo planteó como objetivo evaluar las vulnerabilidades de los servicios web que enmarcan la protección de la identidad digital. Se aplicó el enfoque mixto (cualitativa-cuantitativa) y de tipo no experimental. Dio como resultado que la identidad digital tiene que ver con los rastros en la red a través de fotos, comentarios, búsquedas, información personal que se sube a las páginas web y aplicaciones. Concluyó que se entiende por inseguridad al posible riesgo que atraviesa el usuario con toda la información personal que se plasma en internet debido a que puede ser utilizada por terceros de manera malintencionada para cometer actos delictivos y/o causar algún perjuicio.

A nivel nacional, Rimaicuna (2021) en su tesis planteó como fin describir como agravante el resultado pernicioso del deepfake, respecto del crimen contenido en la Ley N.° 30096 - usurpación de la identidad (artículo 9). La metodología fue de enfoque mixto, de tipo básica y diseño no experimental; aplicando la encuesta a una población de 50 profesionales del derecho, especializados en Derecho Penal. Los resultados obtenidos indicaron que, si los sujetos representados en los deepfake no se encuentran conformes con la imagen publicada en la red, es merecedor de sanción penal. Concluyo que, el empleo de fotos, videos o audios que simulan o

aparentan la imagen de un sujeto (tecnología deepfake) transgrede la seguridad de los usuarios en la red; ya que motiva los ataques textuales y mentales contra la persona.

Flores y Uriarte (2023) en su trabajo de investigación plantearon como objetivo delimitar cual es el grado de incidencia de la tecnología en la proliferación del crimen informático, específicamente el delito de suplantación de identidad. En la metodología aplicaron un enfoque cualitativo, de tipo básico y revisión documental. Los resultados indicaron que, el Estado tiene el deber de ofrecer a la población un documento legal que los logre identificar y diferenciar unos con otros (identidad única). Concluyo que, las TIC's proporcionan a los ciberdelincuentes, los medios (redes sociales e internet) para cometer el delito de suplantación de identidad; tales acciones son ejecutadas sin restricción alguna, por ejemplo, mediante el "malware".

Aldecoa (2020) en su tesis planteó como propósito fijar en qué medida los medios informáticos benefician el cometimiento de la sustitución de la identidad. Se utilizó una metodología de enfoque cualitativo, diseño de teoría fundamentada, y como técnicas la observación y exploración bibliográfica. Los resultados indicaron que, la suplantación de identidad se encuentra dentro de los delitos informáticos; ya que este se vale del uso del internet para generar daños a los derechos fundamentales (dignidad, honor e imagen) y patrimoniales. Concluyó que la identidad es una particularidad propia del ser humano en la cual contiene aspectos como el nombre, domicilio, nacionalidad y filiación, lo cuales permiten a la persona ser sujeto de derecho, pero al ser infringidas a través de medios tecnológicos podrían constituir un peligro en el desarrollo privada y público del sujeto.

Sosa (2022) en su trabajo de investigación planteó como objetivo analizar la actual tipificación del phishing en la legislación peruana, usó una metodología de enfoque cualitativo, de tipo básica, nivel descriptivo, diseño documental a través de la técnica de recolección y análisis de datos. Dio como resultado que hoy en día obtener información de las personas mediante la plataforma virtual de los Entes Públicos como RENIEC, Poder Judicial, ESSALUD, SUNAT, SUNARP y otros, facilita

a los delincuentes obtener el N.° RUC, N.° DNI o C4 y otros y efectuar la suplantación de identidad. Concluyó que el RENIEC y demás órganos estatales deben establecer mejores sistemas de ciberseguridad que con eficacia permitan la protección y la no vulneración del derecho a la identidad por parte de terceros inescrupulosos.

Quispe y Quispe (2023) en su tesis plantearon como intención señalar si la Ley N°30096 es ineficaz frente al delito de suplantación de identidad a través de las redes sociales. Utilizó una metodología de enfoque cualitativo, diseño exploratorio y revisión documental nacional e internacional. La población y muestra estuvo conformada por diez abogados y revisión sistemática de la literatura. Se obtuvo como resultado que los datos personales virtuales (clave de acceso al celular, clave de acceso al Gmail o Facebook, pin de acceso a tarjetas crédito, entre otros), son el bien jurídico protegido en el marco del derecho a la identidad. Concluyó que el phishing es una técnica de suplantación de identidad que busca como propósito burlar a los usuarios empleando métodos para que la víctima brinde información y a partir de ello cometer actos delictivos.

En cuanto a la primera categoría, proliferación de la ciberdelincuencia: se puede indicar que, la sociedad actual demócrata emplea los sistemas informáticos, las redes y, en particular el internet en el día a día; es decir, introducen cada vez más el terreno íntimo de su vida personal en el mundo virtual (Focas,2018). Ello ha traído como consecuencia la configuración del cibercrimen a gran escala; pues, los delincuentes tienen acceso libre a información (datos, videos, fotos, audios, ubicación, etc.) y pueden valerse de ello para poner en peligro o lesionar los bienes jurídicos protegidos por la normativa penal (Lopez,2022).

En ese sentido, el mal o incorrecto uso de los medios electrónicos, aplicaciones telefónicas, transacciones bancarias por la red, entre otras; han provocado que personas u organizaciones delictivas puedan generar daño personalísimos y económicos a los cibernautas, empresas y gobiernos (Bartolomé y Monteiro,2021).

Respecto a la primera sub categoría, caracterización de la ciberdelincuencia: Los estudios criminológicos han fijado que: a) se lleva a cabo a través de internet, b) comunicación instantánea con la victima (mediante de mensajes de voz o texto, páginas web, o del uso de redes sociales), y c) el medio del delito tiene un bajo costo económico, y de fácil acceso para cualquier persona (Mayer, 2018). Asimismo, son características la flexibilidad de la identidad del delincuente (anonimato disociativo), de desterritorializacion (puede cometerse a nivel nacional e internacional) y uso de inteligencia artificial para burlar la seguridad de la persona y/o institución (ingeniería social), entre otros (Cámara, 2020).

Respecto a la segunda sub categoría, efectividad de la sanción penal: La punición de estas conductas deben desarrollarse dentro del marco del debido proceso, sin dejar de tomar en cuenta los principios inherentes a un estado constitucional de derecho como la proporcionalidad y lesividad para hacer frente, advertir y erradicar esta nueva modalidad de delincuencia (Valdebenito y Sanchez,2018).

Respecto a la tercera sub categoría, legislación peruana: cabe indicar que mediante la creación de la Ley N.º 30096 (22 de octubre de 2013) se ha enmarcado ciertos delitos como parte de los delitos cometidos mediante la red. Así tenemos: en el Artículo 2°, 3°, 4°, 5°, 7°, 8°, 9° y 10° los delitos de acceso ilícito, ataque a la integridad de los datos informáticos, ataque a la integridad de sistemas informáticos, proposiciones a niños, niñas y adolescentes con fines sexuales por medios tecnológicos, interceptación de datos informáticos, fraude informático, suplantación de identidad y el abuso de mecanismos y dispositivos informáticos correspondientemente (Pérez y Saldaña,2020).

En cuanto a convenios internacionales suscritos sobre la lucha contra la ciberdelincuencia, es de precisar que el Perú solicitó en el año 2014 adherirse al Convenio de Budapest; donde el Consejo Europeo en el año 2015 aceptó dicha petición. Luego, el 12 de enero de 2019 el Poder Legislativo mediante la Resolución Legislativa N.° 30913 reafirmó la suscripción al mencionado Convenio; el cual fue

ratificado el 01 de diciembre del 2019 a través del Decreto Supremo N.° 010-2019-re (Vilchez,2020).

Respecto a la cuarta sub categoría, en la tendencia actual: La Ingeniera Social es una técnica utilizada por los ciberdelincuentes para realizar ataques de manera más efectiva y a gran escala. Por ejemplo, los ataques de phishing pueden ser más sofisticados al utilizar técnicas de generación de texto basadas en IA (inteligencia artificial) para crear correos electrónicos que parezcan más auténticos y persuasivos para las víctimas potenciales (Méndez et al., 2018).

Ante ello, no puede haber una sola área policial para combatir el cibercrimen. Se requiere que todas las dependencias policiales cuenten con personal capacitado y equipos de comunicación e informática para detectar y sancionar a los delincuentes que cometan ciberdelitos (Fernández y Vargas,2020).

Sobre la segunda categoría, derecho a la identidad: esta configura la esencia de todo ser humano, engloba las características particulares de un individuo que lo hace único; es decir, permite diferenciar a unos de otros (Bravo, Ramírez y Arenas, 2018). La identidad como derecho fundamental es vital para el desenvolvimiento del ciudadano en la sociedad; donde al ser protegida a nivel constitucional, es oponible -carácter erga omnes-, no posibilitando la derogación ni suspensión de este derecho (Ruiz,2021). Así, la nacionalidad, el nombre y los otros componentes; son inseparables de la dignidad de la persona, por ello, el Estado está obligado a garantizar la seguridad y desarrollo pleno de los derechos que desemboca (Álvarez, 2021).

La identidad personal abarca atributos estáticos y dinámicos. La identidad estática, es aquella que permanece inamovible a pesar del tiempo, por lo que los datos no pueden ser alterados, tales como: nombre de los padres, lugar de nacimiento, hora de nacimiento, fecha de nacimiento (día, mes y año), entre otros. Por otro lado, la identidad dinámica supone la libertad del individuo de modificar ciertos aspectos que lo identifique satisfactoriamente, tales como: ideologías políticas y la orientación sexual (Diaz,2020). Para Arvelo, Pucar y Parraga (2022) tanto la

identidad dinámica como estática se relaciona en las plataformas virtuales, y son fundamentales para que el individuo pueda desarrollarse libremente y adherirse a servicios digitales tales como: educación digital, comercio electrónico y el desenvolvimiento en las diferentes redes sociales.

Por otro lado, la identidad legal se consigna en los documentos de identidad esenciales para el reconocimiento del ciudadano y sus respectivos derechos. Siendo, el D.N.I, el certificado de nacimiento, acta de matrimonio, etc.; los cuales son generadores de los documentos de identidad funcionales -licencia de conducir, pasaporte y otros. - (Pareja et al., 2017).

Otro punto es la identidad digital, este va más allá del concepto tradicional que se tiene de “identidad”, el cual abarca rasgos físicos, documentarios, o simplemente habilidades. Esta mezcla de información de la personalidad, datos biológicos y los que el usuario va identificando como distintivo de su imagen en la red. Abarca, los datos publicados de las actividades que ejecuta, forma de hablar, manera de vestir, etc. (Martínez y Rincón, 2021). También puede definirse como el símbolo que identifica a un sujeto, resultante de la participación en las plataformas virtuales, a través de perfiles, fotos, comentarios, cuentas en internet, textos, videos, entre otros rasgos que posibiliten sea reconocido (González y Angela,2018).

Respecto a la primera sub categoría, sobre el bien jurídico protegido: Son la vida y la integridad personal en todos los sentidos – sexual, moral, psíquico y físico-. Pues ellos son protectores del derecho a la imagen, al honor, inviolabilidad del secreto de telecomunicaciones, buen nombre y/o reputación (Toledo y Ochoa, 2020).

La imagen tanto pública como privada de un individuo es vital para el normal desarrollo del ser humano en su ámbito familiar, laboral y social (Molina y Ochoa,2020). La perspectiva que tiene un ser humano de sí mismo, sobre sus atributos y rasgos de comportamiento en general deben ser respetados, y difundirse tal cual la persona los consigna (Mitxelena,2020).

Respecto a la segunda sub categoría, delitos que atenta contra la identidad: Al ser la identidad un derecho personalísimo protegido por la Carta Magna; se ve

vulnerado cuando por medio de la red u otro medio se extraen los datos de un sujeto con un propósito netamente doloso (Zárate y Becerra,2021). Siendo que, la normativa penal establece como delito la “suplantación de identidad”. Entendido este como aquella donde el suplantador (sujeto activo) usurpa, reemplaza o releva a un individuo de existencia real (sujeto pasivo) sin su autorización y/o consentimiento. En otras palabras, es la retención o expropiación de particularidades de identificación personal de un tercero sin permiso previo (Quiñonez,2017).

Por otro lado, para Gamón (2017) la suplantación o robo de identidad es la acción de simular una intercomunicación de origen anónimo y/o incógnito como si en realidad fuera una fuente familiar y fidedigna; llevando a error y confusión respecto a las relaciones entabladas con otros usuarios mediante plataformas web, llamadas telefónicas, correos electrónicos o incluso a través de una dirección IP, ARP (Protocolo de resolución de direcciones) o DNS (servidor del Sistema de nombres de dominio) falsificados. Salvaguardar la identidad se relaciona con la honra misma y el ámbito privado del hombre.

Ahora bien, se debe tener en cuenta que existen diversas conductas ilícitas que pueden cometerse a través de un perfil social falso, ya sea por Facebook, Instagram, twitter y/o Tic tock; lo que significa que la suplantación de identidad va más allá de la vulneración a la intimidad (derecho de reservar datos personales del público) e identidad (derecho de disponer del nombre y la imagen de uno mismo), es un delito compuesto toda vez que en su gran mayoría van de la mano con amenazas, difusión de pornografía infantil, delitos contra el honor y otros (Vinelli,2021).

Respecto a la tercera sub categoría, Métodos de protección de la identidad: La identidad puede ser salvaguardada mediante el implemento de métodos biométricos; estos son información interna de un individuo, que no pueden ser modificados por voluntad propia. Esta característica de perpetuidad genera que no puede ser alterada ni con el transcurso del tiempo (Cerda,2019). En otras palabras, son datos únicos

fisiológicos y físicos que diferencia a unos de otros, tales como: ADN, pulso cardiaco, la voz, radiografía dental, geometría de la mano, etcétera (Ataucuri et al.,2022).

Asimismo, generaría una mayor eficacia los métodos biométricos multimodales; es decir, la implementación de distintas técnicas biométricas como el reconocimiento facial y dactilar o el reconocimiento de iris y de palma (Rivera et al.,2022).

De acuerdo con Irshad y Soomro (2018) las precauciones personales para utilizar redes sociales sin poner en riesgo nuestra privacidad e identidad son: a) evitar mostrar detalles de documentos personales o financieros, b) desactivar la función de inicio de sesión automático, c) no publicar la ubicación en tiempo real, d) configurar estrictas medidas de privacidad en los perfiles, e) utilizar contraseñas seguras y únicas, f) implementar autenticación doble mediante códigos de acceso, y g) habilitar alertas para detectar actividad inusual.

Respecto a la cuarta subcategoría, de eficacia normativa penal de protección: En Perú, actualmente la identidad es protegida tanto a nivel constitucional como legal. En efecto, todo individuo posee el derecho a la vida, a su integridad moral, física y psíquica, a su identidad y a su libre desarrollo y bienestar (Const., 1993, art. 2). Asimismo, La ley N.° 30096, en su Artículo 9° dispone que aquel que utilice los medios informáticos con fines perjudiciales -moral o material-, para usurpar la identidad de un individuo o empresa, será merecedor de encarcelamiento en un periodo no menor de tres ni superior a cinco años (Diaz,2020).

El delito de suplantación de identidad se ve configurado si: la persona suplantada es real (viva o fallecida), los delitos tengan como objetivo usurpar la personalidad de otra persona y debe existir la intención de lesionar intereses ajenos y obtener un beneficio (Valdivia,2020). De acuerdo con el sistema de denuncias policiales (SIDPOL), se han registrado en el año 2022, 1300 casos de suplantación de identidad. Sin embargo, pese al incremento de casos comparado a años anteriores, la mayoría de los casos son archivados por falta de profesionales

especializados y el desconocimiento de los fiscales y policías sobre esta materia (Morales, 2022).

III. METODOLOGÍA

Por su enfoque, la presente investigación tiene enfoque cualitativo. Este tipo de investigaciones se centra en estudiar los fenómenos, del por qué y cómo ocurren los mismos. Para alcanzar sus objetivos aplica el análisis de la situación problemática, establece definiciones, percepciones, pensamientos y experiencias. Además, utiliza diversos recursos y técnicas de recolección de datos a través de observaciones, imágenes, entrevista a expertos y revisiones documentales (Loayza, 2020).

Por eso, en este trabajo se presenta el análisis de una realidad latente que afecta a la sociedad como es el caso del incremento de los delitos cibernéticos que afectan al bien jurídico consagrado en la Carta Magna como es el derecho a la identidad. Un delito que se comete de manera constante a través del mal uso de los medios tecnológicos que facilita al delincuente cibernético acceder a los datos personales desde ese conocimiento puede cometer delitos.

3.1. Tipo y diseño de investigación

Es de tipo básica, denominada pura o fundamentada, teórica o dogmática cuyo objetivo es ampliar los conocimientos científicos en un área determinada, sin llevar a la práctica de manera inmediata (Muntané, 2010).

Por ende, el diseño seleccionado para esta investigación es de teoría fundamentada, toda vez que buscar establecer nuevos fundamentos teóricos sobre el problema de investigación a fin de aportar con las posibles alternativas de solución, para lo cual es fundamental el conocimiento de los estudios previos que se obtienen mediante la revisión documental (Páramo, 2015).

3.2. Categorías, Subcategorías y matriz de categorización

En la investigación se planteó (I) la categoría de proliferación de la ciberdelincuencia que es el incremento desmesurado de los delitos cometidos a través de medios informáticos, del internet, afectando tanto a personas naturales

como jurídicas; el accionar del ciberdelincuente es del anonimato que tiene la capacidad de vulnerar la información personal con el fin de cometer un delito.

A partir de esta categoría se desprende la sub categoría (1) de caracterización de la ciberdelincuencia que consiste en comisión de delitos desde el anonimato disociativo, desterritorialización, aplicación de la inteligencia artificial para transgredir la seguridad personal e institucional, todo ello mediante el uso del internet que permite una comunicación instantánea y a costo asequible (Mayer, 2018). La segunda sub categoría es (2) la efectividad de la sanción penal que consiste en establecer los mecanismos de sanción penal mediante la aplicación del debido proceso, bajo los criterios de lesividad y proporcionalidad a fin de prevenir, enfrentar y erradicar este tipo de delitos.

La tercera (3) sub categoría es la legislación peruana ante la ciberdelincuencia. Ante ello se tiene la Ley Nº 30096 que sanciona diversos hechos ilícitos relacionados a la privacidad de los datos informáticos, interceptación de datos, fraude informático, suplantación de identidad, entre otros. La referida ley guarda estrecha relación con los tratados internacionales como el Convenio de Budapest y el Consejo Europeo. En relación a ello se tiene la cuarta sub categoría (4) que es la tendencia actual que evidencia el incremento de este tipo de delitos sobre todo a través del phishing, lo cual implica la creación de mecanismo de defensa de manera permanente.

Además, se tiene la categoría (II) afectación al bien jurídico del derecho a la identidad que un derecho personalismo cuyo elemento sustancial es que permite al ser humano diferenciarse de unos a otros con características muy especiales, que no puede ser derogado ni suspendido de ningún modo (Bravo et al., 2018). De esta categoría se desprende la primera (1) sub categoría del bien jurídico protegido como la vida, la integridad en todas sus expresiones, el derecho a la imagen, honor, inviolabilidad, secreto de comunicaciones (Toledo y Ochoa, 2020).

Además, la segunda (2) sub subcategoría son los delitos que atentan contra el derecho a la identidad. En este tipo de delitos se subraya la suplantación de

identidad, entendido como usurpación de datos personales sin la autorización o consentimiento del sujeto vulnerado, donde no existe el consentimiento o permiso (Quiñonez,2017). Ante ello, como tercera sub categoría (3) existen diferentes métodos de protección como el uso de herramientas biométricas que no pueden ser fácilmente alterados, sirven como el ADN de la información (Ataucuri et al.,2022). Por eso, se tiene la cuarta (4) sub categoría que es la búsqueda de la eficacia normativa penal para proteger el derecho a la identidad, en base a la Ley N.° 30096 que establece sanciones para los delitos cometidos a través de medios informáticos.

3.3. Escenario de estudio

Para fines de la investigación se considera como escenario de estudio los procesos de investigación llevados a cabo en el Distrito Fiscal del Callao. Si bien es cierto que la ciberdelincuencia no se limita a un espacio geográfico, sin embargo, para efectos del análisis y comprensión de la realidad, se circunscribe la problemática a un espacio físico, razón por la cual se ha elegido el Distrito Fiscal referido.

3.4. Participantes

Según la naturaleza y tipo de investigación, la población de estudio será de naturaleza no probabilística, se trata de una población finita, determinada de manera intencional para la aplicación del instrumento de recolección de datos, a fin de recabar la información de campo. Para ello, se selecciona a seis (6) profesionales que ocupan el cargo de fiscales quienes podrán aportar con sus conocimientos a un mayor conocimiento del tema de estudio.

3.5. Técnicas e instrumentos de recolección de datos

La técnica que se aplicará en esta investigación será la entrevista a expertos. Es la técnica apropiada para las investigaciones cualitativas que consiste en entablar un diálogo en base a unas interrogantes previamente elaboradas por el investigador y se formula al entrevistado a fin de recopilar información importante respecto al tema de investigación (Fernández, 2018); para ello se emplea como instrumento la

guía de entrevista y otras herramientas que pueden ser grabadoras, filmadoras, celulares con cámara, entre otros recursos.

Además, se aplicará la técnica de la revisión bibliográfica con consiste en la recolección de estudios previos de diferentes bases de datos de acceso abierto. Estos estudios pueden ser publicaciones en revistas científicas, libros, tesis, legislaciones, jurisprudencia.

3.6. Procedimiento

El procedimiento está referido esencialmente al modo de recolección de la información. En ese sentido, según el enfoque de la investigación cualitativa, en primer lugar, se aplicó la técnica de revisión bibliográfica para determinar los estudios previos y el estado del arte de la realidad problemática. Para ello se tuvo acceso a diversas revistas científicas, libros, tesis relacionados a los delitos cibernéticos y su afectación al derecho a la identidad personal.

Además se aplicó la técnica de entrevista a expertos, mediante una guía de entrevista debidamente estructurada, las misma que fue validada por expertos en la materia de investigación, con la finalidad de brindar un aporte al conocimiento y planteamiento de alternativas de solución para la solución de la realidad problemática; es decir, sobre el incremento de los delitos cibernéticos en el Perú, especialmente en la jurisdicción del Callao que últimamente se ha convertido en la cuna de la delincuencia cibernética.

3.7. Rigor científico

La presente investigación cumple con los estándares de la investigación científica toda que obedece a una serie de criterios establecidos para el constructor de este tipo de trabajos académicos. Cumple con el criterio de validez y confiabilidad porque se base en la información confiable recabada de los diferentes medios de soporte físico y electrónico (Arias & Giraldo, 2011).

Se cumplió con el criterio de validez por la información recabada, las técnicas y los instrumentos empleados son auténticos, los mismos que contaron con la

validación de expertos en el tema de investigación (Plaza, Uriguen, & Bejarano, 2017). Por ende, los instrumentos validados y aplicados proporcionan como resultado las conclusiones y recomendaciones válidos y confiables (Manterola, et al., 2018), por tener consistencia lógica, credibilidad, auditabilidad y transferibilidad.

3.8. Método de análisis de datos

En primer lugar, como método de análisis de datos se aplicó el método analítico. Es decir, la información recabada previamente, fue analizada con rigor científico, interpretada de acuerdo al contexto de la realidad problemática, según las teorías, categorías y sub categorías establecidas, las mismas que fueron debidamente estructuradas siguiendo una secuencia lógica (Rodríguez, et al., 2005).

En cuanto al análisis de contenido, se aplicó el método inductivo. Es decir, desde el conocimiento de los hechos particulares sobre la ciberdelincuencia en el Perú, particularmente en Callao, se pudo argüir que este tipo de delitos es algo genérico cuya repercusión es en todos los estamentos de la sociedad.

3.9. Aspectos éticos

En la presente investigación se respeta la ética investigativa. Es decir, en cuanto a su constructo se ha formulado en base a los lineamientos establecidos por la Universidad César Vallejo, que aprobó la “Guía de elaboración de trabajos conducentes a grados y títulos” mediante la Resolución N°062-2023-VI-UCV, de fecha 20 de marzo de 2023. Además, esta investigación se realiza teniendo respeto por el derecho de autor, la creación intelectual, evitando cualquier tipo de plagio, copia, apropiación ilícita. En ese sentido, los autores considerados dentro de la investigación están debidamente referenciados según los lineamientos de APA 7ma versión. Por lo que es factible afirmar que guarda con los estándares de calidad exigidos por la institución universitaria y constituye un aporte al conocimiento científico y jurídicos sobre el problema de investigación con sus posibles alternativas de solución.

IV. RESULTADOS Y DISCUSIÓN

En este capítulo del trabajo se desarrolla los resultados y la discusión de la investigación fundamentada en la información recabada por medio de la entrevista a expertos del derecho en el tema de la investigación, los cuales se complementan con los autores nacionales e internacionales indicados en los antecedentes de la investigación. Para ello, se debe indicar que participaron seis (6) fiscales que realizan sus actividades laborales en el Distrito Fiscal del Callao, los cuales son presentados en la siguiente tabla:

Tabla 1

Participantes en la entrevista

ENTREVISTADO 1=E1	Dr. Jesús Daniel Balvin Arbulu. Fiscal Adjunto Provincial, Callao
ENTREVISTADO 2=E2	Dr. José Luis Morales Yataco. Fiscal Adjunto Provincial, Fiscalía Provincial Penal Corporativa del Callao.
ENTREVISTADO 3=E3	Dr. Victor Hugo Montellanos Palomino. Fiscal Adjunto Provincial, Callao.
ENTREVISTADO 4=E4	Dra. Josseline Macbeth Purizaca Zeta. Fiscal Provincial Penal, Callao.
ENTREVISTADO 5=E5	Dra. Lucía de Jesús Huamán Tiza. Fiscal Provincial Penal, Callao
ENTREVISTADO 6=E6	Dra. María Lizbet Benites Cuadros. Fiscal Provincial Penal, Callao.

A continuación, se hace la presentación de los resultados de la entrevista de acuerdo a los objetivos de la investigación:

Objetivo general: Analizar la manera en que la proliferación de la ciberdelincuencia afecta el bien jurídico del derecho a la identidad, Callao 2022

Pregunta 1. Desde su punto de vista, ¿De qué manera la proliferación de la ciberdelincuencia afecta el bien jurídico del derecho a la identidad? Fundamente su respuesta.

Tabla 2

Postura sobre la proliferación de la ciberdelincuencia y su afectación

ENTREVISTADOS	RESPUESTA
ENTREVISTADO 1	El Ámbito digital ha permitido la comunicación por medio del anonimato, la falsedad de información y la carencia de relaciones humanas físicamente. Esto ha servido de nicho para el delincuente, que ve una oportunidad sencilla de poder fraguar identidades falsas como medio o instrumento para cometer sus fines ilícitos
ENTREVISTADO 2	En principio considero que la ciberdelincuencia, como actividad ilícita, afecta una gran variedad de bienes jurídicos protegidos; entre ellos, la afectación al derecho a la identidad, puesto que, entre las diversas formas de materializar los actos delictivos.
ENTREVISTADO 3	Partamos que el bien jurídico protegido en este tipo de delitos se advierte en diversos planos de manera conjunta y enlazada; primero está la información de manera general (información almacenada, tratada y transmitida mediante los sistemas de tratamiento automatizado de datos), y en el segundo plano, los demás bienes afectados como son la indemnidad sexual, intimidad, etc.
ENTREVISTADO 4	Con respecto a la proliferación de los delitos de Ciberdelincuencia, este vendría afectando directamente el derecho a la identidad, toda vez que desde que se hace uso de las tecnologías de la información para hacerse pasar por otra persona o institución, y perjudicarla, sea ésta material o moral, afectando su identidad para hacer uso de la misma y acceder sus cuentas o sistema financiero con la finalidad de afectar su patrimonio.
ENTREVISTADO 5	En la actualidad los datos de una persona, imágenes y demás información que los identifican se encuentran registrados en los medios tecnológicos como el Internet y plataformas digitales; y debido a que la ciberdelincuencia se ejecuta en ese campo, su proliferación implica que los que cometen estos delitos, por lo general, accedan a esta información personal y la empleen para su propio beneficio.
ENTREVISTADO 6	El bien jurídico en los delitos de ciberdelincuencia es la protección a la información, esto es, a la confidencialidad, integridad, disponibilidad de la información y los sistemas informáticos, donde este se encuentre almacenada (entidades bancarias, empresas de telefonía, etc), por ende al vulnerar dicho bien jurídico afecta a la identidad de las personas a quienes le pertenece dicha información.

Según la Tabla 2, todos los entrevistados afirman que las nuevas tecnologías, como el “internet” ha impulsado el crecimiento de la ciberdelincuencia; pues estas benefician a los delincuentes al permitir el anonimato y no consignar ningún tipo de ciberseguridad que evite la extracción de datos y consecuente robo de identidad.

Además, señalan que el ámbito digital ha facilitado la comunicación anónima, la difusión de información falsa y la falta de interacciones humanas físicas, lo cual ha creado un nicho para los delincuentes. Señalan que la ciberdelincuencia afecta una variedad de bienes jurídicos protegidos, incluyendo el derecho a la identidad.

Asimismo, precisan que los delincuentes utilizan herramientas y conocimientos tecnológicos para vulnerar los mecanismos de seguridad y acceder a la esfera privada de las víctimas. El bien jurídico protegido en este tipo de delitos abarca tanto la información en general, almacenada y transmitida a través de sistemas automatizados de datos, como otros bienes afectados, como la indemnidad sexual y la intimidad. De igual forma mencionan los entrevistados que, los delincuentes se hacen pasar por otras personas o instituciones, perjudicándolas material y moralmente, y afectando su identidad para acceder a sus cuentas o sistemas financieros y dañar su patrimonio. Esto puede generar desde simples molestias hasta problemas legales, pérdidas económicas considerables y dañar la reputación o imagen social de la víctima.

La respuesta de los entrevistados coincide con lo manifestado por Rodríguez (2018) quien en su investigación determinó que los usuarios de las distintas redes sociales -Facebook, Twitter e Instagram- son potenciales víctimas de vulneración a su identidad, ya que al consignar datos íntimos en su perfil (nombre, gustos, ubicación, intereses, etc.) facilitan la duplicidad de este que podría facilitar la actividad delincuencial a nivel cibernético. De igual manera, Zelada (2018) que en mayor grado este tipo de delitos se focaliza en el robo de identidad por parte del ciberdelincuente que utiliza dicha información para fines ilícitos. Como refiere Aquino (2020) el internet permite el acceso a datos personales que se almacenan en plataformas digitales y son utilizados por los ciberdelincuentes.

Al respecto, el criterio de la investigadora guarda relación tanto con la respuesta de los entrevistados como con los autores mencionados. Pues, si bien los sistemas de comunicación a través del internet han unificado el mundo global, sin embargo, también es un medio para la comisión de diferentes tipos de delitos

relacionados con el derecho a la identidad, aspecto que se comparte también con Flores y Uriarte (2023), Fernández y Vargas (2020) y Gamón (2017).

Objetivo específico 1: Describir el modo en que la caracterización actual de la ciberdelincuencia repercute en el derecho a la identidad, Callao 2022

Pregunta 2. ¿Conoce el *modus operandi* de los ciberdelincuentes que vulneran el derecho a la identidad mediante el uso de los recursos tecnológicos?

Tabla 3

El uso de las TIC's en el modus operandi de los ciberdelincuentes

ENTREVISTADOS	RESPUESTA
ENTREVISTADO 1	Se pueden realizar diversas actividades delictivas, como la suplantación de identidad, creación de cuentas bancarias o líneas de celulares. Por otro lado, también existen modalidades de manipulación digital, con el uso de software malicioso, para obtener los datos de las tarjetas de crédito, contraseñas y fecha de vencimiento para efectuar consumos no reconocidos.
ENTREVISTADO 2	De acuerdo a la casuística, al igual que lo antes referido, las modalidades también son diversas, pero por lo general, se materializa vulnerando las medidas de seguridad de las personas a través de su acceso a las redes sociales, y así obtener el máximo de información para vulnerar en otros ámbitos relacionados con la intimidad y su patrimonio.
ENTREVISTADO 3	Los ciberdelincuentes se valen de métodos como el phising (captar contraseñas o números de tarjetas de crédito imitando correos electrónicos de organismos u organizaciones oficiales), la monitorización de teclado, el ciberbulling (acoso escolar) o el grooming (ciberacoso sexual a menores) para conseguir sus objetivos.
ENTREVISTADO 4	En la actualidad se vienen desarrollando diversas modalidades para vulnerar el derecho a la identidad, mediante diversos recursos tecnológicos, los cuales permiten ingresar a los datos de las personas y desarrollar el fraude, el más común ahora resulta los correos electrónicos donde les piden ingresar sus datos a fin de acceder a un crédito, es en ese momento donde acceden a toda la información a través del acceso que le brindan los mismos ciudadanos vulnerando su derecho a la identidad al suplantar la misma.
ENTREVISTADO 5	En mi experiencia como fiscal he vistos dos modalidades muy recurrentes; la primera es que suplantan la identidad de una persona para cometer delitos con esta entidad suplantada como estafar a la gente, sea hackeando o clonando su Facebook, o usando información personal obtenida por estos medios para así suplantar la identidad y pedir algún tipo de beneficio económico a sus contactos. La segunda modalidad es que se agencian de datos de esta persona para acceder a sus cuentas bancarias y extraer su dinero.

ENTREVISTADO 6	De los casos que he tenido conocimiento y han sido los más frecuentes son, cuando los delincuentes utilizan el DNI de una persona, que previamente, de manera ingeniosa logran obtenerlo (simulando compras o ventas por internet) y una vez que tiene dicha imagen, lo utilizan para estafar a otras personas (presuntas compras y ventas de productos), ello con el fin de no ser identificados.

De acuerdo con la Tabla 3, existen discrepancias entre los entrevistados, puesto que dos (2) de los entrevistados establecen la suplantación de identidad como el principal modus operandi en la vulneración del derecho de identidad. Por otro lado, dos (2) fiscales señalan el "hackeo" como el actuar más implementado por los delincuentes de la red. Asimismo, en general los entrevistados precisan que las actividades delictivas más ejecutoriadas es la suplantación de identidad, donde los delincuentes se hacen pasar por otras personas para cometer estafas, ya sea hackeando o clonando cuentas de redes sociales como Facebook, o utilizando información personal obtenida de diversas formas para solicitar beneficios económicos a los contactos de la persona suplantada.

Además, mencionan que los métodos utilizados por los ciberdelincuentes, son el phishing, el ciberacoso escolar (cyberbullying) y el ciberacoso sexual a menores (grooming), entre otros. Fijan la diversidad de actividades delictivas relacionadas con la ciberdelincuencia y cómo los delincuentes utilizan diferentes recursos tecnológicos para vulnerar el derecho a la identidad de las personas, ya sea suplantando identidades, obteniendo información personal o accediendo a cuentas bancarias.

La respuesta de los entrevistados guarda relación con lo manifestado por Zelada (2018) quien en su investigación concluyó que el robo de identidad se da cuando se arrebata información personal a través de la red para ejecutar un fraude o delinquir, vulnerando con ello la seguridad jurídica del usuario. De igual forma, Aquino (2020) en su trabajo de investigación manifiesta que el robo de identidad se da cuando un individuo transfiere, obtiene o posee sin autorización datos íntimos como números de licencia, números de tarjetas de crédito, nombres de usuario y contraseña que favorece al ciberdelincuente cometer un acto delictivo. Según Gamón (2017) la suplantación o robo de identidad es la acción de simular una

intercomunicación de origen anónimo y/o incógnito como si en realidad fuera una fuente familiar y fidedigna.

Al respecto, el criterio del investigador es que el modo de operar de los delincuentes es divergente. Coincide con la idea que el robo de identidad es el delito que vulnera el derecho a la intimidad; incluso según Vinelli (2021) este tipo de delitos va más allá de la vulneración a la intimidad (derecho de reservar datos personales del público) e identidad (derecho de disponer del nombre y la imagen de uno mismo), es un delito compuesto toda vez que en su gran mayoría van de la mano con amenazas, difusión de pornografía infantil, delitos contra el honor y otros.

3. ¿Qué responsabilidad tienen los proveedores de servicios en línea y las plataformas digitales en la protección de la identidad personal de sus usuarios?

Tabla 4

Responsabilidad de los proveedores de servicios en línea

ENTREVISTADOS	RESPUESTA
ENTREVISTADO 1	Podría encuadrarse en el delito de acceso ilícito (artículo 2° de la Ley 30096), sin embargo, no es clara la figura, por lo que considero que dicha situación todavía encuentra grandes vacíos de protección y sanción.
ENTREVISTADO 2	Entiendo que esta pregunta está estrechamente relacionada con la protección de datos personales. En la actualidad, sin darnos cuenta, la ciudadanía acepta algunos términos encubiertos (en letras pequeñas) o autoriza que cualquier entidad privada (sea que brinde bienes y servicios) pueda tener acceso a información valiosa de las personas.
ENTREVISTADO 3	Creo que la responsabilidad de estas empresas o proveedores deben ser más severas, llegando hasta sanciones de multas drásticas, ya que éstas son las que prestan el servicio a los usuarios y quienes deberían asumir algún tipo responsabilidad. Se deben de regular con más sus procedimientos, reglamentos y normas de estos proveedores.
ENTREVISTADO 4	En definitiva, los servicios en línea y las plataformas digitales, son responsable al no contar con sistemas de protección de la identidad personal de los usuarios, ya que no implementan mecanismos que sean inquebrantables por los inescrupulosos que acceden de manera ilegal a la información de los usuarios.

ENTREVISTADO 5	Ellos son responsables en establecer mecanismos de seguridad idóneos para prevenir estos delitos, con una política de alerta de detectarse la sospecha de la comisión de estos delitos; ello forma parte de la idoneidad de su servicio.
ENTREVISTADO 6	Hasta la fecha no ha sido posible consignar alguna empresa como responsable y/o tercero civilmente responsable, toda vez que, en los casos de los entidades bancarias, precisan que el usuario para las compras o transferencias han utilizado su clave secreta, la cual no debe ser compartida con terceras personas, y lamentablemente los agraviados han sido sorprendidos y han proporcionado sus datos sensibles.

Según la Tabla 4, la totalidad de los entrevistados toman una posición afirmativa en cuanto a que los proveedores de servicios en línea y las plataformas digitales posee cierto grado de responsabilidad frente a la ejecución de delitos que vulneren la información privada de sus usuarios. Los entrevistados plantean que, las empresas y proveedores de servicios deben asumir una mayor responsabilidad, incluso mediante sanciones de multas drásticas, por lo que se debe regular con mayor detalle sus procedimientos, reglamentos y normas. En consecuencia, los servicios en línea y las plataformas digitales son responsables por no contar con sistemas de protección adecuados para la identidad personal de los usuarios. Se afirma que deben implementar mecanismos de seguridad sólidos e inquebrantables para evitar el acceso ilegal a la información de los usuarios.

Los entrevistados destacan la importancia de establecer políticas de prevención y alerta en caso de detectar actividades sospechosas, tanto para usuarios externos como para los propios empleados de estas empresas, quienes pueden tener un mayor acceso a la información personal de los usuarios. También mencionan la responsabilidad de los propios usuarios en cuanto a la confidencialidad de sus datos sensibles.

Al respecto, Utreras (2021) con su trabajo de investigación coincide con el criterio vertido por los entrevistados en sentido que los titulares de las plataformas de comunicación deben tomar las precauciones para evitar el quebrantamiento del derecho a la intimidad. Se debe evitar el riesgo que atraviesa el usuario con toda la información personal que plasma en internet debido a que puede ser utilizada por

terceros de manera malintencionada para cometer actos delictivos y/o causar algún perjuicio. Este criterio es compartido por Arvelo, Pucar y Parraga (2022) toda vez que el derecho a la identidad tiene un amplio espectro que conlleva a la responsabilidad de educación digital, comercio electrónico y manejo responsable de las redes sociales.

La investigadora comparte el criterio de los entrevistado en sentido que la responsabilidad no solamente recae en los administradores de plataformas digitales, sino también en cada usuario para decidir qué información consigna en los sistemas de internet. Pues, como refiere Sosa (2022) RENIEC y demás órganos estatales deben establecer mejores sistemas de ciberseguridad que con eficacia permitan la protección y la no vulneración del derecho a la identidad por parte de terceros inescrupulosos.

4. ¿Considera que las penas establecidas en el ordenamiento jurídico penal deben incidir en la mitigación de la ciberdelincuencia en el Perú?

Tabla 5

Penas y mitigación de la ciberdelincuencia

ENTREVISTADOS	RESPUESTA
ENTREVISTADO 1	Claro que sí, es un enfoque que ya se ha iniciado hace varios años; sin embargo, la logística y la normativa se ha estancado, mientras que las modalidades delictivas desbordan y se incrementan al mismo tiempo que la tecnología avanza.
ENTREVISTADO 2	Entendiendo el término mitigar como atenuar, considero que la penalización de todo delito siempre buscará atenuar o disminuir aquellos factores que tienen que ver con sus causas. No obstante, deberá tenerse en cuenta, o quizás, no olvidar que el avance tecnológico también permite la aparición de nuevas formas delictivas.
ENTREVISTADO 3	Si, ya que, como todo tipo de penas en el ordenamiento penal, tienen fines como el fin protector de bienes jurídicos; preventivo, es decir, la prevención general y especial de la norma penal; y, el fin resocializador. Así, considero que las penas en el orden penal deban incidir en atenuar la ciberdelincuencia, por lo que deben hacerse más severas, para cumplir los fines de la pena como se ha referido.
ENTREVISTADO 4	En la actualidad las penas como efecto sancionador no estarían surtiendo el efecto para el cual estaría destinados, ya que por más penas altas que se apliquen no se logra mitigar la comisión de dichos ilícitos, a lo que se concluye que no parte por el tema del quantum de la pena, sino que debe de aplicarse

	mejores mecanismos que eviten la comisión de dichos ilícitos penales, como acciones preventivas.
ENTREVISTADO 5	Por supuesto, recordemos que los fines de la pena no solo se centran en la resocialización del agente, sino también en la prevención general y especial, esto con el fin de mermar la comisión de este tipo de delitos, que dado el incremento del uso de los medios tecnológicos para las relaciones inter personales y comerciales, está aumentando de manera alarmante.
ENTREVISTADO 6	En mi opinión las penas pueden servir para sancionar el comportamiento de los que delinquen en estos tipos de delitos, pero lo que se debe hacer es concientizar a la población sobre el uso debido de los sitios web donde ofrecen productos o donde ofrecen ellos productos, debiendo usar páginas confiables; del cuidado y reserva de sus claves que les otorgan las entidades financieras.

De acuerdo a la Tabla 5, cuatro (4) de los entrevistados manifiestan que el incremento de la sanción punitiva en los delitos informáticos, ha repercutido en la disminución de la ciberdelincuencia. Dos (2) de los entrevistados expresan que dichas sanciones son insuficientes, debiendo el Estado enfocarse en políticas públicas preventivas. Los entrevistados argumentan que, a pesar de los esfuerzos iniciados hace varios años para combatir la ciberdelincuencia, la logística y la normativa no han avanzado al mismo ritmo que las modalidades delictivas, lo que ha llevado a un aumento de los delitos cibernéticos a medida que avanza la tecnología. Mencionan que, las penas en la Ley Penal buscan atenuar las causas de los delitos. Sin embargo, se plantea que el avance tecnológico también permite la aparición de nuevas formas delictivas, lo que sugiere la necesidad de adaptar las penas y las estrategias de prevención.

Plantean que, además de endurecer las penas, es importante concientizar a la población sobre el uso adecuado de sitios web y la protección de sus claves otorgadas por entidades financieras. Se enfatiza que la población también debe contribuir a evitar la comisión de estos delitos y proteger su identidad. En ese sentido, Rimaicuna (2021) refiere que no basta la aplicación de la Ley N.° 30096 para proteger el derecho a la identidad, sino que las entidades correspondientes sobre la protección de datos personales deben implementar mecanismos tecnológicos para contrarrestar los delitos cibernéticos. También como refieren Flores y Uriarte (2023)

si bien es importante el uso de las TIC's, sin embargo, deben establecerse mecanismos de protección.

Al respecto la investigadora coincide con la respuesta mayoritaria de los entrevistados en sentido que la sanción penal no resulta suficiente para mitigar la ciberdelincuencia. Es una labor que implica la realización de prácticas preventivas, de la toma de conciencia del ciudadano de proteger sus datos, aunque también es verdad que el internet y el desarrollo de los sistemas de comunicación hacen que cada día aparezcan nuevas modalidades de delito cibernético.

Objetivo específico 2: Analizar la forma en que los fines de la pena ante la ciberdelincuencia incide en la mitigación de la misma.

5. Subraya los desafíos legales y éticos asociados con la recopilación y uso de información personal en el contexto de la ciberdelincuencia.

Tabla 6

Aspectos legales y éticos de la información personal

ENTREVISTADOS	RESPUESTA
ENTREVISTADO 1	Desde la perspectiva jurídica, establecer responsabilidades es muy complicado, cuando hablamos de ciberdelincuencia, pues los autores podrían encontrarse en cualquier parte del mundo. En el ámbito ético, tratar de maximizar el control de datos y comunicaciones en internet puede atentar contra a la intimidad de los usuarios, es difícil establecer o comprender los límites de un lado y el otro.
ENTREVISTADO 2	Definitivamente, considero que el tema axiológico es la base fundamental en toda actividad humana, precisamente la aplicación de los valores en nuestra formación como sociedad permite que aún se mantenga cierto orden y bienestar.
ENTREVISTADO 3	Considero que las penas deben ser más severas para cumplir con los fines de la pena, como el de prevención (especial y general), protectora (de bienes jurídicos) y resocializadora, a fin de que el reo pueda volver a la vida en sociedad. Ello debe ir de la mano con los fines de la pena.
ENTREVISTADO 4	Existen varios desafíos siendo los más resaltantes la normatividad aplicable, reforzar los mecanismos de seguridad frente a la ciberdelincuencia.

ENTREVISTADO 5	Toda vez que, la ciberdelincuencia vulnera la identidad que a su vez está vinculado con la intimidad, el principal desafío radica en establecer a los operadores de justicia medios idóneos que no impliquen una invasión arbitraria a la intimidad; pero que den mayor celeridad y flexibilidad en la obtención de la información que el caso necesita.
ENTREVISTADO 6	Las penas deben ser más severas para cumplir con los fines de la pena en el orden penal.

Según la Tabla 6, tres (3) de los fiscales establecen que la ética es un valor fundamental que pone un límite a la extracción, uso y divulgación de información íntima que configurar la identidad de una persona; y por otro lado la ley resguarda la intimidad como un bien jurídico protegido. Los entrevistados destacan la existencia de la complejidad para establecer responsabilidades en casos de ciberdelincuencia debido a que los autores pueden encontrarse en cualquier parte del mundo. Ello determina a la vez dificultades desde la perspectiva jurídica para perseguir y sancionar a los delincuentes.

Mencionan que el control excesivo de datos y comunicaciones en internet en aras de maximizar la seguridad puede atentar contra la intimidad de los usuarios. Se plantea la dificultad de establecer y comprender los límites entre la protección y la invasión de la privacidad. Los entrevistados argumentan que los valores éticos son fundamentales en todas las actividades humanas y en la formación de una sociedad ordenada y próspera. Sin embargo, se observa una creciente desviación de estos parámetros éticos por parte de instituciones públicas y privadas, lo cual requiere una revisión de sus protocolos y objetivos en el uso de la información.

Al respecto, lo manifestado por los entrevistados es compartido por la investigadora, toda vez que para el campo jurídico es un desafío permanente la lucha contra este tipo de delincuencia que es oculta. Como refiere Tobón (2020) en su trabajo de investigación, la protección de la identidad digital es un reto en constante evolución; pues, los delincuentes cada vez más perfeccionan sus técnicas de robo de información haciendo difícil la identificación de estos. Es importante considerar que los aspectos tienen poca tienen poca trascendencia en la práctica, toda vez que el delincuente cibernético tiene la conciencia laxa con respecto a estos criterios. Como

refiere Aldecoa (2020), es responsabilidad de cada uno de proteger sus datos personales a fin de evitar la exposición ante la delincuencia cibernética.

6. ¿Conoce las medidas legales y tecnológicas que existen en el Perú para prevenir y combatir la ciberdelincuencia que afecta la identidad personal?

Tabla 7

Instrumentos legales y tecnológicos para combatir la ciberdelincuencia

ENTREVISTADOS	RESPUESTA
ENTREVISTADO 1	Sí, conozco la Ley 30096 - ley de delitos informáticos. Además, el Decreto Legislativo Nº 1412-2018 como parte de las políticas públicas del Estado.
ENTREVISTADO 2	Sí, existen muchas medidas legales que los diversos órganos estatales aplican para prevenir y combatir modalidad delictiva.
ENTREVISTADO 3	En el Perú ha habido esfuerzos interesantes respecto a su marco normativo en materia de tratamiento y el combate de la ciberdelincuencia, los que se han venido plasmando siguiendo las pautas que se desprenden del Convenio de Budapest.
ENTREVISTADO 4	Si, en la actualidad ya que se vienen implementando diferentes medidas legales y tecnológicas para prevenir y combatir la ciberdelincuencia, con la finalidad de proteger la identidad personal, pero no están siendo suficientes para poder evitar su vulneración.
ENTREVISTADO 5	Tengo entendido que las empresas que manejan esta información deben establecer adecuadas políticas de protección, bajo responsabilidad, por ende, las páginas de Internet deben contar con programas que no permitan o que bloqueen el acceso de personas no autorizadas.
ENTREVISTADO 6	El atentado a la integridad de los datos informáticos está en la Ley N.° 30096 (artículo 3º)

Según la Tabla 7, dos (2) de los entrevistados señalan a la Ley N.° 30096 como la principal fuente que contrarresta la ciberdelincuencia y protege el derecho de identidad. Destacan que, el Perú ha tomado conciencia de las desventajas que implica el mal uso de las Tecnologías de la Información y Comunicación (TIC).

En respuesta a esta situación, se han realizado esfuerzos para establecer un marco normativo que siga las pautas del Convenio de Budapest, aprobado por el Congreso de la República en febrero de 2019.

Mencionan que el país está adecuando gradualmente su legislación en línea con los estándares internacionales para prevenir, investigar y sancionar los actos ilícitos relacionados con la ciberdelincuencia. Plantean la importancia de que las empresas que manejan información implementen políticas de protección adecuadas y sean responsables en su manejo. Asimismo, se sugiere que las páginas de Internet deben contar con programas que impidan o bloqueen el acceso de personas no autorizadas.

En relación a lo manifestado, Sosa (2022) en su trabajo de investigación la actual tipificación del Phishing en la legislación peruana (Ley N°30096) y en la actualidad obtener información de las personas mediante la plataforma virtual de los Entes Públicos como RENIEC, Poder Judicial, ESSALUD, SUNAT, SUNARP y otros, facilita a los delincuentes obtener el N.° RUC, N.° DNI o C4 y otros y efectuar la suplantación de identidad. Ante esta realidad RENIEC y demás órganos estatales deben establecer mejores sistemas de ciberseguridad que con eficacia permitan la protección y la no vulneración del derecho a la identidad por parte de terceros inescrupulosos.

Al respecto, el criterio de la investigadora es similar a la respuesta de los entrevistados en sentido que el Perú, en cuanto a la implementación de los mecanismos legales y tecnológicos para la protección de datos está en una etapa incipiente. Como refiere Quispe y Quispe (2023) la Ley N°30096 no es plenamente eficaz para proteger los datos personales, toda vez que los delincuentes cibernéticos utilizan recursos tecnológicos muy sofisticados para poner en práctica sus actividades ilícitas.

7. ¿Cuál es la importancia del papel de las autoridades y organismos nacionales e internacionales en la lucha contra la ciberdelincuencia que afecta la identidad personal?

Tabla 8

Organismos Nacionales e internacionales en la lucha contra la ciberdelincuencia

ENTREVISTADOS	RESPUESTA
ENTREVISTADO 1	El papel de los tratados y convenios internaciones han sido la base de la lucha contra la ciberdelincuencia, son el cimiento que dio paso a la legislación nacional, como lo son el Convenio de Budapest y los protocolos adicionales. Ya en Perú, se ha ido legislando sobre los delitos informáticos y políticas de estado para desarrollar, fomentar y proteger el uso de la tecnología, la identidad y el gobierno digital.
ENTREVISTADO 2	Estas entidades tienen una gran responsabilidad en cuanto a la prevención y lucha contra la ciberdelincuencia, ya que éstas son las que fijan y establecen estrategias destinadas a poner en marcha los planes de acción para estos fines.
ENTREVISTADO 3	Considero que el papel y rol que tiene las autoridades y organismos ya sea nacional o internacional, es preponderante; en efecto, están las autoridades gubernamentales que deben regular en estricto las acciones que deben tener los proveedores de servicios en línea o internet, dando protocolos y reglamentos más específicos para priorizar y evitar la vulneración de datos y no afectar la identidad de las personas.
ENTREVISTADO 4	El papel que representa las autoridades y los organismos internacionales resulta ser fundamental ya que permite realizar diversos convenios que contribuyan al acceso de avances tecnológicos que permitan minimizar los riesgos en cuanto a los delitos que se cometen el en ciberespacio.
ENTREVISTADO 5	Ellos son los que deben establecer políticas de prevención para evitar a comisión de estos delitos, así como mecanismos flexibles e idóneos para los operadores de justicia con el fin de lograr una eficiente investigación una vez cometido y denunciado este delito.
ENTREVISTADO 6	En mi opinión el papel y rol que tiene las autoridades y organismos ya sea nacional o internacional, es preponderante; en efecto, están las autoridades gubernamentales que deben regular en estricto las acciones que deben tener los proveedores de servicios en línea.

Según la Tabla 8, todos los entrevistados afirman que tanto las autoridades nacionales como internacionales juegan un papel preponderante frente a la lucha contra la ciberdelincuencia y consecuentemente protegen los datos que identifican a cada individuo de la sociedad. Los entrevistados destacan el papel de los tratados y convenios internacionales en la lucha contra la ciberdelincuencia, mencionando específicamente el Convenio de Budapest y los protocolos adicionales. Estos tratados han sido la base para la legislación nacional en Perú en relación con los

delitos informáticos y las políticas de estado relacionadas con el desarrollo, fomento y protección del uso de la tecnología, la identidad y el gobierno digital.

Mencionan la importancia de las autoridades gubernamentales en la regulación de los proveedores de servicios en línea o internet, mediante la implementación de protocolos y reglamentos más específicos para proteger los datos y la identidad de las personas. Además, los entrevistados destacan el papel de las autoridades de la administración de justicia en la persecución y sanción de los delitos de ciberdelincuencia, incluyendo aquellos que afectan la identidad de las personas, como la suplantación de identidad. Se plantea la necesidad de que estas autoridades cuenten con logística y tecnología adecuadas para identificar a los autores de estos delitos y aplicar sanciones penales ejemplares.

Al respecto, el criterio de la investigadora es coincidente con lo manifestado por Rodríguez (2018) el sistema de regulación y contra ataque a la ciberdelincuencia es una realidad que ha traspasado las fronteras. El Pharming, suplantación de identidad, violación a la intimidad, child grooming, entre otros, es una realidad internacional, razón por la cual los organismos regulatorios deben tomar las medidas preventivas necesarias. Rimaicuna (2021) refiere que el artículo 9° de la Ley N.° 30096 que protege el derecho a la identidad debe ponerse en consideración por los organismos que tienen la responsabilidad de proteger los datos personales. Criterio similar es aplicado por Quispe y Quispe (2023), Pérez y Saldaña,2020 y Diaz (2020).

Objetivo específico 3. Delimitar la manera en que la legislación peruana favorece a la ciberseguridad como antídoto a los delitos cibernéticos.

8. ¿Tiene pleno conocimiento del bien jurídico que protege el derecho a la identidad?

Tabla 9

El bien jurídico protegido

ENTREVISTADOS	RESPUESTA
ENTREVISTADO 1	El derecho a la identidad es el conjunto de atribuciones y características que permiten individualizar a la persona, le permite auto percibirse conscientemente único y distinto a otro y que los demás la reconozcan como tal.
ENTREVISTADO 2	Toda persona tiene derecho a un nombre desde que nace, ello implica su individualización frente al resto de la sociedad y por tanto es deber del Estado garantizar el libre desarrollo de su personalidad. Vulnerar o atentar contra este derecho humano, es afectar este bien jurídico protegido.
ENTREVISTADO 3	Si, en estos tipos de delitos, al usar el sujeto activo, las tecnologías de la información, logran acceder y vulnerar la identidad de terceras personas, para luego obtener provecho que en general es patrimonial, los delincuentes informáticos realizan estos delitos, afectando la identidad de las personas, a efectos de cometer fraudes financieros como compras en línea, transferencias bancarias, etc.
ENTREVISTADO 4	Si, se protege el derecho a la identidad personal (tratamiento de datos), también el patrimonio.
ENTREVISTADO 5	Considero que el derecho a la identidad es un bien jurídico por ser un derecho constitucional que permite individualizar a la persona de los demás miembros de la sociedad.
ENTREVISTADO 6	El bien jurídico protegido serían sus datos personales.

De acuerdo a la Tabla 9, Dos (2) de los entrevistados establecen que el bien jurídico protegido es la protección de datos personales. En general los entrevistados señalan el derecho a la identidad como el conjunto de atribuciones y características que permiten distinguir a una persona de otras y ser reconocida como única. Se menciona que toda persona tiene derecho a un nombre desde su nacimiento, lo cual implica su individualización y el libre desarrollo de su personalidad, siendo responsabilidad del Estado garantizar este derecho humano.

Plantean que, en los delitos informáticos los delincuentes utilizan tecnologías de la información para acceder y vulnerar la identidad de terceras personas, generalmente con el propósito de obtener beneficios económicos, como realizar fraudes financieros, obtener datos ilegalmente, cometer acoso virtual, abuso sexual a menores, entre otros. Los entrevistados precisan que el derecho a la identidad es un bien jurídico protegido, al ser un derecho constitucional que permite distinguir a una persona de los demás miembros de la sociedad, y que su vulneración en el ámbito

de los delitos informáticos puede tener consecuencias tanto en la esfera personal como en la esfera patrimonial de las personas.

Al respecto, el criterio de la investigadora va en consonancia con lo manifestado por los entrevistados en sentido que el bien jurídico protegido efectivamente es el derecho a la identidad personal, un derecho constitucional. Aunque como refiere Rodríguez (2018) tiene connotaciones más prácticas; es decir, se considera aspectos como el nombre, gustos, ubicación, intereses, etc.) facilitan la duplicidad de este que podría facilitar la actividad delincuencial a nivel cibernético. Diversos son los autores que reafirman esta postura, tales como Zelada(2018), Aquino (2020), Tobón (2020) para quienes el bien jurídico es la identidad que es pasible de vulneración a través del mal uso de los sistemas de comunicación e información.

9. ¿Conoce las políticas y legislaciones existentes que protegen el derecho a la identidad personal y cómo se aplican en el Perú?

Tabla 10

Identidad personal y su protección en la normativa nacional

ENTREVISTADOS	RESPUESTA
ENTREVISTADO 1	El Estado peruano ha lanzado diversos mecanismos para digitalizar las instituciones y fomentar el uso de los medios digitales, a través de lo que se denomina la gobernanza de datos o gobierno digital, lo que se evidencia en el Decreto Legislativo Nº 1412-2018
ENTREVISTADO 2	El marco normativo sobre la materia es muy extenso, entre ellas nuestra carta fundamental, la que además se protege a través de las garantías constitucionales, como el hábeas corpus, y otras vinculadas con el ordenamiento jurídico internacional.
ENTREVISTADO 3	En la Ley Nº 30096 rige los delitos asociados a la manipulación indebida de los softwares y hardwares, como base de datos, en perjuicio de los titulares de datos o de terceros.
ENTREVISTADO 4	Se tiene que, en el año 2011, se publicó la Ley N°29733 y en el 2013 la Ley Nº 30096, Ley de Delitos Informáticos, instrumento normativo que describe las conductas delictivas que afectan los sistemas y datos informáticos. En el 2014, esta ley fue complementada con su modificatoria, efectuada por medio de la Ley N° 30171.
ENTREVISTADO 5	La Constitución de 1993 reconoce el derecho a la identidad como un derecho fundamental, se han regulado leyes relacionadas a la identidad de una persona, como su registro en RENIEC y se ha

	emitido la Ley de Protección de Datos Personales justamente destinada a proteger los datos que identifican a una persona y que navegan por Internet.
ENTREVISTADO 6	Existe la Ley 30096 que tiene por objeto prevenir y sancionar las conductas ilícitas que afectan los sistemas y datos informáticos. Los ciberdelitos contra los datos y los sistemas informáticos comprenden el acceso ilícito, los atentados a la integridad de los datos informáticos y de los sistemas informáticos, y el abuso de mecanismos y dispositivos informáticos.

Según la Tabla 10, dos (2) de los entrevistados reconocen a la constitución como la principal fuente de protección del derecho a la identidad. Por otro lado, tres (3) de los fiscales señalan a la Ley N.° 30096 como la política criminal más relevante contra la ciberdelincuencia; y consecuentemente quien protege el derecho fundamental de identidad.

Los entrevistados mencionan que el Estado peruano ha implementado mecanismos para digitalizar las instituciones y promover el uso de medios digitales, lo cual se refleja en el concepto de gobernanza de datos o gobierno digital. Se hace referencia al Decreto Legislativo Nº 1412-2018 como una muestra de estos esfuerzos.

Resaltan que la Constitución de 1993 reconoce el derecho a la identidad como un derecho fundamental, y se han promulgado leyes para regular aspectos relacionados con la identidad, como el registro en el RENIEC (Registro Nacional de Identificación y Estado Civil) y la Ley de Protección de Datos Personales, que busca proteger los datos que identifican a una persona y que circulan por Internet.

La investigadora coincide con la respuesta de los entrevistados en sentido que la ciberdelincuencia puede comprometer la privacidad y seguridad de los datos personales, lo cual puede afectar el derecho a la identidad, así como otros derechos básicos como la salud y la educación. Por eso, tal como refiere Pérez y Saldaña (2020) es importante poner en práctica lo establecido en los Artículo 2°, 3°, 4°, 5°, 7°, 8°, 9° y 10° los delitos de acceso ilícito, a fin de evitar el ataque a la integridad de los datos informáticos, ataque a la integridad de sistemas informáticos, proposiciones a

niños, niñas y adolescentes con fines sexuales por medios tecnológicos, interceptación de datos informáticos, fraude informático, suplantación de identidad y el abuso de mecanismos y dispositivos informáticos.

10. ¿Cuáles son los principales derechos asociados al derecho a la identidad personal y cómo se ven vulnerados por la ciberdelincuencia?

Tabla 11

Derechos vinculados a la identidad personal

ENTREVISTADOS	RESPUESTA
ENTREVISTADO 1	El derecho a la identidad, está relacionado con la propia autodeterminación de la persona y, por lo tanto, vinculación directa con la dignidad humana
ENTREVISTADO 2	Por ejemplo a la intimidad, a la inviolabilidad de sus comunicaciones y documentos privados que, como ya se ha mencionado, estos derechos son vulnerados mediante el uso indebido de la información personal, con diversos fines de naturaleza delictiva.
ENTREVISTADO 3	Por ejemplo a la intimidad, a la inviolabilidad de sus comunicaciones y documentos privados que, como ya se ha mencionado, estos derechos son vulnerados mediante el uso indebido de la información personal, con diversos fines de naturaleza delictiva.
ENTREVISTADO 4	Uno de los principales derechos es el de la intimidad, por cuanto implica la facultad que tiene una persona de reservar para sí y excluir del conocimiento público de terceros, ciertos aspectos personales que a su criterio no deben ser revelados.
ENTREVISTADO 5	En mi opinión son el derecho a la intimidad, toda vez que los datos personales que identifican a los individuos forman parte de un privacidad e intimidad, la que es vulnerada cuando se accede a esta información sin autorización de su titular. También el derecho al patrimonio, pues por lo general a través de la ciberdelincuencia se perpetran sustracciones o estafas que afectan el patrimonio de las personas.
ENTREVISTADO 6	Los derechos asociados al derecho a la identidad, son el derecho a su nombre, nacionalidad, y con ello sus derechos básicos a la salud, educación.

Según la Tabla 11, Cuatro de los fiscales están de acuerdo que el principal derecho asociado con la vulneración de la identidad personal es la intimidad. Los entrevistados alegan que el derecho a la identidad está estrechamente relacionado con la autodeterminación de la persona y, por lo tanto, tiene una vinculación directa con la dignidad humana. Se menciona que este derecho se relaciona con otros derechos, como el derecho a la intimidad y la inviolabilidad de las comunicaciones y documentos privados.

Destacan que estos derechos son vulnerados cuando se hace un mal uso de la información personal con fines delictivos. La ciberdelincuencia puede comprometer la intimidad y la privacidad de las personas, ya que se accede a su información sin autorización, lo cual afecta su derecho a mantener ciertos aspectos personales en secreto. Los principales derechos asociados al derecho a la identidad son el derecho a la intimidad y el derecho al patrimonio. El derecho a la intimidad implica la facultad de reservar ciertos aspectos personales y excluir su conocimiento público, y se ve vulnerado cuando se accede indebidamente a la información personal. El derecho al patrimonio se ve afectado en casos de ciberdelincuencia que involucran sustracciones o estafas que impactan el patrimonio de las personas.

La investigadora coincide con la respuesta de la mayoría de los entrevistados en sentido que los derechos conexos vulnerados son la dignidad humana, la intimidad, los derechos patrimoniales, entre otros. Al respecto, Aldecoa (2020) en su trabajo de investigación determinó que el delito cibernético que se comete mediante el internet afecta una serie de derechos. Los resultados indicaron que, la suplantación de identidad se encuentra dentro de los delitos informáticos; ya que este se vale del uso del internet para generar daños a los derechos fundamentales (dignidad, honor e imagen) y patrimoniales. Además, comprende el nombre, domicilio, nacionalidad y filiación, lo cuales permiten a la persona ser sujeto de derecho, pero al ser infringidas a través de medios tecnológicos podrían constituir un peligro en el desarrollo privada y público del sujeto. Aspecto que también es considerado por Álvarez (2021), Dia (2020), Molina y Ochoa,2020, entre otros.

11. ¿Conoce las políticas y legislaciones existentes que protegen el derecho a la identidad personal ante la vulneración por medios cibernéticos?

Tabla 12. *La ley y el derecho de identidad*

ENTREVISTADOS	RESPUESTA
ENTREVISTADO 1	Se puede entender, que se encarga la Ley 30096 - ley de delitos informáticos. También se han creado Unidades de especialización tanto a nivel judicial, fiscal y policial para investigar estos tipos de delitos.
ENTREVISTADO 2	Dentro de la política criminal que adopta el Estado para combatir éste y otros tipos de delito, la que va de la mano con nuestra legislación penal y de protección de la información, reafirmo cierto conocimiento sobre la materia, mencionado que, como otras conductas delictivas, se van modificando según el avance tecnológico y las diversas formas delictivas que van apareciendo en la sociedad.
ENTREVISTADO 3	Marco Internacional tenemos: El Convenio sobre la Ciberdelincuencia del Consejo de Europa, los Protocolos adicionales al Convenio sobre Ciberdelincuencia de Europa, la Negociación de una convención internacional. Marco normativo Nacional: La respuesta penal inicial, la Ley de Delitos Informáticos, etc.
ENTREVISTADO 4	La Ley N°29733, Ley Nº 30096, instrumento normativo que describe las conductas delictivas que afectan los sistemas y datos informáticos, así como también las protecciones a las libertades civiles en el ámbito de las comunicaciones.
ENTREVISTADO 5	La Constitución Política del Estado y la Ley de Protección de Datos Personales que fue publicada en el Diario Oficial El Peruano el 3 de julio de 2011
ENTREVISTADO 6	En el Perú se tiene la norma legal 30096, que regula todos los delitos de ciberdelincuencia que se presentan en la sociedad.

Según la Tabla 12, Dos de los fiscales están de acuerdo que la ley N.° 29733, brinda protección al derecho de identidad. Por otro lado, tres de los fiscales señalan a la Ley N.° 30096 como sancionadora de la ciberdelincuencia en temas vinculadas con la vulneración del derecho de identidad. De forma general los entrevistados señalan que la política criminal adoptada por el Estado para enfrentar estos delitos está en consonancia con la legislación penal y de protección de la información. Se reconoce que las conductas delictivas en el ámbito de la ciberdelincuencia

evolucionan y se adaptan a medida que avanza la tecnología y surgen nuevas formas delictivas en la sociedad.

Respecto al marco normativo, los entrevistados mencionan diferentes instrumentos a nivel internacional, como el Convenio sobre la Ciberdelincuencia del Consejo de Europa y los Protocolos adicionales a este convenio, así como la negociación de una convención internacional. A nivel nacional, se hace referencia a la Ley de Protección de Datos Personales (N° 29733), la Ley de Delitos Informáticos (N° 30096) y su modificatoria (Ley N° 30171). En resumen, enfatizan la existencia de la Ley de Delitos Informáticos y otras normativas relacionadas, así como la implementación de unidades especializadas y el compromiso del Estado en la lucha contra la ciberdelincuencia en el país.

12. ¿Cuáles son los derechos y responsabilidades de los individuos en la protección de su propia identidad personal frente a la ciberdelincuencia?

Tabla 13

Identidad personal y los derechos emergentes

ENTREVISTADOS	RESPUESTA
ENTREVISTADO 1	Toda persona debe tener el derecho a que la información que proporciona en el mundo digital no deba ser manipulada ni usada para fines diferentes a su propósito. En la otra arista, se tiene el deber de proporcionar los datos verdaderos cuando así corresponda con la exigencia de la información solicitada, en un contexto determinado, siendo que la vulneración de ello genere una responsabilidad administrativa o penal, según sea el caso.
ENTREVISTADO 2	Resalto que toda persona tiene gran responsabilidad en el manejo y exposición de su propia información. Mi recomendación va para el gran sector de la ciudadanía que opta por exponer de manera innecesaria aquellos ámbitos personales y familiares de su vida cotidiana, información valiosa que la delincuencia común y organizada sabe aprovechar.
ENTREVISTADO 3	En cuando a una responsabilidad debemos tener en cuenta que, en el derecho penal, en cuanto al individuo (sujeto pasivo) cabe en algunas oportunidades la imputación a la víctima, cuando no toma precauciones que hacen consumar el delito en su agravio.
ENTREVISTADO 4	Cada individuo tiene derechos y responsabilidades frente a la protección de los datos de su propia identidad frente a los delitos de ciberdelincuencia, los cuales se encuentran protegidos por la normatividad vigente, y así también tiene la responsabilidad de no

	compartir su información y ser responsable con el uso de la misma a fin de evitar sea vulnerada.
ENTREVISTADO 5	Nosotros como usuarios de los medios tecnológicos, debemos comportarnos dentro del marco del consumidor razonable, y protector de nuestros propios intereses, esto es, verificar dentro de nuestras posibilidades que las plataformas a las que accedemos sean confiables, incluso, estar atento a las modalidades de ciberdelincuencia recurrentes, que son publicada de manera constante por la Policía Nacional.
ENTREVISTADO 6	El derecho de una persona en la protección de su identidad en este tipo de delitos, es que las entidades bancarias y telefonías sean más recelosos en los accesos o permisos para poder realizar compras o transferencias vía internet.

De acuerdo a la Tabla 13, todos los entrevistados dictaminan que todo individuo tiene la responsabilidad de proteger sus datos personales, evitando la exposición en la red sin los controles de seguridad pertinentes. Los entrevistados enfatizan el derecho que toda persona tiene a que la información que proporciona en el mundo digital no sea manipulada ni utilizada para fines distintos a los previstos. Al mismo tiempo, se destaca la responsabilidad de proporcionar datos verídicos cuando corresponda, ya que la violación de esta responsabilidad puede generar consecuencias administrativas o penales.

Resaltan la importancia de que cada individuo asuma la responsabilidad en el manejo y exposición de su propia información. Se hace hincapié en la recomendación de no exponer innecesariamente aspectos personales y familiares de la vida cotidiana, ya que esta información puede ser aprovechada por la delincuencia común y organizada. Asimismo, se destaca la responsabilidad de los usuarios de comportarse como consumidores razonables y proteger sus propios intereses al verificar la confiabilidad de las plataformas a las que acceden y estar atentos a las modalidades de ciberdelincuencia.

Al respecto, la investigara coincide con el criterio que es responsabilidad de cada usuario del internet proteger sus datos personales. Si bien es cierto que existe la legislación nacional medianamente desarrollada, sin embargo, le hecho verter información en las redes sociales y otras plataformas de comunicación es

responsabilidad particular. En ese sentido, Rodríguez (2018) advierte que se deben tomar las precauciones del caso ante ataques como Pharming, suplantación de identidad, violación a la intimidad, child grooming, entre otros. Además, los usuarios de las distintas redes sociales -Facebook, Twitter e Instagram- deben tener presente que son potenciales víctimas de vulneración a su identidad, ya que al consignar datos íntimos en su perfil (nombre, gustos, ubicación, intereses, etc.) facilitan la duplicidad de este que podría facilitar la actividad delincuencial a nivel cibernético.

13. ¿Cuáles son las estrategias legales y sociales se pueden implementar para prevenir y abordar la vulneración del derecho a la identidad personal?

Tabla 14

Estrategias preventivas

ENTREVISTADOS	RESPUESTA
ENTREVISTADO 1	Legalmente, se debe plantear y reforzar los equipos de lucha contra los delitos de ciberdelincuencia, porque actualmente se encuentra en una situación precaria. Para prevenir, se deben implementar normas de mayor protección de los datos e información de los usuarios en el mundo digital.
ENTREVISTADO 2	Considero que las estrategias legales están dadas, sin embargo, estas no generarán ningún resultado si la ciudadanía no toma conciencia en el manejo o sobreexposición de su propia información.
ENTREVISTADO 3	Aprobar el marco legal que permita exigir responsabilidad a las personas jurídicas en materia de ciberdelitos. Establecer una normativa que posibilite la conservación rápida de datos almacenados por medio de sistemas informáticos, conforme a los alcances del artículo 29° del Convenio sobre Ciberdelincuencia del Consejo de Europa.
ENTREVISTADO 4	El incremento del uso de internet durante los últimos años ha generado un escenario que es aprovechado por la ciberdelincuencia, ocasionando agravio a las personas. Esta situación se agrava por el desconocimiento de algunas personas sobre el manejo y resguardo de los datos personales. Se deben de implementar mayores mecanismos de seguridad, que disminuyan la vulnerabilidad de datos personales.
ENTREVISTADO 5	Considero que debe existir una mayor difusión sobre cómo se comete la ciberdelincuencia y los mecanismos de protección que deben usar los usuarios, sumado a ello, se debe exigir de manera eficiente que las empresas a cargo de estas plataformas establezcan adecuados mecanismos de seguridad en sus plataformas, y de prevención para detectar incluso si dentro de su empresa operan los ciberdelincuentes.

ENTREVISTADO 6	Difundir con mayor frecuencia las alertas a la población sobre el uso de las redes para realizar alguna operación.

Según la Tabla 14, los fiscales determinan a nivel legal la implementación de normas más severas y a nivel social la concientización de la población sobre la importancia de instaurar medidas de seguridad. Los entrevistados en la implementación de normas que brinden mayor protección de los datos e información de los usuarios en el mundo digital como medida de prevención. Además, se destaca la importancia de sensibilizar a la población a través de proyectos educativos sobre el uso responsable de la información y cómo evitar caer en delitos cibernéticos.

Mencionan diversas propuestas y acciones a diferentes entidades como el Congreso de la República, el Ministerio del Interior, el Ministerio de Relaciones Exteriores, el Poder Judicial y el Instituto Nacional de Estadística e Informática. Estas propuestas van desde aprobar marcos legales que permitan exigir responsabilidad a las personas jurídicas en materia de ciberdelitos, establecer normativas para la conservación de datos almacenados por sistemas informáticos, evaluar la implementación de un subsistema de justicia especializado en ciberdelincuencia, hasta elaborar y difundir información estadística sobre este tipo de delitos.

El criterio de la investigadora coincide con lo manifestado por los entrevistados quienes indican que en la implementación de normas que brinden mayor protección de los datos e información de los usuarios en el mundo digital como medida de prevención. Al respecto Aquino (2020) refiere que es fundamental la actividad preventiva para proteger los datos personales; además Tobón (2020), Utreras (2021) Rimaicuna (2021) y Aldecoa (2020) indican que la mejor estrategia es la prevención, además de las actividades formativas que se pueden hacer sobre el uso responsable del internet.

V. CONCLUSIONES

Primero: En relación al objetivo general, se determina que el incremento de la ciberdelincuencia afecta sustancialmente al derecho a la identidad. Tanto los estudios como el trabajo de campo, demuestran que el uso inadecuado del internet por parte de los ciberdelincuentes, facilita la vulneración de los bienes jurídicos relacionados con el derecho a la intimidad mediante el phishing, para cometer actos como el ciberbulling, el grooming, pharming, suplantación de identidad, actos que se cometen mediante las plataformas de comunicación como Facebook, twitter, Instagram, donde se pueden encontrar información personal y pueden ser sustraídos por los delincuentes cibernéticos.

Segundo: Con respecto al primer objetivo específico, los autores estudiados y los entrevistados determinan que la ciberdelincuencia presenta características diversas, se lleva a cabo mediante el internet, la existencia de una comunicación en tiempo real con la víctima, el medio del delito tiene un bajo costo económico, y de fácil acceso para cualquier persona, flexibilidad de la identidad del delincuente, desterritorializacion y el uso de la inteligencia artificial para burlas la seguridad personal.

Tercero: En relación al segundo objetivo específico, se determina que las penas establecidas para sancionar los delitos cibernéticos no surten los efectos esperados. Muestra de ello es que cada vez más siguen apareciendo nuevas formas de vulneración del derecho a la identidad personal. Razón por la cual, es necesario aplicar mecanismos de prevención en relación al uso responsable de la información personal, toda vez que no basta únicamente recrudecer la sanción penal, sino implementar mecanismos de seguridad tanto por parte del Estado como la responsabilidad del ciudadano para hacer buen uso de los sistemas de comunicación.

Cuarto: En relación al tercer objetivo específico, la conclusión es que la sola normativa no es suficiente para mitigar la ciberdelincuencia que cada vez más es

tecnificado. La mejor estrategia es la prevención, además de las actividades formativas que se pueden hacer sobre el uso responsable del internet.

VI. RECOMENDACIONES

Primera: Relacionado al objetivo general, se recomienda a las autoridades que tienen la responsabilidad de perseguir el delito, los fiscales que tienen a cargo conocer e investigar los delitos relacionados a la ciberdelincuencia, crear espacios de capacitación permanente no solamente en el ámbito nacional sino también en las esferas internacionales, teniendo en cuenta que cada país cuenta con mecanismos de seguridad a nivel cibernético y en cierta manera puede ser emulado en beneficio del país. Si bien es cierto que la adquisición de equipos tecnológicos implica inversión considerable, sin embargo, la utilidad de la misma podría ser beneficiosa para el país, aspecto que se debe promover desde la esfera de las responsabilidades que le compete a cada autoridad.

Segunda: Se han indicado los delitos cibernéticos se comenten en sus diversas modalidades. Ante ello, se recomienda a las entidades encargadas de velar por la seguridad de la identidad personal, buscar la adquisición de equipos o software que permita la detección de la intromisión de agente extraño en los datos personales. Ello implica hacer las gestiones y coordinaciones para exponer la situación problemática a fin de buscar las alternativas de solución de manera oportuna.

Tercera: Se recomienda a los jueces y fiscales que tienen la responsabilidad de conocer este tipo de delitos, aplicar mayor celeridad en las investigaciones y sanciones penales correspondientes. Es cierto que los delitos cibernéticos son de carácter complejo, sin embargo, a través de mecanismos de detección temprana de delitos se pueden optimizar los recursos de tiempo, economía, humanos, y alcanzar los resultados en el menor tiempo posible.

Cuarta: En relación al tercer objetivo específico se recomienda a los jueces y fiscales proponer formulas legislativas al Congreso de la República en relación a la seguridad cibernética. Pues, es de conocimiento común, así como existen esfuerzos nacionales e internacionales para implementar las leyes en protección de la intimidad personal,

también los delincuentes cambian de estrategia de manera constante, aspecto que debe conllevar al interés de actualizar la legislación nacional de manera permanentes.

REFERENCIAS

Aldecoa, M. (2020). El Delito de Suplantación de Identidad y los Medios Informáticos, en el Sector Financiero de Lima, 2019. Lima: Perú https://repositorio.ucv.edu.pe/handle/20.500.12692/61838

Álvarez Robles, T. (2022). Las garantías de los derechos fundamentales en y desde la red: El contexto español. *Revista chilena de derecho y tecnología*, *11*(1), 5-40. https://www.scielo.cl/scielo.php?pid=S0719-25842022000100005&script=sci_arttext&tlng=pt

Álvarez, R. B. (2017). El robo de identidad en México. *Dikê: Revista de Investigación en Derecho, Criminología y Consultoría Jurídica*, (22), 245-260. https://dialnet.unirioja.es/servlet/articulo?codigo=6622310

Aquino Barreto, N. Y. (2020). Comparación de regulaciones jurídicas sobre la prevención del robo de identidad entre México y Argentina del año 2010 al 2018. http://ri.uaemex.mx/handle/20.500.11799/112985

Arias, M., & Giraldo, C. (2011). Scientific Rigor In Qualitative Research. Scielo Analyties, 29(3), 500-514. http://www.scielo.org.co/scielo.php?script=sci_arttext&pid=S0120-53072011000300020

Arvelo, P. M. M., Paucar, C. E. P., & Parraga, C. M. C. (2022). Regulación global para evitar la suplantación de identidad digital. *Universidad y Sociedad*, *14*(6), 690-696. https://rus.ucf.edu.cu/index.php/rus/article/view/3419

Ataucuri Ynfante, I. D., Braúl Porras, R. R., Valdivia Ramos, R. J., & Mendoza De Los Santos, A. (2022). Sistema de autenticación de doble factor en un sistema web de facturación. *Revista de Investigación Multidisciplinaria CTSCAFE*, *6*(17), 11-11. http://www.ctscafe.pe/index.php/ctscafe/article/view/205

BARTOLOMÉ, M., & MONTEIRO LIMA, A. G. (2021). EL CIBERESPACIO, DURANTE Y DESPUÉS DE LA PANDEMIA COVID-19. *Revista De La Academia Del Guerra Del Ejército Ecuatoriano*, *14*(1), 10. https://doi.org/10.24133/age.n14.2021.06

Benítez, V.M. (2022). El Ciberdelito, desafíos para la ley penal y civil. Marco jurídico nacional y comparado. Revista Jurídica, edición especial. 2022;7(1):177-188. http://revistacientifica.uaa.edu.py/index.php/juridica/article/view/1434/1224

Bravo, C. J., Ramírez, P. E., & Arenas, J. (2018). Aceptación del reconocimiento facial como medida de vigilancia y seguridad: Un estudio empírico en Chile. *Información tecnológica*, *29*(2), 115-122. https://www.scielo.cl/scielo.php?pid=S0718-07642018000200115&script=sci_arttext&tlng=en

Cerdán, T. A. R. (2019). La autenticación y verificación de la identidad a través de información biométrica como paradigma del tratamiento de datos personales en México. *Revista del Posgrado en Derecho de la UNAM*, (10), 32-32. https://revistaderecho.posgrado.unam.mx/index.php/rpd/article/view/854

Diana Catalina Toledo-Verdugo, & Fernando Esteban Ochoa-Rodríguez. (2021). Derechos fundamentales y criminalidad cibernética en niños, niñas y adolescentes: análisis para la no indefensión de la víctima. *Revista Científica*, *6*(4), 336-363. https://fipcaec.com/index.php/fipcaec/article/view/485

Díaz, M. P. G. D. (2020). Los nuevos retos del derecho a la identidad en el Perú: desde la heteroasignación hacia la autodeterminación. *Persona y Familia*, (9), 221-242. https://revistas.unife.edu.pe/index.php/personayfamilia/article/view/2340

Fernández, P. (2018). La importancia de la Técnica de la Entrevista en la Investigación en Comunicación y las Ciencias Sociales. Investigación Documental. Ventajas y Limitaciones. Sintaxis, Revista del Centro de

Investigación Para la Comunicación Aplicada, 07(1), 78-93. doi:https://doi.org/10.36105/stx.2018n1.07

FERNÁNDEZ, W.; VARGAS, C. ¿Son útiles las TIC para combatir la ciberdelincuencia? La relación entre la denuncia de delitos informáticos y el equipamiento tecnológico de las comisarías. Law, State and Telecommunications Review, [S. l.], v. 10, n. 2, p. 37–52, 2018. https://periodicos.unb.br/index.php/RDET/article/view/21492

Flores Machuca, M. A., & Uriarte Pérez, G. S. (2023). Contribución de los medios tecnológicos en el delito informático de la suplantación de identidad en las telecomunicaciones, Jaén 2022. https://repositorio.ucv.edu.pe/handle/20.500.12692/113122

Focás, B. (2018). Miedo al crimen, prevención del delito y narcotráfico: desafíos para las políticas públicas de seguridad ciudadana en América Latina. Entrevista a Lucía Dammert. *URVIO Revista Latinoamericana de Estudios de Seguridad*, (22), 102-108. http://scielo.senescyt.gob.ec/scielo.php?pid=S1390-42992018000100102&script=sci_arttext

Gamón, V. P. (2017). Internet, la nueva era del delito: ciberdelito, ciberterrorismo, legislación y ciberseguridad. *URVIO Revista Latinoamericana de Estudios de Seguridad*, (20), 80-93. http://scielo.senescyt.gob.ec/scielo.php?pid=S1390-42992017000200080&script=sci_arttext

González-Ramírez, Teresa y Ángela López-Gracia (2018). «La identidad digital de los adolescentes: Usos y riesgos de las Tecnologías de la Información y la Comunicación». Revista Latinoamericana de Tecnología Educativa, 17 (2): 73-85. https://relatec.unex.es/article/view/3319

Irshad, S., & Soomro, T. R. (2018). Identity theft and social media. International Journal of Computer Science and Network Security, 18(1), 43-55. chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://www.researchgate.net/profile/Tariq-Soomro-

2/publication/323185128_Identity_Theft_and_Social_Media/links/5a850d2aa6fdcc201b9f044c/Identity-Theft-and-Social-Media.pdf

Loayza, E. (2020). La Investigación Cualitativa en Ciencias Humanas y Educación. Criterios Para Elaborar Artículos Científicos. Educare Et Comunicare, 8(2), 56-66. doi:https://doi.org/10.35383/educare.v8i2.536

López Gorostidi, J. (2022). Sobre el alcance de los fines de la pena en el fenómeno criminal de la ciberdelincuencia. Revista Chilena De Derecho Y Tecnología, 11(1), 121–146. https://doi.org/10.5354/0719-2584.2022.60913

Manterola, C., Grande, L., Otzen, T., Garcia, N., Salazar, P., & Quiroz, G. (2018). Confiabilidad, Precisión o Reproducibilidad de las Mediciones. Métodos de Valoración, Utilidad y Aplicaciones en la Práctica Clínica. Revista Chilena de Infectologia, Scielo Analytics, 35(6), 680-688. https://www.scielo.cl/scielo.php?script=sci_arttext&pid=S0716-10182018000600680

Martínez Molano, V., & Rincón Cárdenas, E. (2021). Problemas y desarrollo de la identidad en el mundo digital. *Revista chilena de derecho y tecnología*, *10*(2), 251-276. https://www.scielo.cl/scielo.php?pid=S0719-25842021000200251&script=sci_arttext

Mayer Lux, L. (2018). Elementos criminológicos para el análisis jurídico-penal de los delitos informáticos. *Ius et Praxis*, *24*(1), 159-206. https://www.scielo.cl/scielo.php?pid=S0718-00122018000100159&script=sci_arttext

MENDEZ, C., ANAMOURA, P. & NOVAIS, P. (2018). Intelligent phishing detection system. International Journal of Information Management, 38(1), 137-147. doi: 10.1016/j.ijinfomgt.2017.09.004

Mitxelena, X. (2020). Euskadi 2025-Sin ciberseguridad no hay futuro. *Ekonomiaz: Revista vasca de economía*, (98), 194-227. https://dialnet.unirioja.es/servlet/articulo?codigo=7694317

Molina, A. L. S., & Ochoa, N. V. V. (2020). El entorno virtual íntimo y privado como Derecho Humano de nueva generación. *Revista UNIANDES Episteme*, *7*(1), 1034-1047. https://dialnet.unirioja.es/servlet/articulo?codigo=8298056

Muntané, J. (2010). Introducción a la Investigación Básica. Revista Temáticas, RAPD Online, 33(3), 221-227. https://www.sapd.es/revista/2010/33/3/03/resumen

Páramo, D. (2015). La Teoría Fundamentada (Grounded Theory), Metodología Cualitativa de Investigación Científica. Redalyc, Pensamiento & Gestión (39), viixiii. Obtenido de https://www.redalyc.org/pdf/646/64644480001.pdf

Pareja, Alejandro, Mari Pedak, Carlos Gómez y Alejandro Barros (2017). La gestión de la identidad y su impacto en la economía digital. Banco Interamericano de Desarrollo. https://bit.ly/3DkAL2I

Pérez, F. V. N., & Zaldaña, B. C. (2020). Ciberdelincuencia en tiempos de covid-19:¿ La vulneración a derechos constitucionales?. *Lumen*, *16*(1), 93-100. https://revistas.unife.edu.pe/index.php/lumen/article/view/2287

Plaza, J., Uriguen, P., & Bejarano, H. (2017). Validez y Confiabilidad en la Investigación Cualitativa. ARJÉ, Revista de Postgrado FaCE-UC, 11(21), 352-357. http://arje.bc.uc.edu.ve/arj21/art24.pdf

Quiñonez Acevedo, E. (2017). La suplantación de identidad en las redes sociales. *Revista jurídica. Investigación En Ciencias jurídicas Y Sociales*, (6), 15–48. https://ojs.ministeriopublico.gov.py/index.php/rjmp/article/view/7

Quispe Ayala, V. F., & Quispe Saire, L. S. (2023). Análisis jurídico de la ineficacia de la Ley N° 30096 en el delito de suplantación de identidad por medios informáticos. https://repositorio.ucv.edu.pe/handle/20.500.12692/110772

Ralón, M. A. M. (2021). Robo de identidad y clonación de tarjetas de crédito y débito utilizando cajeros automáticos alterados. *Revista Diálogo Forense*, *2*(4). https://dialogoforense.inacif.gob.gt/index.php/dialogoforense/article/view/46

Rimaicuna Torres, M. F. (2021). Incorporación de las consecuencias nocivas del deepfake como agravantes del delito de suplantación de identidad en la Ley N° 30096. https://repositorio.ucv.edu.pe/handle/20.500.12692/82458

Rivera, Y., Mangone, A. D. P., Castaño, S., Tovio, J. M. T., Hernández, F. I., & Guevara, P. (2022). Análisis bibliométrico sobre Ciberseguridad: técnica de ataque de suplantación de identidad y evolución. *Revista Ibérica de Sistemas e Tecnologias de Informação*, (E52), 21-35. https://www.proquest.com/docview/2758392936?pq-origsite=gscholar&fromopenview=true

Rodríguez Cevallos, C. D. L. M. (2018). Metodología de clasificación de delitos informáticos en redes sociales su tipificación según las leyes del Ecuador, determinación de vacíos legales y el proceso para propuesta de ley. https://repositorio.uisek.edu.ec/handle/123456789/3220

Rodríguez, C., Lorenzo, O., & Herrera, L. (2005). Teoría y Práctica del Análisis de Datos Cualitativos. Proceso General y Criterios de Calidad. International Journal Of Social Sciencies a Humanities, 15(2), 133-154. https://www.redalyc.org/articulo.oa?id=65415209

Ruiz, S. A. (2021). La ciberdelincuencia como fenómeno jurídico. Su tratamiento procesal. Revista Aequitas: Estudios sobre historia, derecho e instituciones, (18), 371-402. https://dialnet.unirioja.es/servlet/articulo?codigo=8101080

Sosa Umbo, O. A. (2022). Phishing como modalidad de delitos informáticos: a propósito de la suplantación y robo a los beneficiarios del Bono Universal en el Perú. https://repositorio.unp.edu.pe/handle/20.500.12676/3559

Tobón Betancur, C. A. (2020). Modelo de administración de identidad digital (IdM) sobre blockchain para la mitigación del riesgo por suplantación en sistemas e-banking. http://repositorio.itm.edu.co/handle/20.500.12622/4457

Utreras Logacho, P. L. (2021). *Gestión de identidad digital de usuarios en servicios web para la protección de la privacidad de la información* (Doctoral

dissertation, Ecuador-PUCESE-Escuela de Sistemas y Computación). https://repositorio.pucese.edu.ec/handle/123456789/2419

Valdebenito, H. J., & Sánchez, A. M. (2018). Seguridad hemisférica latinoamericana adaptada a las nuevas tecnologías: Ciberseguridad y avances de cooperación regional e internacional para la sanción del ciberdelito. Revista ESPACIOS, 39(39). chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/http://es.revistaespacios.com/a18v39n39/a18v39n39p31.pdf

Valdivia, A. R. G. (2020). La identidad en la era digital. *Revista Mexicana de Ciencias Penales*, *3*(10), 19-34. https://revistaciencias.inacipe.gob.mx/index.php/02/article/view/95

Vilchez Limay, R. C. (2020). La ciberdelincuencia en el contexto de la pandemia del coronavirus: una aproximación desde el marco convencional. *La ciberdelincuencia en el contexto de la pandemia del coronavirus: una aproximación desde el marco convencional*, 21-25. https://dialnet.unirioja.es/servlet/articulo?codigo=7931775

Vilchez, L.C. (2020). La ciberdelincuencia en el contexto de la pandemia del coronavirus. Una aproximación desde el marco convencional. *Ars Iuris Salmanticensis TRIBUNA DE ACTUALIDAD 8*, 21-25. https://revistas.usal.es/index.php/ais/article/download/25688/24992/88341

Vinelli Vereau, R. (2021). Los delitos informáticos y su relación con la criminalidad económica. Ius Et Praxis, 95-110. https://doi.org/10.26439/iusetpraxis2021.n053.4995

Zarate, P., & Becerra, M. D. C. (2021). Robo de Identidad y su Incidencia en el Cibercrimen. In *XXI Simposio Argentino de Informática y Derecho (SID 2021)-JAIIO 50*. http://sedici.unlp.edu.ar/handle/10915/141414

Zelada Ruano, J. C. (2018) Procedimientos a seguir por las víctimas del robo de identidad. chrome-

extension://efaidnbmnnnibpcajpcglclefindmkaj/https://glifos.upana.edu.gt/library/images/4/44/TESIS_DE_JUAN_CARLOS_ZELADA_RUANO.pdf

ANEXOS

Anexo 1. Tabla de categorización

Problemas	Objetivos	Categorías	Subcategorías	Códigos
Problema general ¿De qué manera la proliferación dela ciberdelincuencia afecta el bien jurídico del derecho a la identidad, Callao 2022? **Problemas específicos** 1. ¿De qué modo la caracterización actual de la ciberdelincuencia repercute en el derecho a la identidad? 2. ¿De qué forma las sanciones penales ante la ciberdelincuencia incide en la mitigación de la misma? 3. ¿De qué manera la legislación peruana favorece a la ciberseguridad como antídoto a los delitos cibernéticos?	**Objetivo general** Analizar la manera en que la proliferación de la ciberdelincuencia afecta el bien jurídico del derecho a la identidad, Callao 2022 **Objetivos específicos** 1. Describir el modo en que la caracterización actual de la ciberdelincuencia repercute en el derecho a la identidad. 2. Analizar la forma en que los fines de la pena ante la ciberdelincuencia incide en la mitigación de la misma. 3. Delimitar la manera en que la legislación peruana favorece a la ciberseguridad como antídoto a los delitos cibernéticos.	Ciberdelincuencia Derecho a la identidad	Caracterización de la ciberdelincuencia Efectividad de la sanción penal Legislación peruana ante la ciberdelincuencia Tendencia actual El bien jurídico protegido Delitos que atentan al derecho a la identidad Métodos de protección de la identidad Eficacia normativa penal para proteger el derecho a la identidad	Participantes: - Seis fiscales del Distrito Fiscal del Callao / FP-DFC

Nota: elaboración propia

Anexo 2. Categorías, subcategorías y matriz de categorización

Categorías de estudio	Autor base	Subcategorías	Definición conceptual
Ciberdelincuencia	La ciberdelincuencia que es el incremento desmesurado de los delitos cometidos a través de medios informáticos, del internet, afectando tanto a personas naturales como jurídicas; el accionar del ciberdelincuente es del anonimato que tiene la capacidad de vulnerar la información personal con el fin de cometer un delito (Benítez, 2022)	Caracterización de la ciberdelincuencia	Son características la flexibilidad de la identidad del delincuente, de desterritorializacion y uso de inteligencia artificial para burlar la seguridad de la persona y/o institución (Cámara, 2020).
		Efectividad de la sanción penal	La punición de estas conductas debe desarrollarse dentro del marco del debido proceso, sin dejar de tomar en cuenta los principios inherentes a un estado constitucional de derecho (Valdebenito y Sanchez,2018).
		Legislación peruana ante la ciberdelincuencia	Ley N° 30096 (22 de octubre de 2013) se ha enmarcado ciertos delitos como parte de los delitos cometidos mediante la red.
		Tendencia actual	Los ataques de ransomware han sido una tendencia al alza en la ciberdelincuencia.
Derecho a la identidad	La identidad como derecho fundamental es vital para el desenvolvimiento del ciudadano en la sociedad; donde al ser protegida a nivel constitucional, es oponible - carácter erga omnes-, no posibilitando la derogación ni suspensión de este derecho (Ruiz,2021).	El bien jurídico protegido	Son la vida y la integridad personal en todos los sentidos – sexual, moral, psíquico y físico-. (Toledo y Ochoa, 2020).
		Delitos que atentan al derecho a la identidad	Se ve vulnerado cuando por medio de la red u otro medio se extraen los datos de un sujeto con un propósito netamente doloso (Zárate y Becerra,2021).
		Métodos de protección de la identidad	La identidad puede ser salvaguardada mediante el implemento de métodos biométricos; estos son información interna de un individuo, que no pueden ser modificados por voluntad propia (Cerda,2019).
		Eficacia normativa penal para proteger el derecho a la identidad	La ley N.° 30096 – Ley de delitos cibernéticos-, en su Artículo 9° dispone que aquel que utilice los medios informáticos con fines perjudiciales, para usurpar la identidad de un individuo o empresa, (Diaz,2020).

VALIDEZ POR JUICIO DE EXPERTOS

Señor(a)(ita): ALEJANDRO SABINO MENACHO RIVERA

Presente

Asunto: Validación de instrumentos a través de juicio de experto

Me es muy grato comunicarme con Usted para expresarle mi saludo y, así mismo, hacer de su conocimiento que, siendo estudiante del Programa Académico de Maestría en Derecho Penal y Procesal Penal de la Escuela de Posgrado de la UCV, Sede Lima Norte, requiero validar el instrumento con el cual recogeré la información necesaria para desarrollar mi trabajo de investigación.

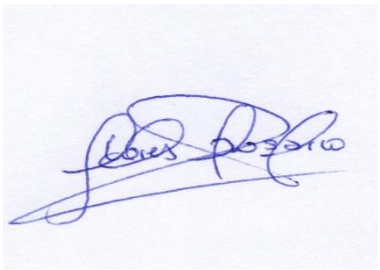
El título del proyecto de investigación es: **Proliferación de la ciberdelincuencia como afectación al bien jurídico del derecho a la identidad, Callao 2022**, y siendo imprescindible contar con la aprobación de docentes especializados para poder aplicar los instrumentos en mención, he considerado conveniente recurrir a usted, ante su connotada experiencia en temas relacionados a al programa en mención.

El expediente de validación que le hago llegar contiene:

- Carta de presentación.
- Definiciones conceptuales de las categorías y subcategorías
- Matriz de consistencia
- Guía de entrevista

Expresándole mis sentimientos de respeto y consideración me despido de Usted, no sin antes agradecerle por la atención que dispense a la presente.

Atentamente



Jessica Andrea Flores Rosario

DNI: 40604029

Evaluación por juicio de expertos

La evaluación del instrumento es de gran relevancia para lograr que sea válido y que los resultados obtenidos a partir de éste sean utilizados eficientemente. Agradecemos su valiosa colaboración.

1. Datos generales

Nombre del juez:	**ALEJANDRO SABINO MENACHO RIVERA**	
Grado profesional:	Maestría ( )	**Doctor (X)**
Área de formación académica:	Clínica ( ) **Educativa (X)**	Social ( ) Organizacional ( )
Áreas de experiencia profesional:	**Educación, derecho, gestión pública, Docencia Universitaria**	
Institución donde labora:	**Universidad César Vallejo**	
Tiempo de experiencia profesional en el área:	2 a 4 años ( )	**Más de 5 años (X)**
Experiencia en Investigación Psicométrica: (si corresponde)	Trabajo(s) psicométricos realizados	

2. Propósito de la evaluación:

Validar el contenido del instrumento por juicio de expertos.

3. Datos de la guía de entrevista:

Nombre de la Prueba:	Validar el instrumento – Guía de entrevista semiestructurada
Autor (a):	Jessica Andrea Flores Rosario
Objetivo:	Validar el instrumento
Año:	2023
Ámbito de aplicación:	Lima Noroeste
Categorías:	C1: Proliferación de la ciberdelincuencia C2: Derecho a la identidad
Niveles o rango:	1 al 4
Cantidad de ítems:	12
Tiempo de aplicación:	60 minutos

4. <u>Presentación de instrucciones para el juez:</u>

A continuación, a Usted le presento la guía de la entrevista elaborado por la suscrita en el año 2023, de acuerdo con los siguientes indicadores califique cada uno de los ítems según corresponda.

Categoría	Calificación	Indicador
CLARIDAD El ítem se comprende fácilmente, es decir, su sintáctica y semántica son adecuadas.	1. No cumple con el criterio	El ítem no es claro.
	2. Bajo Nivel	El ítem requiere bastantes modificaciones o una modificación muy grande en el uso de las palabras de acuerdo con su significado o por la ordenación de estas.
	3. Moderado nivel	Se requiere una modificación muy específica de algunos de los términos del ítem.
	4. Alto nivel	El ítem es claro, tiene semántica y sintaxis adecuada.
COHERENCIA El ítem tiene relación lógica con la dimensión o indicador que está midiendo.	1. totalmente en desacuerdo (no cumple con el criterio)	El ítem no tiene relación lógica con la dimensión.
	2. Desacuerdo (bajo nivel de acuerdo)	El ítem tiene una relación tangencial /lejana con la dimensión.
	3. Acuerdo (moderado nivel)	El ítem tiene una relación moderada con la dimensión que se está midiendo.
	4. Totalmente de Acuerdo (alto nivel)	El ítem se encuentra está relacionado con la dimensión que está midiendo.
RELEVANCIA El ítem es esencial o importante, es decir debe ser.	1. No cumple con el criterio	El ítem puede ser eliminado sin que se vea afectada la medición de la dimensión.
	2. Bajo Nivel	El ítem tiene alguna relevancia, pero otro ítem puede estar incluyendo lo que mide éste.
	3. Moderado nivel	El ítem es relativamente importante.
	4. Alto nivel	El ítem es muy relevante y debe ser incluido.

Leer con detenimiento los ítems y calificar en una escala de 1 a 4 su valoración, así como solicitamos brinde sus observaciones que considere pertinente.

4: Alto nivel
3: Moderado nivel
2: Bajo Nivel
1: No cumple con el criterio

Instrumento que mide la categoría 1: Proliferación de la ciberdelincuencia

Definición de la categoría:

La ciberdelincuencia se refiere al conjunto de actividades delictivas que se llevan a cabo a través de medios electrónicos o digitales, utilizando tecnologías de la información y la comunicación como herramientas para cometer actos ilícitos. Estos actos pueden involucrar el acceso no autorizado a sistemas informáticos, el robo de información confidencial, la propagación de malware, el fraude en línea, el ciberespionaje, el acoso cibernético y otras formas de delitos cibernéticos.

Subcategoría 1: Caracterización de la ciberdelincuencia

Son características la flexibilidad de la identidad del delincuente (anonimato disociativo), de desterritorializacion (puede cometerse a nivel nacional e internacional) y uso de inteligencia artificial para burlar la seguridad de la persona y/o institución (ingeniería social), entre otros (Cámara, 2020).

Subcategoría 2: Efectividad de la sanción penal

La punición de estas conductas debe desarrollarse dentro del marco del debido proceso, sin dejar de tomar en cuenta los principios inherentes a un estado constitucional de derecho como la proporcionalidad y lesividad para hacer frente, advertir y erradicar esta nueva modalidad de delincuencia (Valdebenito y Sanchez,2018).

Subcategoría 3: Legislación peruana ante la ciberdelincuencia

Mediante la creación de la Ley N.º 30096 (22 de octubre de 2013) se ha enmarcado ciertos delitos como parte de los delitos cometidos mediante la red. Así tenemos: en el Artículo 2°, 3°, 4°, 5°, 7°, 8°, 9° y 10° los delitos de acceso ilícito, ataque a la integridad de los datos informáticos, ataque a la integridad de sistemas informáticos, proposiciones a niños, niñas y adolescentes con fines sexuales por medios tecnológicos, interceptación de datos informáticos, fraude informático, suplantación de identidad y el abuso de mecanismos y dispositivos informáticos correspondientemente (Pérez y Saldaña,2020).

Ítem	**Claridad**	**Coherencia**	**Relevancia**	**Observaciones/ Recomendaciones**
1. Desde su punto de vista, ¿De qué manera la proliferación de la ciberdelincuencia afecta el bien jurídico del derecho a la identidad? Fundamente su respuesta.	Alto nivel	Alto nivel	Alto nivel	
2. ¿Conoce el modus operandi de los ciberdelincuentes que vulneran el derecho a la identidad mediante el uso de los recursos tecnológicos?	Alto nivel	Alto nivel	Alto nivel	
3. ¿Qué responsabilidad tienen los proveedores de servicios en línea y las plataformas digitales	Alto nivel	Alto nivel	Alto nivel	

en la protección de la identidad personal de sus usuarios?				
4. ¿Considera que las penas establecidas en el ordenamiento jurídico penal deben incidir en la mitigación de la ciberdelincuencia en el Perú?	Alto nivel	Alto nivel	Alto nivel	
5. Subraya los desafíos legales y éticos asociados con la recopilación y uso de información personal en el contexto de la ciberdelincuencia.	Alto nivel	Alto nivel	Alto nivel	
6. ¿Conoce las medidas legales y tecnológicas que existen en el Perú para prevenir y combatir la ciberdelincuencia que afecta la identidad personal?	Alto nivel	Alto nivel	Alto nivel	
7. ¿Cuáles es la importancia del papel de las autoridades y organismos nacionales e internacionales en la lucha contra la ciberdelincuencia que afecta la identidad personal?	Alto nivel	Alto nivel	Alto nivel	

Instrumento que mide la categoría 2: Derecho a la identidad

Definición de categoría:

"El derecho a la identidad es un derecho humano básico, esencial para el pleno desarrollo y dignidad de cada individuo." (Comité de los Derechos del Niño de las Naciones Unidas).

Subcategoría 1: El bien jurídico protegido

Son la vida y la integridad personal en todos los sentidos – sexual, moral, psíquico y físico-. Pues ellos son protectores del derecho a la imagen, al honor, inviolabilidad del secreto de telecomunicaciones, buen nombre y/o reputación (Toledo y Ochoa, 2020).

Subcategoría 2: Delitos que atentan al derecho a la identidad

Al ser la identidad un derecho personalísimo protegido por la Carta Magna; se ve vulnerado cuando por medio de la red u otro medio se extraen los datos de un sujeto con un propósito netamente doloso (Zárate y Becerra,2021).

Subcategoría 3: Métodos de protección de la identidad

La identidad puede ser salvaguardada mediante el implemento de métodos biométricos; estos son información interna de un individuo, que no pueden ser modificados por voluntad propia. Esta característica de perpetuidad genera que no puede ser alterada ni con el transcurso del tiempo (Cerda,2019).

Subcategoría 4: Eficacia normativa penal para proteger el derecho a la identidad

La ley N.° 30096 – Ley de delitos cibernéticos-, en su Artículo 9° dispone que aquel que utilice los medios informáticos con fines perjudiciales -moral o material-, para usurpar la identidad de un individuo o empresa, será merecedor de encarcelamiento en un periodo no menor de tres ni superior a cinco años (Diaz,2020).

Ítem	Claridad	Coherencia	Relevancia	Observaciones/ Recomendaciones
8. ¿Tiene pleno conocimiento del bien jurídico que protege el derecho a la identidad?	Alto nivel	Alto nivel	Alto nivel	
9. ¿Conoce las políticas y legislaciones existentes que protegen el derecho a la identidad personal y cómo se aplican en el Perú?	Alto nivel	Alto nivel	Alto nivel	
10. ¿Cuáles son los principales derechos asociados al derecho a la identidad personal y cómo se ven vulnerados por la ciberdelincuencia?	Alto nivel	Alto nivel	Alto nivel	
11. ¿Conoce las políticas y legislaciones existentes que protegen el derecho a la identidad personal	Alto nivel	Alto nivel	Alto nivel	

ante la vulneración por medios cibernéticos?				
12 ¿Cuáles son los derechos y responsabilidades de los individuos en la protección de su propia identidad personal frente a la ciberdelincuencia?	Alto nivel	Alto nivel	Alto nivel	
13. ¿Cuáles son las estrategias legales y sociales se pueden implementar para prevenir y abordar la vulneración del derecho a la identidad personal?	Alto nivel	Alto nivel	Alto nivel	

Observaciones (precisar si hay suficiencia en la cantidad de ítem):

TIENESUFICIENCIA, ES APLICABLE

Opinión de aplicabilidad: Aplicable [x] Aplicable después de corregir [ ] No aplicable [ ]

Apellidos y nombres del juez validador Dr/ Mg: MENACHO RIVERA ALEJANDRO SABINO

DNI: 32403439
Orcid: https://orcid.org/0000-0003-2365-8932

Especialidad del validador: Metodólogo

01 de junio del 2023

[1]**Pertinencia:** El ítem corresponde al concepto teórico formulado.

[2]**Relevancia:** El ítem es apropiado para representar al componente odimensión específica del constructo.
[3]**Claridad:** Se entiende sin dificultad alguna el enunciado del ítem, esconciso, exacto y directo.

Firma

Guía de entrevista

Título: Aplicación de la habitualidad en los procesos penales y afectación de la presunción de inocencia, Callao 2022
Entrevistado: ……...……...…….
Cargo/ Profesión/ Grado académico: …….....
Institución: …….....
_____

OBJETIVO GENERAL

Analizar la manera en que la proliferación de la ciberdelincuencia afecta el bien jurídico del derecho a la identidad, Callao 2022

1. Desde su punto de vista, ¿De qué manera la proliferación de la ciberdelincuencia afecta el bien jurídico del derecho a la identidad? Fundamente su respuesta.

OBJETIVO ESPECÍFICO 1

Describir el modo en que la caracterización actual de la ciberdelincuencia repercute en el derecho a la identidad, Callao 2022

2. ¿Conoce el modus operandi de los ciberdelincuentes que vulneran el derecho a la identidad mediante el uso de los recursos tecnológicos?

3. ¿Qué responsabilidad tienen los proveedores de servicios en línea y las plataformas digitales en la protección de la identidad personal de sus usuarios?

4. ¿Considera que las penas establecidas en el ordenamiento jurídico penal deben incidir en la mitigación de la ciberdelincuencia en el Perú?

OBJETIVO ESPECÍFICO 2

Analizar la forma en que los fines de la pena ante la ciberdelincuencia incide en la mitigación de la misma.

5. Subraya los desafíos legales y éticos asociados con la recopilación y uso de información personal en el contexto de la ciberdelincuencia.

6. ¿Conoce las medidas legales y tecnológicas que existen en el Perú para prevenir y combatir la ciberdelincuencia que afecta la identidad personal?

7. ¿Cuál es la importancia del papel de las autoridades y organismos nacionales e internacionales en la lucha contra la ciberdelincuencia que afecta la identidad personal?

OBJETIVO ESPECÍFICO 3

Delimitar la manera en que la legislación peruana favorece a la ciberseguridad como antídoto a los delitos cibernéticos.

8. ¿Tiene pleno conocimiento del bien jurídico que protege el derecho a la identidad?

9. ¿Conoce las políticas y legislaciones existentes que protegen el derecho a la identidad personal y cómo se aplican en el Perú?

10. ¿Cuáles son los principales derechos asociados al derecho a la identidad personal y cómo se ven vulnerados por la ciberdelincuencia?

11. ¿Conoce las políticas y legislaciones existentes que protegen el derecho a la identidad personal ante la vulneración por medios cibernéticos?

12. ¿Cuáles son los derechos y responsabilidades de los individuos en la protección de su propia identidad personal frente a la ciberdelincuencia?

13. ¿Cuáles son las estrategias legales y sociales se pueden implementar para prevenir y abordar la vulneración del derecho a la identidad personal?

VALIDEZ POR JUICIO DE EXPERTOS

Señor(a)(ita): Eleximia Soledad Díaz Díaz

Presente

Asunto: Validación de instrumentos a través de juicio de experto

Me es muy grato comunicarme con Usted para expresarle mi saludo y, así mismo, hacer de su conocimiento que, siendo estudiante del Programa Académico de Maestría en Derecho Penal y Procesal Penal de la Escuela de Posgrado de la UCV, Sede Lima Norte, requiero validar el instrumento con el cual recogeré la información necesaria para desarrollar mi trabajo de investigación.

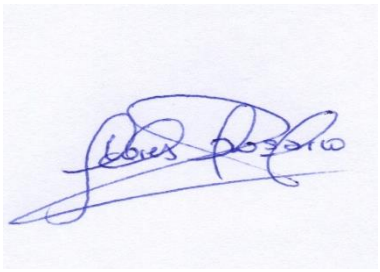
El título del proyecto de investigación es: **Proliferación de la ciberdelincuencia como afectación al bien jurídico del derecho a la identidad, Callao 2022**, y siendo imprescindible contar con la aprobación de docentes especializados para poder aplicar los instrumentos en mención, he considerado conveniente recurrir a usted, ante su connotada experiencia en temas relacionados a al programa en mención.

El expediente de validación que le hago llegar contiene:

- Carta de presentación.
- Definiciones conceptuales de las categorías y subcategorías
- Matriz de consistencia
- Guía de entrevista

Expresándole mis sentimientos de respeto y consideración me despido de Usted, no sin antes agradecerle por la atención que dispense a la presente.

Atentamente



Jessica Andrea Flores Rosario

DNI: 40604029

Evaluación por juicio de expertos

La evaluación del instrumento es de gran relevancia para lograr que sea válido y que los resultados obtenidos a partir de éste sean utilizados eficientemente. Agradecemos su valiosa colaboración.

1. Datos generales

Nombre del juez:	**Eleximia Soledad Díaz Díaz**	
Grado profesional:	**Maestría (x)**	Doctor ( )
Área de formación académica:	Clínica ( ) **Educativa (X)**	**Social (X)** **Organizacional (X)**
Áreas de experiencia profesional:	**Educación, derecho, gestión pública, Docencia Universitaria**	
Institución donde labora:	**Universidad César Vallejo**	
Tiempo de experiencia profesional en el área:	2 a 4 años ( )	**Más de 5 años (X)**
Experiencia en Investigación Psicométrica: (si corresponde)	Trabajo(s) psicométricos realizados	

2. Propósito de la evaluación:

Validar el contenido del instrumento por juicio de expertos.

3. Datos de la guía de entrevista:

Nombre de la Prueba:	Validar el instrumento – Guía de entrevista semiestructurada
Autor (a):	Jessica Andrea Flores Rosario
Objetivo:	Validar el instrumento
Año:	2023
Ámbito de aplicación:	Lima Noroeste
Categorías:	C1: Proliferación de la ciberdelincuencia C2: Derecho a la identidad
Niveles o rango:	1 al 4
Cantidad de ítems:	12
Tiempo de aplicación:	60 minutos

4. <u>Presentación de instrucciones para el juez:</u>

A continuación, a Usted le presento la guía de la entrevista elaborado por la suscrita en el año 2023, de acuerdo con los siguientes indicadores califique cada uno de los ítems según corresponda.

Categoría	Calificación	Indicador
CLARIDAD El ítem se comprende fácilmente, es decir, su sintáctica y semántica son adecuadas.	1. No cumple con el criterio	El ítem no es claro.
	2. Bajo Nivel	El ítem requiere bastantes modificaciones o una modificación muy grande en el uso de las palabras de acuerdo con su significado o por la ordenación de estas.
	3. Moderado nivel	Se requiere una modificación muy específica de algunos de los términos del ítem.
	4. Alto nivel	El ítem es claro, tiene semántica y sintaxis adecuada.
COHERENCIA El ítem tiene relación lógica con la dimensión o indicador que está midiendo.	1. totalmente en desacuerdo (no cumple con el criterio)	El ítem no tiene relación lógica con la dimensión.
	2. Desacuerdo (bajo nivel de acuerdo)	El ítem tiene una relación tangencial /lejana con la dimensión.
	3. Acuerdo (moderado nivel)	El ítem tiene una relación moderada con la dimensión que se está midiendo.
	4. Totalmente de Acuerdo (alto nivel)	El ítem se encuentra está relacionado con la dimensión que está midiendo.
RELEVANCIA El ítem es esencial o importante, es decir debe ser.	1. No cumple con el criterio	El ítem puede ser eliminado sin que se vea afectada la medición de la dimensión.
	2. Bajo Nivel	El ítem tiene alguna relevancia, pero otro ítem puede estar incluyendo lo que mide éste.
	3. Moderado nivel	El ítem es relativamente importante.
	4. Alto nivel	El ítem es muy relevante y debe ser incluido.

Leer con detenimiento los ítems y calificar en una escala de 1 a 4 su valoración, así como solicitamos brinde sus observaciones que considere pertinente.

4: Alto nivel
3: Moderado nivel
2: Bajo Nivel
1: No cumple con el criterio

Instrumento que mide la categoría 1: Proliferación de la ciberdelincuencia

Definición de la categoría:

La ciberdelincuencia se refiere al conjunto de actividades delictivas que se llevan a cabo a través de medios electrónicos o digitales, utilizando tecnologías de la información y la comunicación como herramientas para cometer actos ilícitos. Estos actos pueden involucrar el acceso no autorizado a sistemas informáticos, el robo de información confidencial, la propagación de malware, el fraude en línea, el ciberespionaje, el acoso cibernético y otras formas de delitos cibernéticos.

Subcategoría 1: Caracterización de la ciberdelincuencia

Son características la flexibilidad de la identidad del delincuente (anonimato disociativo), de desterritorializacion (puede cometerse a nivel nacional e internacional) y uso de inteligencia artificial para burlar la seguridad de la persona y/o institución (ingeniería social), entre otros (Cámara, 2020).

Subcategoría 2: Efectividad de la sanción penal

La punición de estas conductas debe desarrollarse dentro del marco del debido proceso, sin dejar de tomar en cuenta los principios inherentes a un estado constitucional de derecho como la proporcionalidad y lesividad para hacer frente, advertir y erradicar esta nueva modalidad de delincuencia (Valdebenito y Sanchez,2018).

Subcategoría 3: Legislación peruana ante la ciberdelincuencia

Mediante la creación de la Ley N.º 30096 (22 de octubre de 2013) se ha enmarcado ciertos delitos como parte de los delitos cometidos mediante la red. Así tenemos: en el Artículo 2°, 3°, 4°, 5°, 7°, 8°, 9° y 10° los delitos de acceso ilícito, ataque a la integridad de los datos informáticos, ataque a la integridad de sistemas informáticos, proposiciones a niños, niñas y adolescentes con fines sexuales por medios tecnológicos, interceptación de datos informáticos, fraude informático, suplantación de identidad y el abuso de mecanismos y dispositivos informáticos correspondientemente (Pérez y Saldaña,2020).

Ítem	Claridad	Coherencia	Relevancia	Observaciones/ Recomendaciones
1. Desde su punto de vista, ¿De qué manera la proliferación de la ciberdelincuencia afecta el bien jurídico del derecho a la identidad? Fundamente su respuesta.	Alto nivel	Alto nivel	Alto nivel	
2. ¿Conoce el modus operandi de los ciberdelincuentes que vulneran el derecho a la identidad mediante el uso de los recursos tecnológicos?	Alto nivel	Alto nivel	Alto nivel	
3. ¿Qué responsabilidad tienen los proveedores de servicios en línea y las plataformas digitales	Alto nivel	Alto nivel	Alto nivel	

en la protección de la identidad personal de sus usuarios?				
4. ¿Considera que las penas establecidas en el ordenamiento jurídico penal deben incidir en la mitigación de la ciberdelincuencia en el Perú?	Alto nivel	Alto nivel	Alto nivel	
5. Subraya los desafíos legales y éticos asociados con la recopilación y uso de información personal en el contexto de la ciberdelincuencia.	Alto nivel	Alto nivel	Alto nivel	
6. ¿Conoce las medidas legales y tecnológicas que existen en el Perú para prevenir y combatir la ciberdelincuencia que afecta la identidad personal?	Alto nivel	Alto nivel	Alto nivel	
7. ¿Cuáles es la importancia del papel de las autoridades y organismos nacionales e internacionales en la lucha contra la ciberdelincuencia que afecta la identidad personal?	Alto nivel	Alto nivel	Alto nivel	

Instrumento que mide la categoría 2: Derecho a la identidad

Definición de categoría:

"El derecho a la identidad es un derecho humano básico, esencial para el pleno desarrollo y dignidad de cada individuo." (Comité de los Derechos del Niño de las Naciones Unidas).

Subcategoría 1: El bien jurídico protegido

Son la vida y la integridad personal en todos los sentidos – sexual, moral, psíquico y físico-. Pues ellos son protectores del derecho a la imagen, al honor, inviolabilidad del secreto de telecomunicaciones, buen nombre y/o reputación (Toledo y Ochoa, 2020).

Subcategoría 2: Delitos que atentan al derecho a la identidad

Al ser la identidad un derecho personalísimo protegido por la Carta Magna; se ve vulnerado cuando por medio de la red u otro medio se extraen los datos de un sujeto con un propósito netamente doloso (Zárate y Becerra,2021).

Subcategoría 3: Métodos de protección de la identidad

La identidad puede ser salvaguardada mediante el implemento de métodos biométricos; estos son información interna de un individuo, que no pueden ser modificados por voluntad propia. Esta característica de perpetuidad genera que no puede ser alterada ni con el transcurso del tiempo (Cerda,2019).

Subcategoría 4: Eficacia normativa penal para proteger el derecho a la identidad

La ley N.° 30096 – Ley de delitos cibernéticos-, en su Artículo 9° dispone que aquel que utilice los medios informáticos con fines perjudiciales -moral o material-, para usurpar la identidad de un individuo o empresa, será merecedor de encarcelamiento en un periodo no menor de tres ni superior a cinco años (Diaz,2020).

Ítem	Claridad	Coherencia	Relevancia	Observaciones/ Recomendaciones
8. ¿Tiene pleno conocimiento del bien jurídico que protege el derecho a la identidad?	Alto nivel	Alto nivel	Alto nivel	
9. ¿Conoce las políticas y legislaciones existentes que protegen el derecho a la identidad personal y cómo se aplican en el Perú?	Alto nivel	Alto nivel	Alto nivel	
10. ¿Cuáles son los principales derechos asociados al derecho a la identidad personal y cómo se ven vulnerados por la ciberdelincuencia?	Alto nivel	Alto nivel	Alto nivel	
11. ¿Conoce las políticas y legislaciones existentes que protegen el derecho a la identidad personal	Alto nivel	Alto nivel	Alto nivel	

ante la vulneración por medios cibernéticos?				
12 ¿Cuáles son los derechos y responsabilidades de los individuos en la protección de su propia identidad personal frente a la ciberdelincuencia?	Alto nivel	Alto nivel	Alto nivel	
13. ¿Cuáles son las estrategias legales y sociales se pueden implementar para prevenir y abordar la vulneración del derecho a la identidad personal?	Alto nivel	Alto nivel	Alto nivel	

Observaciones (precisar si hay suficiencia en la cantidad de ítem): T**IENE SUFICIENCIA, ES APLICABLE**

Opinión de aplicabilidad: Aplicable [x] Aplicable después de corregir [ ] No aplicable

Apellidos y nombres del juez validador Dr/ Mg: Eleximia Soledad Díaz Díaz

DNI: 31664856
Orcid: *https://orcid.org/0000-0002-6299-7462*

Especialidad del validador: Temática

06 de junio del 2023

[1]**Pertinencia:** El ítem corresponde al concepto teórico formulado.
[2]**Relevancia:** El ítem es apropiado para representar al componente o dimensión específica del constructo.
[3]**Claridad:** Se entiende sin dificultad alguna el enunciado del ítem, es conciso, exacto y directo.

Firma

VALIDEZ POR JUICIO DE EXPERTOS

Señor(a)(ita): Ochoa Tataje Fredy

Presente

Asunto: Validación de instrumentos a través de juicio de experto

Me es muy grato comunicarme con Usted para expresarle mi saludo y, así mismo, hacer de su conocimiento que, siendo estudiante del Programa Académico de Maestría en Derecho Penal y Procesal Penal de la Escuela de Posgrado de la UCV, Sede Lima Norte, requiero validar el instrumento con el cual recogeré la información necesaria para desarrollar mi trabajo de investigación.

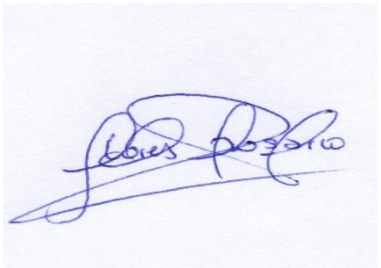
El título del proyecto de investigación es: **Proliferación de la ciberdelincuencia como afectación al bien jurídico del derecho a la identidad, Callao 2022**, y siendo imprescindible contar con la aprobación de docentes especializados para poder aplicar los instrumentos en mención, he considerado conveniente recurrir a usted, ante su connotada experiencia en temas relacionados a al programa en mención.

El expediente de validación que le hago llegar contiene:

- Carta de presentación.
- Definiciones conceptuales de las categorías y subcategorías
- Matriz de consistencia
- Guía de entrevista

Expresándole mis sentimientos de respeto y consideración me despido de Usted, no sin antes agradecerle por la atención que dispense a la presente.

Atentamente



Jessica Andrea Flores Rosario

DNI: 40604029

Evaluación por juicio de expertos

La evaluación del instrumento es de gran relevancia para lograr que sea válido y que los resultados obtenidos a partir de éste sean utilizados eficientemente. Agradecemos su valiosa colaboración.

1. Datos generales

Nombre del juez:	**Fredy Ochoa Tataje**
Grado profesional:	Maestría ( ) **Doctor (x)**
Área de formación académica:	Clínica ( ) **Social (X)** **Educativa (x)** **Organizacional (X)**
Áreas de experiencia profesional: **Institución donde labora:**	**Universidad César Vallejo**
Año de experiencia	2 a 4 años ( ) **Más de 5 años (X)**
Experiencia en Investigación Psicométrica: (si corresponde)	Trabajo(s) psicométricos realizados

2. Propósito de la evaluación:

Validar el contenido del instrumento por juicio de expertos.

3. Datos de la guía de entrevista:

Nombre de la Prueba:	Validar el instrumento – Guía de entrevista semiestructurada
Autor (a):	Jessica Andrea Flores Rosario
Objetivo:	Validar el instrumento
Año:	2023
Ámbito de aplicación:	Lima Noroeste
Categorías:	C1: Proliferación de la ciberdelincuencia C2: Derecho a la identidad
Niveles o rango:	1 al 4
Cantidad de ítems:	12
Tiempo de aplicación:	60 minutos

4. <u>Presentación de instrucciones para el juez:</u>

A continuación, a Usted le presento la guía de la entrevista elaborado por la suscrita en el año 2023, de acuerdo con los siguientes indicadores califique cada uno de los ítems según corresponda.

Categoría	Calificación	Indicador
CLARIDAD El ítem se comprende fácilmente, es decir, su sintáctica y semántica son adecuadas.	1. No cumple con el criterio	El ítem no es claro.
	2. Bajo Nivel	El ítem requiere bastantes modificaciones o una modificación muy grande en el uso de las palabras de acuerdo con su significado o por la ordenación de estas.
	3. Moderado nivel	Se requiere una modificación muy específica de algunos de los términos del ítem.
	4. Alto nivel	El ítem es claro, tiene semántica y sintaxis adecuada.
COHERENCIA El ítem tiene relación lógica con la dimensión o indicador que está midiendo.	1. totalmente en desacuerdo (no cumple con el criterio)	El ítem no tiene relación lógica con la dimensión.
	2. Desacuerdo (bajo nivel de acuerdo)	El ítem tiene una relación tangencial /lejana con la dimensión.
	3. Acuerdo (moderado nivel)	El ítem tiene una relación moderada con la dimensión que se está midiendo.
	4. Totalmente de Acuerdo (alto nivel)	El ítem se encuentra está relacionado con la dimensión que está midiendo.
RELEVANCIA El ítem es esencial o importante, es decir debe ser.	1. No cumple con el criterio	El ítem puede ser eliminado sin que se vea afectada la medición de la dimensión.
	2. Bajo Nivel	El ítem tiene alguna relevancia, pero otro ítem puede estar incluyendo lo que mide éste.
	3. Moderado nivel	El ítem es relativamente importante.
	4. Alto nivel	El ítem es muy relevante y debe ser incluido.

Leer con detenimiento los ítems y calificar en una escala de 1 a 4 su valoración, así como solicitamos brinde sus observaciones que considere pertinente.

4: Alto nivel
3: Moderado nivel
2: Bajo Nivel
1: No cumple con el criterio

Instrumento que mide la categoría 1: Proliferación de la ciberdelincuencia

Definición de la categoría:

La ciberdelincuencia se refiere al conjunto de actividades delictivas que se llevan a cabo a través de medios electrónicos o digitales, utilizando tecnologías de la información y la comunicación como herramientas para cometer actos ilícitos. Estos actos pueden involucrar el acceso no autorizado a sistemas informáticos, el robo de información confidencial, la propagación de malware, el fraude en línea, el ciberespionaje, el acoso cibernético y otras formas de delitos cibernéticos.

Subcategoría 1: Caracterización de la ciberdelincuencia

Son características la flexibilidad de la identidad del delincuente (anonimato disociativo), de desterritorializacion (puede cometerse a nivel nacional e internacional) y uso de inteligencia artificial para burlar la seguridad de la persona y/o institución (ingeniería social), entre otros (Cámara, 2020).

Subcategoría 2: Efectividad de la sanción penal

La punición de estas conductas debe desarrollarse dentro del marco del debido proceso, sin dejar de tomar en cuenta los principios inherentes a un estado constitucional de derecho como la proporcionalidad y lesividad para hacer frente, advertir y erradicar esta nueva modalidad de delincuencia (Valdebenito y Sanchez,2018).

Subcategoría 3: Legislación peruana ante la ciberdelincuencia

Mediante la creación de la Ley N.º 30096 (22 de octubre de 2013) se ha enmarcado ciertos delitos como parte de los delitos cometidos mediante la red. Así tenemos: en el Artículo 2°, 3°, 4°, 5°, 7°, 8°, 9° y 10° los delitos de acceso ilícito, ataque a la integridad de los datos informáticos, ataque a la integridad de sistemas informáticos, proposiciones a niños, niñas y adolescentes con fines sexuales por medios tecnológicos, interceptación de datos informáticos, fraude informático, suplantación de identidad y el abuso de mecanismos y dispositivos informáticos correspondientemente (Pérez y Saldaña,2020).

Ítem	Claridad	Coherencia	Relevancia	Observaciones/ Recomendaciones
1. Desde su punto de vista, ¿De qué manera la proliferación de la ciberdelincuencia afecta el bien jurídico del derecho a la identidad? Fundamente su respuesta.	***Alto nivel***	***Alto nivel***	***Alto nivel***	
2. ¿Conoce el modus operandi de los ciberdelincuentes que vulneran el derecho a la identidad mediante el uso de los recursos tecnológicos?	***Alto nivel***	***Alto nivel***	***Alto nivel***	
3. ¿Qué responsabilidad tienen los proveedores	***Alto nivel***	***Alto nivel***	***Alto nivel***	

de servicios en línea y las plataformas digitales en la protección de la identidad personal de sus usuarios?				
4. ¿Considera que las penas establecidas en el ordenamiento jurídico penal deben incidir en la mitigación de la ciberdelincuencia en el Perú?	***Alto nivel***	***Alto nivel***	***Alto nivel***	
5. Subraya los desafíos legales y éticos asociados con la recopilación y uso de información personal en el contexto de la ciberdelincuencia.	***Alto nivel***	***Alto nivel***	***Alto nivel***	
6. ¿Conoce las medidas legales y tecnológicas que existen en el Perú para prevenir y combatir la ciberdelincuencia que afecta la identidad personal?	***Alto nivel***	***Alto nivel***	***Alto nivel***	
7. ¿Cuáles es la importancia del papel de las autoridades y organismos nacionales e internacionales en la lucha contra la ciberdelincuencia que afecta la identidad personal?	***Alto nivel***	***Alto nivel***	***Alto nivel***	

Instrumento que mide la categoría 2: Derecho a la identidad

Definición de categoría:

"El derecho a la identidad es un derecho humano básico, esencial para el pleno desarrollo y dignidad de cada individuo." (Comité de los Derechos del Niño de las Naciones Unidas).

Subcategoría 1: El bien jurídico protegido

Son la vida y la integridad personal en todos los sentidos – sexual, moral, psíquico y físico-. Pues ellos son protectores del derecho a la imagen, al honor, inviolabilidad del secreto de telecomunicaciones, buen nombre y/o reputación (Toledo y Ochoa, 2020).

Subcategoría 2: Delitos que atentan al derecho a la identidad

Al ser la identidad un derecho personalísimo protegido por la Carta Magna; se ve vulnerado cuando por medio de la red u otro medio se extraen los datos de un sujeto con un propósito netamente doloso (Zárate y Becerra,2021).

Subcategoría 3: Métodos de protección de la identidad

La identidad puede ser salvaguardada mediante el implemento de métodos biométricos; estos son información interna de un individuo, que no pueden ser modificados por voluntad propia. Esta característica de perpetuidad genera que no puede ser alterada ni con el transcurso del tiempo (Cerda,2019).

Subcategoría 4: Eficacia normativa penal para proteger el derecho a la identidad

La ley N.° 30096 – Ley de delitos cibernéticos-, en su Artículo 9° dispone que aquel que utilice los medios informáticos con fines perjudiciales -moral o material-, para usurpar la identidad de un individuo o empresa, será merecedor de encarcelamiento en un periodo no menor de tres ni superior a cinco años (Diaz,2020).

Ítem	Claridad	Coherencia	Relevancia	Observaciones/ Recomendaciones
8. ¿Tiene pleno conocimiento del bien jurídico que protege el derecho a la identidad?	***Alto nivel***	***Alto nivel***	***Alto nivel***	
9. ¿Conoce las políticas y legislaciones existentes que protegen el derecho a la identidad personal y cómo se aplican en el Perú?	***Alto nivel***	***Alto nivel***	***Alto nivel***	
10. ¿Cuáles son los principales derechos asociados al derecho a la identidad personal y cómo se ven vulnerados por la ciberdelincuencia?	***Alto nivel***	***Alto nivel***	***Alto nivel***	
11. ¿Conoce las políticas y legislaciones existentes que protegen el derecho a la identidad personal	***Alto nivel***	***Alto nivel***	***Alto nivel***	

ante la vulneración por medios cibernéticos?				
12 ¿Cuáles son los derechos y responsabilidades de los individuos en la protección de su propia identidad personal frente a la ciberdelincuencia?	***Alto nivel***	***Alto nivel***	***Alto nivel***	
13. ¿Cuáles son las estrategias legales y sociales se pueden implementar para prevenir y abordar la vulneración del derecho a la identidad personal?	***Alto nivel***	***Alto nivel***	***Alto nivel***	

Observaciones (precisar si hay suficiencia en la cantidad de ítem): TIENE SUFICIENCIA, ES APLICABLE

Opinión de aplicabilidad: Aplicable [x] Aplicable después de corregir [ ] No aplicable [ ]

Apellidos y nombres del juez validador. Dr/ Mg: **OCHOA TATAJE FREDY**
DNI: 07015123

Especialidad del validador: Metodólogo

ORCID: 0000-0002-1410-1588

[1]**Pertinencia:** El ítem corresponde al concepto teórico formulado.
[2]**Relevancia:** El ítem es apropiado para representar al componente o dimensión específica del constructo
[3]**Claridad:** Se entiende sin dificultad alguna el enunciado del ítem, es conciso, exacto y directo

Nota: Suficiencia, se dice suficiencia cuando los ítems planteados

19 de octubre del 2020

Firma del Experto Informante.

UNIVERSIDAD CÉSAR VALLEJO

CONSENTIMIENTO INFORMADO

Título de la investigación:
"La proliferación de la ciberdelincuencia como afectación al bien jurídico del derecho a la identidad, Callao 2022"

Investigador:
Jessica Andrea Flores Rosario

Propósito del estudio
Le invitamos a participar en la investigación titulada **"La proliferación de la ciberdelincuencia como afectación al bien jurídico del derecho a la identidad, Callao 2022"** cuyo objetivo es analizar la manera en que la proliferación de la ciberdelincuencia afecta el bien jurídico del derecho a la identidad.
Esta investigación es desarrollada en el marco del Programa Académico Maestría en Derecho Penal y Procesal Penal de la Universidad César Vallejo del campus Lima Norte, aprobado por la autoridad correspondiente de la Universidad.

Procedimiento
Si usted decide participar en la investigación se realizará lo siguiente:

1. Se le enviara una guía de entrevista donde se recogerán sus datos personales y se consignaran algunas preguntas sobre la investigación titulada: **"La proliferación de la ciberdelincuencia como afectación al bien jurídico del derecho a la identidad, Callao 2022"**

2. Por efectos de la pandemia y a fin de no interrumpir su horario de trabajo trataremos de aprovechar todos los medios tecnológicos, de ser posible la presente guía de entrevista se realizará a través de aplicativo Google en la fecha y hora previamente acordada.

3. Por lo expuesto el participante acepta de manera voluntaria participar y contribuir con su experiencia en esta entrevista, firmando al final de este consentimiento informado en señal de conformidad.

INVESTIGA UCV

UNIVERSIDAD CÉSAR VALLEJO

Participación voluntaria (principio de autonomía):
Puede hacer todas las preguntas para aclarar sus dudas antes de decidir si desea participar o no, y su decisión será respetada. Posterior a la aceptación si no desea continuar puede hacerlo sin ningún problema.

Riesgo (principio de No maleficencia):
Indicar al participante la existencia que NO existe riesgo o daño al participar en la investigación. Sin embargo, en el caso que existan preguntas que le puedan generar incomodidad. Usted tiene la libertad de responderlas o no.

Beneficios (principio de beneficencia):
Se le informará que los resultados de la investigación se le alcanzará a la institución al término de la investigación. No recibirá ningún beneficio económico ni de ninguna otra índole. El estudio no va a aportar a la salud individual de la persona, sin embargo, los resultados del estudio podrán convertirse en beneficio de la salud pública.

Confidencialidad (principio de justicia):
Los datos recolectados deben ser anónimos y no tener ninguna forma de identificar al participante. Garantizamos que la información que usted nos brinde es totalmente confidencial y no será usada para ningún otro propósito fuera de la investigación. Los datos permanecerán bajo custodia del investigador principal y pasado un tiempo determinado serán eliminados convenientemente.

Problemas o preguntas:
Si tiene preguntas sobre la investigación puede contactar con el:
Investigador: Jessica Andrea Flores Rosario
Email: jessiani0102@gmail.com
y Docente asesor: JAVIER A. NEYRA VILLANUEVA
jneyrav@ucvvirtual.edu.pe

Consentimiento
Después de haber leído los propósitos de la investigación autorizo participar en la investigación antes mencionada.

Nombres y apellidos: Víctor Hugo Montellanos Palomino

DNI 40723682

Fecha y hora: Lima, 12 de julio de 2023

Firma del entrevistado:

Victor H. Montellanos Palomino
FISCAL ADJUNTO
10 FPPC - CALLAO

UNIVERSIDAD CÉSAR VALLEJO

CONSENTIMIENTO INFORMADO

Título de la investigación:
"La proliferación de la ciberdelincuencia como afectación al bien jurídico del derecho a la identidad, Callao 2022"

Investigador:
Jessica Andrea Flores Rosario

Propósito del estudio
Le invitamos a participar en la investigación titulada **"La proliferación de la ciberdelincuencia como afectación al bien jurídico del derecho a la identidad, Callao 2022"** cuyo objetivo es analizar la manera en que la proliferación de la ciberdelincuencia afecta el bien jurídico del derecho a la identidad.
Esta investigación es desarrollada en el marco del Programa Académico Maestría en Derecho Penal y Procesal Penal de la Universidad César Vallejo del campus Lima Norte, aprobado por la autoridad correspondiente de la Universidad.

Procedimiento
Si usted decide participar en la investigación se realizará lo siguiente:

1. Se le enviara una guía de entrevista donde se recogerán sus datos personales y se consignaran algunas preguntas sobre la investigación titulada: **"La proliferación de la ciberdelincuencia como afectación al bien jurídico del derecho a la identidad, Callao 2022"**

2. Por efectos de la pandemia y a fin de no interrumpir su horario de trabajo trataremos de aprovechar todos los medios tecnológicos, de ser posible la presente guía de entrevista se realizará a través de aplicativo Google en la fecha y hora previamente acordada.

3. Por lo expuesto el participante acepta de manera voluntaria participar y contribuir con su experiencia en esta entrevista, firmando al final de este consentimiento informado en señal de conformidad.

INVESTIGA UCV

Participación voluntaria (principio de autonomía):

Puede hacer todas las preguntas para aclarar sus dudas antes de decidir si desea participar o no, y su decisión será respetada. Posterior a la aceptación si no desea continuar puede hacerlo sin ningún problema.

Riesgo (principio de No maleficencia):

Indicar al participante la existencia que NO existe riesgo o daño al participar en la investigación. Sin embargo, en el caso que existan preguntas que le puedan generar incomodidad. Usted tiene la libertad de responderlas o no.

Beneficios (principio de beneficencia):

Se le informará que los resultados de la investigación se le alcanzará a la institución al término de la investigación. No recibirá ningún beneficio económico ni de ninguna otra índole. El estudio no va a aportar a la salud individual de la persona, sin embargo, los resultados del estudio podrán convertirse en beneficio de la salud pública.

Confidencialidad (principio de justicia):

Los datos recolectados deben ser anónimos y no tener ninguna forma de identificar al participante. Garantizamos que la información que usted nos brinde es totalmente confidencial y no será usada para ningún otro propósito fuera de la investigación. Los datos permanecerán bajo custodia del investigador principal pasado un tiempo determinado serán eliminados convenientemente.

Problemas o preguntas:

Si tiene preguntas sobre la investigación puede contactar con el:

Investigador: Jessica Andrea Flores Rosario

Email: jessiani0102@gmail.com

y Docente asesor: JAVIER A. NEYRA VILLANUEVA
jneyrav@ucvvirtual.edu.pe

Consentimiento

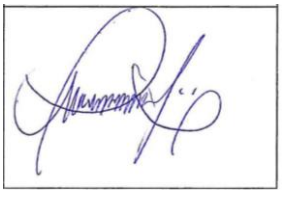
Después de haber leído los propósitos de la investigación autorizo participar en la investigación antes mencionada.

Nombres y apellidos: José Luis Morales Yataco

DNI 15450078

Fecha y hora: Lima, 12 de julio de 2023

Firma del entrevistado:



UNIVERSIDAD CÉSAR VALLEJO

CONSENTIMIENTO INFORMADO

Título de la investigación:
"La proliferación de la ciberdelincuencia como afectación al bien jurídico del derecho a la identidad, Callao 2022"

Investigador:
Jessica Andrea Flores Rosario

Propósito del estudio

Le invitamos a participar en la investigación titulada **"La proliferación de la ciberdelincuencia como afectación al bien jurídico del derecho a la identidad, Callao 2022"** cuyo objetivo es analizar la manera en que la proliferación de la ciberdelincuencia afecta el bien jurídico del derecho a la identidad.
Esta investigación es desarrollada en el marco del Programa Académico Maestría en Derecho Penal y Procesal Penal de la Universidad César Vallejo del campus Lima Norte, aprobado por la autoridad correspondiente de la Universidad.

VICERRECTORADO DE INVESTIGACIÓN
UNIVERSIDAD CÉSAR VALLEJO

Procedimiento

Si usted decide participar en la investigación se realizará lo siguiente:

1. Se le enviara una guía de entrevista donde se recogerán sus datos personales y se consignaran algunas preguntas sobre la investigación titulada: **"La proliferación de la ciberdelincuencia como afectación al bien jurídico del derecho a la identidad, Callao 2022"**

2. Por efectos de la pandemia y a fin de no interrumpir su horario de trabajo trataremos de aprovechar todos los medios tecnológicos, de ser posible la presente guía de entrevista se realizará a través de aplicativo Google en la fecha y hora previamente acordada.

3. Por lo expuesto el participante acepta de manera voluntaria participar y contribuir con su experiencia en esta entrevista, firmando al final de este consentimiento informado en señal de conformidad.

INVESTIGA UCV

Participación voluntaria (principio de autonomía):

Puede hacer todas las preguntas para aclarar sus dudas antes de decidir si desea participar o no, y su decisión será respetada. Posterior a la aceptación si no desea continuar puede hacerlo sin ningún problema.

Riesgo (principio de No maleficencia):

Indicar al participante la existencia que NO existe riesgo o daño al participar en la investigación. Sin embargo, en el caso que existan preguntas que le puedan generar incomodidad. Usted tiene la libertad de responderlas o no.

Beneficios (principio de beneficencia):

Se le informará que los resultados de la investigación se le alcanzará a la institución al término de la investigación. No recibirá ningún beneficio económico ni de ninguna otra índole. El estudio no va a aportar a la salud individual de la persona, sin embargo, los resultados del estudio podrán convertirse en beneficio de la salud pública.

Confidencialidad (principio de justicia):

Los datos recolectados deben ser anónimos y no tener ninguna forma de identificar al participante. Garantizamos que la información que usted nos brinde es totalmente confidencial y no será usada para ningún otro propósito fuera de la investigación. Los datos permanecerán bajo custodia del investigador principal y pasado un tiempo determinado serán eliminados convenientemente.

Problemas o preguntas:

Si tiene preguntas sobre la investigación puede contactar con el:

Investigador: Jessica Andrea Flores Rosario

Email: jessiani0102@gmail.com

y Docente asesor: JAVIER A. NEYRA VILLANUEVA
jneyrav@ucvvirtual.edu.pe

Consentimiento

Después de haber leído los propósitos de la investigación autorizo participar en la investigación antes mencionada.

Nombres y apellidos: Jesús Daniel Balvin Arbulú

DNI 47419086

Fecha y hora: Lima, 12 de julio de 2023

Firma del entrevistado:

JESÚS DANIEL BALVÍN ARBULÚ
DNI 47419086

UNIVERSIDAD CÉSAR VALLEJO

CONSENTIMIENTO INFORMADO

Título de la investigación:
"La proliferación de la ciberdelincuencia como afectación al bien jurídico del derecho a la identidad, Callao 2022"

Investigador:
Jessica Andrea Flores Rosario

Propósito del estudio
Le invitamos a participar en la investigación titulada **"La proliferación de la ciberdelincuencia como afectación al bien jurídico del derecho a la identidad, Callao 2022"** cuyo objetivo es analizar la manera en que la proliferación de la ciberdelincuencia afecta el bien jurídico del derecho a la identidad.
Esta investigación es desarrollada en el marco del Programa Académico Maestría en Derecho Penal y Procesal Penal de la Universidad César Vallejo del campus Lima Norte, aprobado por la autoridad correspondiente de la Universidad.

Procedimiento
Si usted decide participar en la investigación se realizará lo siguiente:

1. Se le enviara una guía de entrevista donde se recogerán sus datos personales y se consignaran algunas preguntas sobre la investigación titulada: **"La proliferación de la ciberdelincuencia como afectación al bien jurídico del derecho a la identidad, Callao 2022"**

2. Por efectos de la pandemia y a fin de no interrumpir su horario de trabajo trataremos de aprovechar todos los medios tecnológicos, de ser posible la presente guía de entrevista se realizará a través de aplicativo Google en la fecha y hora previamente acordada.

3. Por lo expuesto el participante acepta de manera voluntaria participar y contribuir con su experiencia en esta entrevista, firmando al final de este consentimiento informado en señal de conformidad.

INVESTIGA UCV

UNIVERSIDAD CÉSAR VALLEJO

Participación voluntaria (principio de autonomía):
Puede hacer todas las preguntas para aclarar sus dudas antes de decidir si desea participar o no, y su decisión será respetada. Posterior a la aceptación si no desea continuar puede hacerlo sin ningún problema.

Riesgo (principio de No maleficencia):
Indicar al participante la existencia que NO existe riesgo o daño al participar en la investigación. Sin embargo, en el caso que existan preguntas que le puedan generar incomodidad. Usted tiene la libertad de responderlas o no.

Beneficios (principio de beneficencia):
Se le informará que los resultados de la investigación se le alcanzará a la institución al término de la investigación. No recibirá ningún beneficio económico ni de ninguna otra índole. El estudio no va a aportar a la salud individual de la persona, sin embargo, los resultados del estudio podrán convertirse en beneficio de la salud pública.

Confidencialidad (principio de justicia):
Los datos recolectados deben ser anónimos y no tener ninguna forma de identificar al participante. Garantizamos que la información que usted nos brinde es totalmente confidencial y no será usada para ningún otro propósito fuera de la investigación. Los datos permanecerán bajo custodia del investigador principal y pasado un tiempo determinado serán eliminados convenientemente.

Problemas o preguntas:
Si tiene preguntas sobre la investigación puede contactar con el:
Investigador: Jessica Andrea Flores Rosario
Email: jessiani0102@gmail.com
y Docente asesor: JAVIER A. NEYRA VILLANUEVA
jneyrav@ucvvirtual.edu.pe

Consentimiento
Después de haber leído los propósitos de la investigación autorizo participar en la investigación antes mencionada.

Nombres y apellidos: Josseline Macbeth Purizaca Zeta

DNI 40176210

Fecha y hora: Lima, 12 de julio de 2023

Firma del entrevistado:

UNIVERSIDAD CÉSAR VALLEJO

CONSENTIMIENTO INFORMADO

Título de la investigación:
"La proliferación de la ciberdelincuencia como afectación al bien jurídico del derecho a la identidad, Callao 2022"

Investigador:
Jessica Andrea Flores Rosario

Propósito del estudio

Le invitamos a participar en la investigación titulada **"La proliferación de la ciberdelincuencia como afectación al bien jurídico del derecho a la identidad, Callao 2022"** cuyo objetivo es analizar la manera en que la proliferación de la ciberdelincuencia afecta el bien jurídico del derecho a la identidad.
Esta investigación es desarrollada en el marco del Programa Académico Maestría en Derecho Penal y Procesal Penal de la Universidad César Vallejo del campus Lima Norte, aprobado por la autoridad correspondiente de la Universidad.

Procedimiento

Si usted decide participar en la investigación se realizará lo siguiente:

1. Se le enviara una guía de entrevista donde se recogerán sus datos personales y se consignaran algunas preguntas sobre la investigación titulada: **"La proliferación de la ciberdelincuencia como afectación al bien jurídico del derecho a la identidad, Callao 2022"**

2. Por efectos de la pandemia y a fin de no interrumpir su horario de trabajo trataremos de aprovechar todos los medios tecnológicos, de ser posible la presente guía de entrevista se realizará a través de aplicativo Google en la fecha y hora previamente acordada.

3. Por lo expuesto el participante acepta de manera voluntaria participar y contribuir con su experiencia en esta entrevista, firmando al final de este consentimiento informado en señal de conformidad.

INVESTIGA UCV

Participación voluntaria (principio de autonomía):

Puede hacer todas las preguntas para aclarar sus dudas antes de decidir si desea participar o no, y su decisión será respetada. Posterior a la aceptación si no desea continuar puede hacerlo sin ningún problema.

Riesgo (principio de No maleficencia):

Indicar al participante la existencia que NO existe riesgo o daño al participar en la investigación. Sin embargo, en el caso que existan preguntas que le puedan generar incomodidad. Usted tiene la libertad de responderlas o no.

Beneficios (principio de beneficencia):

Se le informará que los resultados de la investigación se le alcanzará a la institución al término de la investigación. No recibirá ningún beneficio económico ni de ninguna otra índole. El estudio no va a aportar a la salud individual de la persona, sin embargo, los resultados del estudio podrán convertirse en beneficio de la salud pública.

Confidencialidad (principio de justicia):

Los datos recolectados deben ser anónimos y no tener ninguna forma de identificar al participante. Garantizamos que la información que usted nos brinde es totalmente confidencial y no será usada para ningún otro propósito fuera de la investigación. Los datos permanecerán bajo custodia del investigador principal y pasado un tiempo determinado serán eliminados convenientemente.

Problemas o preguntas:

Si tiene preguntas sobre la investigación puede contactar con el:

Investigador: Jessica Andrea Flores Rosario

Email: jessiani0102@gmail.com

y Docente asesor: JAVIER A. NEYRA VILLANUEVA
jneyrav@ucvvirtual.edu.pe

Consentimiento

Después de haber leído los propósitos de la investigación autorizo participar en la investigación antes mencionada.

Nombres y apellidos: Lucía de Jesús Huamán Tiza

DNI 42510507

Fecha y hora: Lima, 12 de julio de 2023

Firma del entrevistado:

Lucía De Jesús Huaman Tiza
Fiscal Provincial
Octava Fiscalía Provincial Penal Corporativa
Distrito Fiscal del Callao

UNIVERSIDAD CÉSAR VALLEJO

CONSENTIMIENTO INFORMADO

Título de la investigación:
"La proliferación de la ciberdelincuencia como afectación al bien jurídico del derecho a la identidad, Callao 2022"

Investigador:
Jessica Andrea Flores Rosario

Propósito del estudio
Le invitamos a participar en la investigación titulada **"La proliferación de la ciberdelincuencia como afectación al bien jurídico del derecho a la identidad, Callao 2022"** cuyo objetivo es analizar la manera en que la proliferación de la ciberdelincuencia afecta el bien jurídico del derecho a la identidad.
Esta investigación es desarrollada en el marco del Programa Académico Maestría en Derecho Penal y Procesal Penal de la Universidad César Vallejo del campus Lima Norte, aprobado por la autoridad correspondiente de la Universidad.

Procedimiento
Si usted decide participar en la investigación se realizará lo siguiente:

1. Se le enviara una guía de entrevista donde se recogerán sus datos personales y se consignaran algunas preguntas sobre la investigación titulada: **"La proliferación de la ciberdelincuencia como afectación al bien jurídico del derecho a la identidad, Callao 2022"**

2. Por efectos de la pandemia y a fin de no interrumpir su horario de trabajo trataremos de aprovechar todos los medios tecnológicos, de ser posible la presente guía de entrevista se realizará a través de aplicativo Google en la fecha y hora previamente acordada.

3. Por lo expuesto el participante acepta de manera voluntaria participar y contribuir con su experiencia en esta entrevista, firmando al final de este consentimiento informado en señal de conformidad.

INVESTIGA UCV

Firma Digital
Firmado digitalmente por BENITES CUADROS Maria Lizbet FAU 20131370301 soft
Motivo: Soy el autor del documento
Fecha: 12.07.2023 15:57:18 -05:00

Participación voluntaria (principio de autonomía):

Puede hacer todas las preguntas para aclarar sus dudas antes de decidir si desea participar o no, y su decisión será respetada. Posterior a la aceptación si no desea continuar puede hacerlo sin ningún problema.

Riesgo (principio de No maleficencia):

Indicar al participante la existencia que NO existe riesgo o daño al participar en la investigación. Sin embargo, en el caso que existan preguntas que le puedan generar incomodidad. Usted tiene la libertad de responderlas o no.

Beneficios (principio de beneficencia):

Se le informará que los resultados de la investigación se le alcanzará a la institución al término de la investigación. No recibirá ningún beneficio económico ni de ninguna otra índole. El estudio no va a aportar a la salud individual de la persona, sin embargo, los resultados del estudio podrán convertirse en beneficio de la salud pública.

Confidencialidad (principio de justicia):

Los datos recolectados deben ser anónimos y no tener ninguna forma de identificar al participante. Garantizamos que la información que usted nos brinde es totalmente confidencial y no será usada para ningún otro propósito fuera de la investigación. Los datos permanecerán bajo custodia del investigador principal y pasado un tiempo determinado serán eliminados convenientemente.

VICERRECTORADO DE INVESTIGACIÓN
UNIVERSIDAD CÉSAR VALLEJO

Problemas o preguntas:

Si tiene preguntas sobre la investigación puede contactar con el:

Investigador: Jessica Andrea Flores Rosario

Email: jessiani0102@gmail.com

y Docente asesor: JAVIER A. NEYRA VILLANUEVA
jneyrav@ucvvirtual.edu.pe

Consentimiento

Después de haber leído los propósitos de la investigación autorizo participar en la investigación antes mencionada.

Nombres y apellidos: María Lizbet Benites Cuadros

DNI 40331369

Fecha y hora: Lima, 12 de julio de 2023

Firma del entrevistado:

Firma Digital

Firmado digitalmente por BENITES CUADROS Maria Lizbet FAU 20131370301 soft
Motivo: Soy el autor del documento
Fecha: 12.07.2023 15:57:39 -05:00

Guía de entrevista

Título: Proliferación de la ciberdelincuencia como afectación al bien jurídico del derecho a la identidad, Callao 2022
Entrevistado: Lucía de Jesús Huamán Tiza
Cargo/ Profesión/ Grado académico: Fiscal Provincial 8FPPCALLAO / Abogada/Abogada
Institución: Ministerio Público

OBJETIVO GENERAL

Analizar la manera en que la proliferación de la ciberdelincuencia afecta el bien jurídico del derecho a la identidad, Callao 2022

1. Desde su punto de vista, ¿De qué manera la proliferación de la ciberdelincuencia afecta el bien jurídico del derecho a la identidad? Fundamente su respuesta.

En la actualidad los datos de una persona, imágenes y demás información que los identifican se encuentran registrados en los medios tecnológicos como el Internet y plataformas digitales; y debido a que la ciberdelincuencia se ejecuta en ese campo, su proliferación implica que los que cometen estos delitos, por lo general, accedan a esta información personal y la empleen para su propio beneficio.

OBJETIVO ESPECÍFICO 1

Describir el modo en que la caracterización actual de la ciberdelincuencia repercute en el derecho a la identidad, Callao 2022

2. ¿Conoce el modus operandi de los ciberdelincuentes que vulneran el derecho a la identidad mediante el uso de los recursos tecnológicos?

   En mi experiencia como fiscal he vistos dos modalidades muy recurrentes; la primera es que suplantan la identidad de una persona para cometer delitos con esta entidad suplantada como estafar a la gente, sea hackeando o clonando su Facebook, o usando información personal obtenida por estos medios para así suplantar la identidad y pedir algún tipo de beneficio económico a sus contactos. La segunda modalidad es que se agencian de datos de esta persona para acceder a sus cuentas bancarias y extraer su dinero.

3. ¿Qué responsabilidad tienen los proveedores de servicios en línea y las plataformas digitales en la protección de la identidad personal de sus usuarios?

   Ellos son responsables en establecer mecanismos de seguridad idóneos para prevenir estos delitos, con una política de alerta de detectarse la sospecha de la comisión de estos delitos; ello forma parte de la idoneidad de su servicio, incluso esta política de

prevención no sólo debe ser para externos sino también para sus propios empleados, quiénes pueden acceder con mayor facilidad a la información personal de sus usuarios.

4. ¿Considera que las penas establecidas en el ordenamiento jurídico penal deben incidir en la mitigación de la ciberdelincuencia en el Perú?

   Por supuesto, recordemos que los fines de la pena no solo se centran en la resocialización del agente, sino también en la prevención general y especial, esto con el fin de mermar la comisión de este tipo de delitos, que dado el incremento del uso de los medios tecnológicos para las relaciones inter personales y comerciales, está aumentando de manera alarmante.

OBJETIVO ESPECÍFICO 2

Analizar la forma en que los fines de la pena ante la ciberdelincuencia incide en la mitigación de la misma.

5. Subraya los desafíos legales y éticos asociados con la recopilación y uso de información personal en el contexto de la ciberdelincuencia.

Toda vez que, la ciberdelincuencia vulnera la identidad que a su vez está vinculado con la intimidad, el principal desafío radica en establecer a los operadores de justicia medios idóneos que no impliquen una invasión arbitraria a la intimidad; pero que den mayor celeridad y flexibilidad en la obtención de la información que el caso necesita, muchas veces la demora en requerir autorización al Juez y una vez obtenida esta, solicitar información a las empresas que guardan la información, retrasa y obstaculiza una eficiente investigación.

6. ¿Conoce las medidas legales y tecnológicas que existen en el Perú para prevenir y combatir la ciberdelincuencia que afecta la identidad personal?

Tengo entendido que las empresas que manejan esta información deben establecer adecuadas políticas de protección, bajo responsabilidad, por ende, las páginas de Internet deben contar con programas que no permitan o que bloqueen el acceso de personas no autorizadas.

7. ¿Cuál es la importancia del papel de las autoridades y organismos nacionales e internacionales en la lucha contra la ciberdelincuencia que afecta la identidad personal?

Ellos son los que deben establecer políticas de prevención para evitar a comisión de estos delitos, así como mecanismos flexibles e idóneos para los operadores de justicia con el fin de lograr una eficiente investigación una vez cometido y denunciado este delito.

OBJETIVO ESPECÍFICO 3

Delimitar la manera en que la legislación peruana favorece a la ciberseguridad como antídoto a los delitos cibernéticos.

8. ¿Tiene pleno conocimiento del bien jurídico que protege el derecho a la identidad?

   Considero que el derecho a la identidad es un bien jurídico por ser un derecho constitucional que permite individualizar a la persona de los demás miembros de la sociedad.

9. ¿Conoce las políticas y legislaciones existentes que protegen el derecho a la identidad personal y cómo se aplican en el Perú?

   La Constitución de 1993 reconoce el derecho a la identidad como un derecho fundamental, se han regulado leyes relacionadas a la identidad de una persona, como su registro en RENIEC y se ha emitido la Ley de Protección de Datos Personales justamente destinada a proteger los datos que identifican a una persona y que navegan por Internet.

10. ¿Cuáles son los principales derechos asociados al derecho a la identidad personal y cómo se ven vulnerados por la ciberdelincuencia?

    En mi opinión son el derecho a la intimidad, toda vez que los datos personales que identifican a los individuos forman parte de un privacidad e intimidad, la que es vulnerada cuando se accede a esta información sin autorización de su titular. También el derecho al patrimonio, pues por lo general a través de la ciberdelincuencia se perpetran sustracciones o estafas que afectan el patrimonio de las personas.

11. ¿Conoce las políticas y legislaciones existentes que protegen el derecho a la identidad personal ante la vulneración por medios cibernéticos?

    La Constitución Política del Estado y la Ley de Protección de Datos Personales que fue publicada en el Diario Oficial El Peruano el 3 de julio de 2011

12. ¿Cuáles son los derechos y responsabilidades de los individuos en la protección de su propia identidad personal frente a la ciberdelincuencia?

    Nosotros como usuarios de los medios tecnológicos, debemos comportarnos dentro del marco del consumidor razonable, y protector de nuestros propios intereses, esto es, verificar dentro de nuestras posibilidades que las plataformas a las que accedemos sean confiables, incluso, estar atento a las modalidades de ciberdelincuencia recurrentes, que son publicada de manera constante por la Policía Nacional.

13. ¿Cuáles son las estrategias legales y sociales se pueden implementar para prevenir y abordar la vulneración del derecho a la identidad personal?

Considero que debe existir una mayor difusión sobre cómo se comete la ciberdelincuencia y los mecanismos de protección que deben usar los usuarios, sumado a ello, se debe exigir de manera eficiente que las empresas a cargo de estas plataformas establezcan adecuados mecanismos de seguridad en sus plataformas, y de prevención para detectar incluso si dentro de su empresa operan los ciberdelincuentes.

Nombre del entrevistado	Sello y firma

Guía de entrevista

Título: Proliferación de la ciberdelincuencia como afectación al bien jurídico del derecho a la identidad, Callao 2022
Entrevistado: Victor Hugo Montellanos Palomino.
Cargo/ Profesión/ Grado académico: Fiscal Penal –Abogado y Bachiller en Derecho.
Institución: Ministerio Público del Callao.

OBJETIVO GENERAL

Analizar la manera en que la proliferación de la ciberdelincuencia afecta el bien jurídico del derecho a la identidad, Callao 2022

1. Desde su punto de vista, ¿De qué manera la proliferación de la ciberdelincuencia afecta el bien jurídico del derecho a la identidad? Fundamente su respuesta.

   Partamos que el bien jurídico protegido en el este tipo de delitos se concibe en diversos planos de manera conjunta y concatenada; en el primero se encuentra la información de manera general (información almacenada, tratada y transmitida mediante los sistemas de tratamiento automatizado de datos), y en el segundo plano, los demás bienes afectados a través de este tipo de delitos como son la indemnidad sexual, intimidad, etc. Respecto de la información debe ser entendido como el contenido de las bases y/o bancos de datos o el producto de los procesos informáticos automatizados, por lo tanto, se constituye en un bien autónomo de valor económico. Es allí, la importancia del valor económico de la información lo que ha hecho que se incorpore como bien jurídico tutelado. Luego, este tipo de delitos considero que es un delito pluriofensivo, vulnerando varios bienes jurídicos, como la identidad, como el delito de suplantación a la identidad, para luego realizar otros delitos como podría bien ser los delitos de estafas.

OBJETIVO ESPECÍFICO 1

Describir el modo en que la caracterización actual de la ciberdelincuencia repercute en el derecho a la identidad, Callao 2022

2. ¿Conoce el modus operandi de los ciberdelincuentes que vulneran el derecho a la identidad mediante el uso de los recursos tecnológicos?

   Son muchos los delitos informáticos que se instrumentan a través de las nuevas tecnologías e Internet. Los ciberdelincuentes se valen de métodos como el *phising* (captar contraseñas o números de tarjetas de crédito imitando correos electrónicos de organismos u organizaciones oficiales), la monitorización de teclado, el *ciberbulling* (acoso escolar) o el *grooming* (ciberacoso sexual a menores) para conseguir sus objetivos. Entre otros métodos.

3. ¿Qué responsabilidad tienen los proveedores de servicios en línea y las plataformas digitales en la protección de la identidad personal de sus usuarios?.

   Creo que la responsabilidad de estas empresas o proveedores deben ser mas severas, llegando hasta sanciones de multas drásticas, ya que éstas son las que prestan el servicio a los usuarios y quienes deberían asumir algún tipo responsabilidad. Se deben de regular con más sus procedimientos, reglamentos y normas de estos proveedores.

4. ¿Considera que las penas establecidas en el ordenamiento jurídico penal deben incidir en la mitigación de la ciberdelincuencia en el Perú?

   ……..……Si, ya que como todo tipo de penas en el ordenamiento penal, tienen fines como el fin protector de bienes jurídicos; preventivo, es decir, la prevención general y especial de la norma penal; y, el fin resocializador. Así, considero que las penas en el orden penal deban incidir en atenuar la ciberdelincuencia, por lo que deben hacerse más severas, para cumplir los fines de la pena como se ha referido.

OBJETIVO ESPECÍFICO 2

Analizar la forma en que los fines de la pena ante la ciberdelincuencia incide en la mitigación de la misma.

5. Subraya los desafíos legales y éticos asociados con la recopilación y uso de información personal en el contexto de la ciberdelincuencia.

   Considero que las penas deben ser más severas para cumplir con los fines de la pena en el orden penal, como los fines de prevención (especial y general), protectora (de bienes jurídicos) y resocializadora, a fin de que el reo pueda volver a la vida en sociedad. Ello debe ir de la mano con los fines de la pena.

6. ¿Conoce las medidas legales y tecnológicas que existen en el Perú para prevenir y combatir la ciberdelincuencia que afecta la identidad personal?

   El Perú no ha sido ajeno a las desventajas que acarrea el mal uso de las TIC; frente a esta situación, ha habido esfuerzos interesantes respecto a su marco normativo en materia de tratamiento y el combate de la ciberdelincuencia, los que se han venido plasmando siguiendo las pautas que se desprenden del Convenio de Budapest, luego que el Congreso de la República lo aprobara en febrero del 2019. Cabe recordar como antecedente importante a la adhesión de nuestro país al aludido convenio, la primera versión del Código Penal (publicado hace más de 30 años), en el que ya se mostraba un primer intento en regular los actos ilícitos realizados a través de la tecnología, como fue el tipificar el hurto telemático. Adicionalmente, tenemos que en el año 2011 ya había sido publicada la Ley N°29733, Ley de Protección de Datos Personales, y en el 2013 la Ley Nº

30096, Ley de Delitos Informáticos, instrumento normativo que –entre otros puntos– describe las conductas delictivas que afectan los sistemas y datos informáticos, así como también las protecciones a las libertades civiles en el ámbito de las comunicaciones. En el 2014, esta ley fue complementada con su modificatoria, efectuada por medio de la Ley N° 30171. En igual contexto, en el Perú se ha continuado emitiendo normas de diferente naturaleza por parte de entidades de diferentes niveles y competencias. No obstante, aún existen marcados retos al respecto en aras de fortalecer el marco jurídico nacional existente sobre la materia, a la luz de los compromisos internacionales asumidos y a la propia realidad y necesidades, que demandan una urgente protección de los derechos de las personas, urgente e indispensable de acuerdo al aumento de denuncias por delitos informáticos que anualmente recibe la Policía Nacional.

La Ley de Delitos Informáticos –modificada extensamente por la Ley Nº 30171, publicada el 10 de marzo del 2014 para adecuar de mejor manera la descripción de sus conductas delictivas al Convenio de Budapest–33 establece cinco grandes grupos de ciberdelitos en función a los bienes jurídicos, a saber, los datos y los sistemas informáticos, la indemnidad y la libertad sexuales, la intimidad y el secreto de las comunicaciones, el patrimonio y, por último, la fe pública. Los ciberdelitos contra los datos y los sistemas informáticos comprenden el acceso ilícito, los atentados a la integridad de los datos informáticos y de los sistemas informáticos, y el abuso de mecanismos y dispositivos informáticos. El acceso ilícito (artículo 2º) es cometido por quien, deliberada e ilegítimamente, accede a todo o parte de un sistema informático, siempre que se realice con vulneración de medidas de seguridad establecidas o excediendo lo autorizado. El atentado a la integridad de los datos informáticos (artículo 3º) lo efectúa quien deliberada e ilegítimamente daña, introduce, borra, deteriora, altera, suprime o hace inaccesibles datos informáticos, que constituyen una representación de hechos, información o conceptos expresados de cualquier forma que se preste a tratamiento informático, incluidos los programas diseñados para que un sistema informático ejecute una función. El atentado contra la integridad de los sistemas informáticos (artículo 4º), conocido como sabotaje informático,34 lo realiza quien deliberada e ilegítimamente inutiliza, de manera total o parcial, un sistema informático, impide el acceso a este, entorpece o imposibilita su funcionamiento o la prestación de sus servicios; se entiende por sistema informático todo dispositivo o conjunto de dispositivos interconectados o relacionados entre sí, cuya función, o la de algunos de sus elementos, sea el tratamiento automatizado de datos en ejecución de un programa. yEl abuso de mecanismos y dispositivos informáticos (artículo 10º) es realizado por quien deliberada e ilegítimamente fabrica, diseña, desarrolla, vende, facilita, distribuye, importa u obtiene para su utilización uno o más mecanismos, programas informáticos, dispositivos, contraseñas, códigos de acceso o cualquier otro dato informático, específicamente diseñados para la comisión de los ciberdelitos; o por quien ofrece o presta servicio que contribuya a ese propósito.

7. ¿Cuál es la importancia del papel de las autoridades y organismos nacionales e internacionales en la lucha contra la ciberdelincuencia que afecta la identidad personal?

Considero que el papel y rol que tiene las autoridades y organismos ya sea nacional o internacional, es preponderante; en efecto, están las autoridades gubernamentales que

deben regular en estricto las acciones que deben tener los proveedores de servicios en línea o internet, dando protocolos y reglamentos más específicos para priorizar y evitar la vulneración de datos y no afectar la identidad de las personas; de otro lado, estan las autoridades de la administración de justicia que persiguen y sancionan los delitos de ciberdelincuencia (entre ellos las que afectan la identidad de las personas, como la suplantación de identidad, entre otros), buscando efectivizar sanciones penales mas ejemplares, conllevando asimismo, que éstas autoridades estén y tengan mayor logística y tecnología para identificar a los autores de estos delitos. Asimismo, esta la Policía Nacional como la Policía de Interpol, que conlleve a mejores coordinaciones e intercambios de información entre la policía en el mundo, en la lucha contra la ciberdelincuencia. También existen la División de Investigación de Delitos de Alta Tecnología, el Ministerio Público, la Unidad Fiscal Especializada en Ciberdelincuencia, la Oficina de Peritajes, la Cooperación Judicial Internacional, entre otros.

OBJETIVO ESPECÍFICO 3

Delimitar la manera en que la legislación peruana favorece a la ciberseguridad como antídoto a los delitos cibernéticos.

8. ¿Tiene pleno conocimiento del bien jurídico que protege el derecho a la identidad?

   Si, en estos tipos de delitos, al usar el sujeto activo, las tecnologías de la información , logran acceder y vulnerar la identidad de terceras personas, para luego obtener provecho que en general es patrimonial, los delincuentes informáticos realizan estos delitos, afectando la identidad de las personas, a efectos de cometer fraudes financieros como compras en línea, transferencias bancarias, etc; obtener datos de otras personas de manera ilegal; cometer ciberbullying o acoso virtual, hacer grooming o ganar la confianza de un menor y cometer abuso sexual contra éste, etc.

9. ¿Conoce las políticas y legislaciones existentes que protegen el derecho a la identidad personal y cómo se aplican en el Perú?

   En el Perú, la **Ley Nº 30096** rige los delitos asociados a la manipulación indebida de los softwares y hardwares, como base de datos, en perjuicio de los titulares de datos o de terceros. Mencionamos los delitos contenidos en la norma:

   - **Tráfico ilegal de datos.**

   Es el **delito que sanciona la creación, ingreso o utilización indebida a una base de datos sobre una persona natural o jurídica, identificada o identificable, para comercializar, traficar, vender, promover, favorecer o facilitar información relativa a cualquier ámbito de la esfera** personal, familiar, patrimonial, laboral, financiera u otro de naturaleza análoga, creando o no perjuicio, será reprimido con pena privativa de libertad no menor de tres ni mayor de cinco años.

   - **Interceptación de datos informáticos.**

Es el **delito que se configura por el uso de las tecnologías de la información o de la comunicación, con la finalidad de interceptar datos informáticos en transmisiones no públicas, dirigidas a un sistema informático**, originadas en un sistema informático o efectuadas dentro del mismo, incluidas las emisiones electromagnéticas provenientes de un sistema informático que transporte dichos datos informáticos, será reprimido con pena privativa de libertad no menor de tres ni mayor de seis años.

La pena privativa de libertad será no menor de cinco ni mayor de ocho años cuando el delito recaiga sobre información clasificada como secreta, reservada o confidencial de conformidad con las normas de la materia.

La pena privativa de libertad será no menor de ocho ni mayor de diez años cuando el delito comprometa la defensa, la seguridad o la soberanía nacionales.

- **Fraude informático**

Es el **delito que sanciona a toda persona que procura a través de las tecnologías de la información o de la comunicación**, un beneficio o provecho ilícito para sí o para otro en perjuicio de tercero mediante el diseño, introducción, alteración, borrado, supresión, clonación de datos informáticos o cualquier interferencia o manipulación en el funcionamiento de un sistema informático, será reprimido con una pena privativa de libertad no menor de tres ni mayor de ocho años y con sesenta a ciento veinte días multa.

La pena será privativa de libertad no menor de cinco ni mayor de diez años y de ochenta a ciento cuarenta días multa cuando se afecte el patrimonio del Estado destinado a fines asistenciales o a programas de apoyo social. (como bonos)

- **Suplantación de identidad**

Es el **delito que sanciona la suplantación de la identidad de una persona natural o jurídica mediante las tecnologías de la información o de la comunicación**, siempre que de dicha conducta resulte algún perjuicio, material o moral. La pena es prisión no menor de tres ni mayor de cinco años.

- **Abuso de mecanismos y dispositivos informáticos**

Este **delito sanciona la fabricación, diseño, desarrollo, venta, distribución, importación u obtención de programas, informáticos, dispositivos, contraseñas, códigos de acceso o cualquier otro dato informático**, específicamente diseñados para la comisión de los delitos previstos en la presente Ley, o el que ofrece o presta servicio que contribuya a ese propósito. La pena es no menor de un año ni mayor que cuatro y con treinta a noventa días multa.

También tenemos el Código Penal, en los delitos tipificados como suplantación de identidad y otros.

10. ¿Cuáles son los principales derechos asociados al derecho a la identidad personal y cómo se ven vulnerados por la ciberdelincuencia?

Existen conexidad para con otros derechos como el de la intimidad, el secreto de las comunicaciones, derechos intelectuales, contra la libertad personal, contra la tranquilidad pública, entre otros.

11. ¿Conoce las políticas y legislaciones existentes que protegen el derecho a la identidad personal ante la vulneración por medios cibernéticos?

    Marco Internacional tenemos: El Convenio sobre la Ciberdelincuencia del Consejo de Europa, los Protocolos adicionales al Covenio sobre Ciberdelincuencia de Europa, la Negociación de una convención internacional.
    Marco normativo Nacional: La respuesta penal inicial, la Ley de Delitos Informáticos, etc.

12. ¿Cuáles son los derechos y responsabilidades de los individuos en la protección de su propia identidad personal frente a la ciberdelincuencia?

    En cuando a una responsabilidad debemos tener en cuenta que en el derecho penal, en cuanto al individuo (sujeto pasivo) cabe en algunas oportunidades la imputación a la víctima, cuando no toma precauciones que hacen consumar el delito en su agravio. Sin embargo, más allá de ello, las personas en general deben tomar ciertas precauciones como:

    - Navegar solo por páginas web seguras y de confianza, especialmente si estás realizando compras online o brindando información confidencial. Verifica que la URL comience con https:// en lugar de http. Además, en la barra del navegador debe aparecer el ícono de un candado cerrado.

    - Tener cuidado con los correos electrónicos en los que las entidades bancarias o sitios de venta soliciten datos personales o contraseñas.

    - Cuando se reciba alguna solicitud de amistad en las redes sociales, confirma siempre la identidad de la cuenta antes de aceptar.

    - Usar contraseñas seguras, que estén compuestas por al menos ocho caracteres como mínimo y combinen distintos tipos de letras, entre mayúsculas y minúsculas, además de números y símbolos. No es recomendable usar la misma contraseña en todas tus cuentas.

13. ¿Cuáles son las estrategias legales y sociales se pueden implementar para prevenir y abordar la vulneración del derecho a la identidad personal?

    Al Congreso de la República Aprobar el marco legal que permita exigir responsabilidad a las personas jurídicas en materia de ciberdelitos, conforme a los alcances del artículo 12 del Convenio sobre Ciberdelincuencia del Consejo de Europa. Establecer una normativa

que posibilite la conservación rápida de datos almacenados por medio de sistemas informáticos, conforme a los alcances del artículo 29° del Convenio sobre Ciberdelincuencia del Consejo de Europa.

Al Ministerio del Interior: Evaluar –en coordinación con la Comandancia General de la PNP– la modificación de la estructura orgánica de la Policía, con el fin de elevar la Divindat–PNP al nivel de Dirección, dependiente de la Dirección Nacional de Investigación Criminal. Asimismo, modificar su denominación por Dirección contra la Ciberdelincuencia, constituyéndose así como un órgano especializado, de carácter técnico y sistémico, normativo y operativo en materia de ciberdelincuencia, con competencia a nivel nacional.

Al Ministerio de Relaciones Exteriores Promover la adhesión, aprobación y ratificación, por parte del Estado peruano, de los dos protocolos adicionales al Convenio sobre la Ciberdelincuencia del Consejo de Europa, referidos a la criminalización de las conductas de carácter racista y xenófoba cometidas a través de los sistemas informáticos (2003), y a la mejora de la cooperación y la divulgación de las pruebas electrónicas (2022).

Al Poder Judicial Evaluar la implementación de un subsistema de justicia especializado en ciberdelincuencia, con personal debidamente capacitado, para conocer casos sobre delitos informáticos y otros que se realizan con el uso de las tecnologías de la información y las comunicaciones.

Al Instituto Nacional de Estadística e Informática Elaborar –sobre la base de los registros administrativos de denuncias de la Policía Nacional y del Ministerio Público– estadística oficial de los ciberdelitos e incorporarla como una sección específica y permanente en el Sistema Integrado de Estadísticas de la Criminalidad y Seguridad Ciudadana (DATA-CRIM), así como en sus correspondientes informes y boletines técnicos periódicos. La presentación de la estadística de las denuncias debería acompañarse de su distribución geográfica y su caracterización.

……..……
……..……
……..……
……..……
……..

Firma Digital

Firmado digitalmente por MONTELLANOS PALOMINO Victor Hugo FAU 20131370301 soft
Motivo: Soy el autor del documento
Fecha: 10.06.2023 09:17:28 -05:00

Firmado digitalmente por MONTELLANOS PALOMINO Victor Hugo FAU 20131370301 soft
Motivo: Soy el autor del documento
Fecha: 10.06.2023 09:17:38 -05:00

Nombre del entrevistado	Sello y firma

Guía de entrevista

Título: Título: Proliferación de la ciberdelincuencia como afectación al bien jurídico del derecho a la identidad, Callao 2022
Entrevistado: JESUS DANIEL BALVIN ARBULU
Cargo/ Profesión/ Grado académico: ABOGADO
Institución: MINISTERIO PUBLICO CALLAO

OBJETIVO GENERAL

Analizar la manera en que la proliferación de la ciberdelincuencia afecta el bien jurídico del derecho a la identidad, Callao 2022

1. **Desde su punto de vista, ¿De qué manera la proliferación de la ciberdelincuencia afecta el bien jurídico del derecho a la identidad? Fundamente su respuesta.**
   El Ámbito digital ha permitido la comunicación por medio del anonimato, la falsedad de información y la carencia de relaciones humanas físicamente. Esto ha servido de nicho para la delincuente, que ve una oportunidad sencilla de poder fraguar identidades falsas como medio o instrumento para cometer sus fines ilícitos

OBJETIVO ESPECÍFICO 1

Describir el modo en que la caracterización actual de la ciberdelincuencia repercute en el derecho a la identidad, Callao 2022

2. **¿Conoce el modus operandi de los ciberdelincuentes que vulneran el derecho a la identidad mediante el uso de los recursos tecnológicos?**
   Se pueden realizar diversas actividades delictivas, como la suplantación de identidad, creación de cuentas bancarias o líneas de celulares. Por otro lado, también existen modalidades de manipulación digital, con el uso de software malicioso, para obtener los datos de las tarjetas de crédito, contraseñas y fecha de vencimiento para efectuar consumos no reconocidos. O bajo la remisión de correos falsos, en los que se solicitan datos del propio usuario para que estos mismas dispongan de dinero.

3. **¿Qué responsabilidad tienen los proveedores de servicios en línea y las plataformas digitales en la protección de la identidad personal de sus usuarios?**
   Podría encuadrarse en el delito de acceso ilícito (artículo 2° de la Ley 30096) "quien, deliberada e ilegítimamente, accede a todo o parte de un sistema informático, siempre que se realice con vulneración de medidas de seguridad establecidas o excediendo lo autorizado". Sin embargo, no es clara la figura, por lo que considero que dicha situación todavía encuentra grandes vacíos de protección y sanción.

4. **¿Considera que las penas establecidas en el ordenamiento jurídico penal deben incidir en la mitigación de la ciberdelincuencia en el Perú?**
   Claro que sí, es un enfoque que ya se ha iniciado hace varios años; sin embargo, la logística y la normativa se ha estancado, mientras que las modalidades delictivas desbordan y se incrementan al mismo tiempo que la tecnología avanza.

OBJETIVO ESPECÍFICO 2

Analizar la forma en que los fines de la pena ante la ciberdelincuencia incide en la mitigación de la misma.

5. **Subraya los desafíos legales y éticos asociados con la recopilación y uso de información personal en el contexto de la ciberdelincuencia.**
   Desde la perspectiva jurídica, establecer responsabilidades es muy complicado, cuando hablamos de ciberdelincuencia, pues los autores podrían encontrarse en cualquier parte del mundo. En el ámbito ético, tratar de maximizar el control de datos y comunicaciones en internet puede atentar contra a la intimidad de los usuarios, es difícil establecer o comprender los límites de un lado y el otro.

6. **¿Conoce las medidas legales y tecnológicas que existen en el Perú para prevenir y combatir la ciberdelincuencia que afecta la identidad personal?**
   Conozco la Ley 30096 – ley de delitos informáticos. Además, el Decreto Legislativo Nº 1412-2018 como parte de las políticas públicas del Estado.

7. **¿Cuál es la importancia del papel de las autoridades y organismos nacionales e internacionales en la lucha contra la ciberdelincuencia que afecta la identidad personal?**
   El papel de los tratados y convenios internaciones han sido la base de la lucha contra la ciberdelincuencia, son el cimiento que dio paso a la legislación nacional, como lo son el Convenio de Budapest y los protocolos adicionales. Ya en Perú, se ha ido legislando sobre los delitos informáticos y políticas de estado para desarrollar, fomentar y proteger el uso de la tecnología, la identidad y el gobierno digital.

OBJETIVO ESPECÍFICO 3

Delimitar la manera en que la legislación peruana favorece a la ciberseguridad como antídoto a los delitos cibernéticos.

8. **¿Tiene pleno conocimiento del bien jurídico que protege el derecho a la identidad?**
   El derecho a la identidad es el conjunto de atribuciones y características que permiten individualizar a la persona, le permite auto percibirse conscientemente único y distinto a otro y que los demás la reconozcan como tal.

9. **¿Conoce las políticas y legislaciones existentes que protegen el derecho a la identidad personal y cómo se aplican en el Perú?**
   El estado peruano ha lanzado diversos mecanismos para digitalizar las instituciones y fomentar el uso de los medios digitales, a través de lo que se denomina la gobernanza de datos o gobierno digital, lo que se evidencia en el Decreto Legislativo Nº 1412-2018

10. **¿Cuáles son los principales derechos asociados al derecho a la identidad personal y cómo se ven vulnerados por la ciberdelincuencia?**
    El derecho a la identidad, está relacionado con la propia autodeterminación de la personas y por lo tanto, vinculación directa con la dignidad humana

11. **¿Conoce las políticas y legislaciones existentes que protegen el derecho a la identidad personal ante la vulneración por medios cibernéticos?**
    Se puede entender, que se encarga la Ley 30096 – ley de delitos informáticos. También se han creado Unidades de especialización tanto a nivel judicial, fiscal y policial para investigar estos tipos de delitos.

12. **¿Cuáles son los derechos y responsabilidades de los individuos en la protección de su propia identidad personal frente a la ciberdelincuencia?**
    Toda persona debe tener el derecho a que la información que proporciona en el mundo digital no deba ser manipulada ni usada para fines diferentes a su propósito. En la otra arista, se tiene el deber de proporcionar los datos verdaderos cuando así corresponda con la exigencia de la información solicitada, en un contexto determinado, siendo que la vulneración de ello genere una responsabilidad administrativa o penal, según sea el caso.

13. **¿Cuáles son las estrategias legales y sociales se pueden implementar para prevenir y abordar la vulneración del derecho a la identidad personal?**
    Legalmente, se debe plantear y reforzar los equipos de lucha contra los delitos de ciberdelincuencia, porque actualmente se encuentra en una situación precaria. Para prevenir, se deben implementar normas de mayor protección de los datos e información de los usuarios en el mundo digital. Como medidas sociales, sensibilizar a la población con proyectos de educación en uso responsable de la información de datos y como evitar caer en delitos cibernéticos.

Nombre del entrevistado	Sello y firma
JESÚS DANIEL BALVÍN ARBULÚ	Jesús Daniel Balvín Arbulú Fiscal Adjunto Provincial (P) Distrito Fiscal del Callao

Guía de entrevista

Título: Proliferación de la ciberdelincuencia como afectación al bien jurídico del derecho a la identidad, Callao 2022
Entrevistado: José Luis Morales Yataco
Cargo/ Profesión/ Grado académico: Fiscal Adjunto Provincial
Institución: Ministerio Público – Distrito Fiscal del Callao

OBJETIVO GENERAL

Analizar la manera en que la proliferación de la ciberdelincuencia afecta el bien jurídico del derecho a la identidad, Callao 2022

1. Desde su punto de vista, ¿De qué manera la proliferación de la ciberdelincuencia afecta el bien jurídico del derecho a la identidad? Fundamente su respuesta.
   En principio considero que la ciberdelincuencia, como actividad ilícita, afecta una gran variedad de bienes jurídicos protegidos; entre ellos, la afectación al derecho a la identidad, puesto que, entre las diversas formas de materializar los actos delictivos, el delincuente utiliza las herramientas y sus conocimientos tecnológicos para vulnerar mecanismos de seguridad, lo cual implica su intromisión en la esfera privada de la víctima. En consecuencia, en muchos casos, el delincuente empieza por vulnerar el derecho a la identidad de la víctima, ya sea suplantando su identidad o afectando su intimidad, dependiendo del propósito final que se ha propuesto realizar.

OBJETIVO ESPECÍFICO 1

Describir el modo en que la caracterización actual de la ciberdelincuencia repercute en el derecho a la identidad, Callao 2022

2. ¿Conoce el modus operandi de los ciberdelincuentes que vulneran el derecho a la identidad mediante el uso de los recursos tecnológicos?

   De acuerdo a la casuística, al igual que lo antes referido, las modalidades también son diversas, pero por lo general, se materializa vulnerando las medidas de seguridad de las personas a través de su acceso a las redes sociales, y así obtener el máximo de información para vulnerar en otros ámbitos relacionados con la intimidad y su patrimonio.

3. ¿Qué responsabilidad tienen los proveedores de servicios en línea y las plataformas digitales en la protección de la identidad personal de sus usuarios?
   Entiendo que esta pregunta esta estrechamente relacionada con la protección de datos personales. En la actualidad, sin darnos cuenta, la ciudadanía acepta algunos términos encubiertos (en letras pequeñas) o autoriza que cualquier entidad privada (sea que brinde bienes y servicios) pueda tener acceso a información valiosa de las personas; si bien es

cierto, esta información tiene fines de mercadotecnia o marketing, en malas manos, trae como consecuencia la comisión de diversos delitos. En ese sentido, considero que estos proveedores de servicios tienen una alta responsabilidad; sin embargo, como ya se ha indicado, será responsabilidad de la ciudadanía, a quienes debe proporcionar o confiar esta información.

4. ¿Considera que las penas establecidas en el ordenamiento jurídico penal deben incidir en la mitigación de la ciberdelincuencia en el Perú?

   Entendiendo el término mitigar como atenuar, considero que la penalización de todo delito siempre buscará atenuar o disminuir aquellos factores que tienen que ver con sus causas. No obstante, deberá tenerse en cuenta, o quizás, no olvidar que el avance tecnológico también permite la aparición de nuevas formas delictivas.

OBJETIVO ESPECÍFICO 2

Analizar la forma en que los fines de la pena ante la ciberdelincuencia incide en la mitigación de la misma.

5. Subraya los desafíos legales y éticos asociados con la recopilación y uso de información personal en el contexto de la ciberdelincuencia.

   Definitivamente, considero que el tema axiológico es la base fundamental en toda actividad humana, precisamente la aplicación de los valores en nuestra formación como sociedad permite que aún se mantenga cierto orden y bienestar; sin embargo, en la actualidad, cada vez más nos alejamos de los parámetros éticos que toda institución pública o privada debería demostrar; en ese sentido, aquellas entidades deberán replantear sus protocolos o objetivos en el uso de la información.

6. ¿Conoce las medidas legales y tecnológicas que existen en el Perú para prevenir y combatir la ciberdelincuencia que afecta la identidad personal?

   Sí, existen muchas medidas legales que los diversos órganos estatales aplican para prevenir y combatir modalidad delictiva.

7. ¿Cuál es la importancia del papel de las autoridades y organismos nacionales e internacionales en la lucha contra la ciberdelincuencia que afecta la identidad personal?

   Estas entidades tienen una gran responsabilidad en cuanto a la prevención y lucha contra la ciberdelincuencia, ya que éstas son las que fijan y establecen estrategias destinadas a poner en marcha los planes de acción para estos fines.

OBJETIVO ESPECÍFICO 3

Delimitar la manera en que la legislación peruana favorece a la ciberseguridad como antídoto a los delitos cibernéticos.

8. ¿Tiene pleno conocimiento del bien jurídico que protege el derecho a la identidad?

   Toda persona tiene derecho a un nombre desde que nace, ello implica su individualización frente al resto de la sociedad y por tanto es deber del Estado garantizar el libre desarrollo de su personalidad. Vulnerar o atentar contra este derecho humano, es afectar este bien jurídico protegido.

9. ¿Conoce las políticas y legislaciones existentes que protegen el derecho a la identidad personal y cómo se aplican en el Perú?

   El marco normativo sobre la materia es muy extenso, entre ellas nuestra carta fundamental, la que además se protege a través de las garantías constitucionales, como el hábeas corpus, y otras vinculadas con el ordenamiento jurídico internacional.

10. ¿Cuáles son los principales derechos asociados al derecho a la identidad personal y cómo se ven vulnerados por la ciberdelincuencia?

    Por ejemplo a la intimidad, a la inviolabilidad de sus comunicaciones y documentos privados que, como ya se ha mencionado, estos derechos son vulnerados mediante el uso indebido de la información personal, con diversos fines de naturaleza delictiva.

11. ¿Conoce las políticas y legislaciones existentes que protegen el derecho a la identidad personal ante la vulneración por medios cibernéticos?

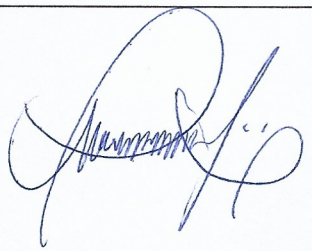
    Dentro de la política criminal que adopta el Estado para combatir éste y otros tipos de delito, la que va de la mano con nuestra legislación penal y de protección de la información, reafirmo cierto conocimiento sobre la materia, mencionado que como otras conductas delictivas, se van modificando según el avance tecnológico y las diversas formas delictiva que van apareciendo en la sociedad.

12. ¿Cuáles son los derechos y responsabilidades de los individuos en la protección de su propia identidad personal frente a la ciberdelincuencia?

    Resalto que toda persona tiene gran responsabilidad en el manejo y exposición de su propia información. Mi recomendación va para el gran sector de la ciudadanía que opta por exponer de manera innecesaria aquellos ámbitos personales y familiares de su vida cotidiana, información valiosa que la delincuencia común y organizada sabe aprovechar.

13. ¿Cuáles son las estrategias legales y sociales se pueden implementar para prevenir y abordar la vulneración del derecho a la identidad personal?

Considero que las estrategias legales están dadas, sin embargo, estas no generarán ningún resultado si la ciudadanía no toma conciencia en el manejo o sobreexposición de su propia información.

Nombre del entrevistado	**Sello y firma**
José Luis Morales Yataco	

Guía de entrevista

Título: Proliferación de la ciberdelincuencia como afectación al bien jurídico del derecho a la identidad, Callao 2022
Entrevistado: JOSSELINE MACBETH PURIZACA ZETA
Cargo/ Profesión/ Grado académico: FISCAL PROVINCIAL – ABOGADO **-** MAESTRO EN DERECHO PENAL
Institución: MINISTERIO PÚBLICO – FISCALIA DE LA NACIÓN.

OBJETIVO GENERAL

Analizar la manera en que la proliferación de la ciberdelincuencia afecta el bien jurídico del derecho a la identidad, Callao 2022

1. Desde su punto de vista, ¿De qué manera la proliferación de la ciberdelincuencia afecta el bien jurídico del derecho a la identidad? Fundamente su respuesta.

Con respecto a la proliferación de los delitos de Ciberdelincuencia, este vendría afectando directamente el derecho a la identidad, toda vez que desde que se hace uso de las tecnologías de la información para hacerse pasar por otra persona o institución, y perjudicarla de forma material o moral, afectando su identidad para hacer uso de la misma y acceder sus cuentas o sistema financiero con la finalidad de afectar su patrimonio, este solo hecho llega a ocasionar desde simples molestias en la víctima, hasta serios problemas legales, grandes pérdidas económicas, así como afectar negativamente su reputación o imagen social.

OBJETIVO ESPECÍFICO 1

Describir el modo en que la caracterización actual de la ciberdelincuencia repercute en el derecho a la identidad, Callao 2022

2. ¿Conoce el modus operandi de los ciberdelincuentes que vulneran el derecho a la identidad mediante el uso de los recursos tecnológicos?

   En la actualidad se vienen desarrollando diversas modalidades para vulnerar el derecho a la identidad, mediante diversos recursos tecnológicos, los cuales permiten ingresar a los datos de las personas y desarrollar el fraude, el más común ahora resulta los correos electrónicos donde les piden ingresar sus datos a fin de acceder a un crédito, es en ese momento donde acceden a toda la información a través del acceso que le brindan los mismos ciudadanos vulnerando su derecho a la identidad al suplantar la misma.

3. ¿Qué responsabilidad tienen los proveedores de servicios en línea y las plataformas digitales en la protección de la identidad personal de sus usuarios?

En definitiva, los servicios en línea y las plataformas digitales, son responsable al no contar con sistemas de protección de la identidad personal de los usuarios, ya que no implementan mecanismos que sean inquebrantables por los inescrupulosos que acceden de manera ilegal a la información de los usuarios.

4. ¿Considera que las penas establecidas en el ordenamiento jurídico penal deben incidir en la mitigación de la ciberdelincuencia en el Perú?

   En la actualidad las penas como efecto sancionador no estarían surtiendo el efecto para el cual estaría destinados, ya que por mas penas altas que se apliquen no se logra mitigar la comisión de dichos ilícitos, a lo que se concluye que no parte por el tema del quantum de la pena, si no que debe de aplicarse mejores mecanismos que eviten la comisión de dichos ilícitos penales, como acciones preventivas.

OBJETIVO ESPECÍFICO 2

Analizar la forma en que los fines de la pena ante la ciberdelincuencia incide en la mitigación de la misma.

5. Subraya los desafíos legales y éticos asociados con la recopilación y uso de información personal en el contexto de la ciberdelincuencia.

   Existen varios desafíos siendo los más resaltantes la normatividad aplicable, reforzar los mecanismos de seguridad frente a la ciberdelincuencia.

6. ¿Conoce las medidas legales y tecnológicas que existen en el Perú para prevenir y combatir la ciberdelincuencia que afecta la identidad personal?

   Si, en la actualidad ya que se vienen implementando diferentes medidas legales y tecnológicas para prevenir y combatir la ciberdelincuencia, con la finalidad de proteger la identidad personal, pero no están siendo suficientes para poder evitar su vulneración. De esta forma, diferentes países, como el Perú, vienen adecuando progresivamente su legislación en concordancia con la normatividad internacional, con el objeto de prevenir, investigar y sancionar esta clase de actos ilícitos y a sus responsables. La producción normativa abarca la regulación de diferentes asuntos, como es, el uso de las tecnologías de la información y comunicación, las medidas a implementarse para cautelar y proteger los datos y sistemas informáticos, la tipificación penal de actos y conductas delictivas y los procedimientos a seguir por las autoridades que resulten competentes al respecto, para perseguir y sancionar de forma eficaz a quienes delinquen en el ciberespacio.

7. ¿Cuál es la importancia del papel de las autoridades y organismos nacionales e internacionales en la lucha contra la ciberdelincuencia que afecta la identidad personal?

El papel que representa las autoridades y los organismos internacionales resulta ser fundamental ya que permite realizar diversos convenios que contribuyan al acceso de avances tecnológicos que permitan minimizar los riesgos en cuanto a los delitos que se cometen el en ciberespacio. La extensión rápida de este fenómeno a nivel global ha ido obligando a los Estados a elaborar sus propios diagnósticos situacionales para conocer y observar sus causas e impactos en los derechos, seguridad y economía de la ciudadanía. En algunos países la atención y tratamiento de esta problemática se ha dado con mayor énfasis y forma parte de sus políticas públicas, lo que ha generado que se promuevan y dicten disposiciones normativas de distinta índole, en armonía con lo señalado en el Convenio de Budapest.

OBJETIVO ESPECÍFICO 3

Delimitar la manera en que la legislación peruana favorece a la ciberseguridad como antídoto a los delitos cibernéticos.

8. ¿Tiene pleno conocimiento del bien jurídico que protege el derecho a la identidad?

   Si, se protege el derecho a la identidad personal (tratamiento de datos), también el patrimonio.

9. ¿Conoce las políticas y legislaciones existentes que protegen el derecho a la identidad personal y cómo se aplican en el Perú?

   Se tiene que en el año 2011, se publicó la Ley N°29733, Ley de Protección de Datos Personales, y en el 2013 la Ley Nº 30096, Ley de Delitos Informáticos, instrumento normativo que describe las conductas delictivas que afectan los sistemas y datos informáticos, así como también las protecciones a las libertades civiles en el ámbito de las comunicaciones. En el 2014, esta ley fue complementada con su modificatoria, efectuada por medio de la Ley N° 30171.

   En igual contexto, en el Perú se ha ido emitiendo normas de diferente naturaleza por parte de entidades de diferentes niveles y competencias. No obstante, aún existen marcados retos al respecto en aras de fortalecer el marco jurídico nacional existente sobre la materia, a la luz de los compromisos internacionales asumidos y a la propia realidad y necesidades, que demandan una urgente protección de los derechos de las personas, urgente e indispensable de acuerdo al aumento de denuncias por delitos informáticos que anualmente recibe la Policía Nacional.

10. ¿Cuáles son los principales derechos asociados al derecho a la identidad personal y cómo se ven vulnerados por la ciberdelincuencia?

    Uno de los principales derechos es el de la intimidad, el cual es inherente a todo ser humano, por cuanto implica la facultad que tiene una persona de reservar para

sí y excluir del conocimiento público de terceros, ciertos aspectos personales que a su criterio no deben ser revelados. Este derecho es bastante amplio ya que lleva dentro de sí elementos personales que, de acuerdo a su naturaleza, deben mantenerse en secreto y ahora con los delitos de ciberdelincuencia se han visto vulnerados.

11. ¿Conoce las políticas y legislaciones existentes que protegen el derecho a la identidad personal ante la vulneración por medios cibernéticos?

    La Ley N°29733, Ley de Protección de Datos Personales,
    La Ley Nº 30096, Ley de Delitos Informáticos, instrumento normativo que describe las conductas delictivas que afectan los sistemas y datos informáticos, así como también las protecciones a las libertades civiles en el ámbito de las comunicaciones.
    En el 2014, esta ley fue complementada con su modificatoria, efectuada por medio de la Ley N° 30171.

12. ¿Cuáles son los derechos y responsabilidades de los individuos en la protección de su propia identidad personal frente a la ciberdelincuencia?

    Cada individuo tiene derechos y responsabilidades frente a la protección de los datos de su propia identidad frente a los delitos de ciberdelincuencia, los cuales se encuentran protegidos por la normatividad vigente, y así también tiene la responsabilidad de no compartir su información y ser responsable con el uso de la misma a fin de evitar sea vulnerada.

13. ¿Cuáles son las estrategias legales y sociales se pueden implementar para prevenir y abordar la vulneración del derecho a la identidad personal?

    Si bien las ventajas de las tecnologías de la información y las comunicaciones son innegables, el incremento del uso de internet durante los últimos años ha generado un escenario que es aprovechado por la ciberdelincuencia, ocasionando agravio a las personas. Esta situación se agrava por el desconocimiento de algunas personas sobre el manejo y resguardo de los datos personales. Se deben de implementar mayores mecanismos de seguridad, que disminuyan la vulnerabilidad de datos personales.

Nombre del entrevistado	Sello y firma
JOSSELINE MACBETH PURIZACA ZETA	

Guía de entrevista

Título: Proliferación de la ciberdelincuencia como afectación al bien jurídico del derecho a la identidad, Callao 2022
Entrevistado: María Lizbet Benites Cuadros
Cargo/ Profesión/ Grado académico: Fiscal Provincial
Institución: Ministerio Público

OBJETIVO GENERAL

Analizar la manera en que la proliferación de la ciberdelincuencia afecta el bien jurídico del derecho a la identidad, Callao 2022

1. Desde su punto de vista, ¿De qué manera la proliferación de la ciberdelincuencia afecta el bien jurídico del derecho a la identidad? Fundamente su respuesta.
   El bien jurídico en los delitos de ciberdelincuencia es la protección a la información, esto es, a la confidencialidad, integridad, disponibilidad de la información y los sistemas informáticos, donde este se encuentre almacenada (entidades bancarias, empresas de telefonía, etc), por ende al vulnerar dicho bien jurídico afecta a la identidad de las personas a quienes le pertenece dicha información, dado a que en muchas ocasiones no solo usas sus datos para hacer alguna transferencia a compras, sino que también usan sus nombres antes terceros (se identifican), para estafar a otras personas, resultando perjudicada el dueño de dicha identidad.

OBJETIVO ESPECÍFICO 1

Describir el modo en que la caracterización actual de la ciberdelincuencia repercute en el derecho a la identidad, Callao 2022

2. ¿Conoce el modus operandi de los ciberdelincuentes que vulneran el derecho a la identidad mediante el uso de los recursos tecnológicos?

   De los casos que he tenido conocimiento y han sido los más frecuentes son, cuando los delincuentes utilizan el DNI de una persona, que previamente, de manera ingeniosa logran obtenerlo (simulando compras o ventas por internet) y una vez que tiene dicha imagen, lo utilizan para estafar a otras personas (presuntas compras y ventas de productos), ello con el fin de no ser identificados.

   Otra modalidad que se está dando, es cuando sustraen teléfonos celulares, lo utilizan para escribirles a los contactos del dueño del celular y solicitarle préstamo de dinero, ya sea por transferencia o yape, logrando despojar a esas personas de su patrimonio (dinero).

MARÍA LIZBET BENITES CUADROS
Fiscal Provincial Penal
10° Fiscalía Provincial Corporativa Penal
4° Despacho - Distrito Fiscal del Callao

3. ¿Qué responsabilidad tienen los proveedores de servicios en línea y las plataformas digitales en la protección de la identidad personal de sus usuarios?
   Hasta la fecha no ha sido posible consignar alguna empresa como responsable y/o tercero civilmente responsable, toda vez que, en los casos de los entidades bancarias, precisan que el usuario para las compras o transferencias han utilizado su clave secreta, la cual no debe ser compartida con terceras personas, y lamentablemente, los agraviados han sido de tal manera "sorprendidos" que han proporcionado sus datos sensibles (claves) a los delincuentes en la creencia que son trabajadores de las entidades bancarias.

4. ¿Considera que las penas establecidas en el ordenamiento jurídico penal deben incidir en la mitigación de la ciberdelincuencia en el Perú?

   En mi opinión las penas pueden servir para sancionar el comportamiento de los que delinquen en estos tipos de delitos, pero lo que de debe hacer es concientizar a la población sobre el uso debido de los sitios web donde ofrecen productos o donde ofrecen ellos productos, debiendo usar páginas confiables; del cuidado y reserva de sus claves que les otorgan las entidades financieras. A mi parecer no es solo endurecer penas sino que la población no contribuya a la realización de dicha conducta delictiva, que con mucha frecuencia se dan en estos casos, exponiendo incluso su identidad.

OBJETIVO ESPECÍFICO 2

Analizar la forma en que los fines de la pena ante la ciberdelincuencia incide en la mitigación de la misma.

5. Subraya los desafíos legales y éticos asociados con la recopilación y uso de información personal en el contexto de la ciberdelincuencia.
   Considero que las penas deben ser más severas para cumplir con los fines de la pena en el orden penal, como los fines de prevención (especial y general), protectora (de bienes jurídicos) y resocializadora, a fin de que el reo pueda volver a la vida en sociedad. Ello debe ir de la mano con los fines de la pena.

6. ¿Conoce las medidas legales y tecnológicas que existen en el Perú para prevenir y combatir la ciberdelincuencia que afecta la identidad personal?
   El atentado a la integridad de los datos informáticos (artículo 3º) lo efectúa quien deliberada e ilegítimamente daña, introduce, borra, deteriora, altera, suprime o hace inaccesibles datos informáticos, que constituyen una representación de hechos, información o conceptos expresados de cualquier forma que se preste a tratamiento informático, incluidos los programas diseñados para que un sistema informático ejecute una función. El atentado contra la integridad de los sistemas informáticos (artículo 4º), conocido como sabotaje informático,34 lo realiza quien deliberada e ilegítimamente inutiliza, de manera total o parcial, un sistema informático, impide el acceso a este, entorpece o imposibilita su funcionamiento o la prestación de sus servicios; se

MARIA LIZBET BENITES CUADROS
Fiscal Provincial Penal
10° Fiscalia Provincial Corporativa Penal
4° Despacho - Distrito Fiscal del Callao

entiende por sistema informático todo dispositivo o conjunto de dispositivos interconectados o relacionados entre sí, cuya función, o la de algunos de sus elementos, sea el tratamiento automatizado de datos en ejecución de un programa. yEl abuso de mecanismos y dispositivos informáticos (artículo 10º) es realizado por quien deliberada e ilegítimamente fabrica, diseña, desarrolla, vende, facilita, distribuye, importa u obtiene para su utilización uno o más mecanismos, programas informáticos, dispositivos, contraseñas, códigos de acceso o cualquier otro dato informático, específicamente diseñados para la comisión de los ciberdelitos; o por quien ofrece o presta servicio que contribuya a ese propósito

7. ¿Cuál es la importancia del papel de las autoridades y organismos nacionales e internacionales en la lucha contra la ciberdelincuencia que afecta la identidad personal?
En mi opinión el papel y rol que tiene las autoridades y organismos ya sea nacional o internacional, es preponderante; en efecto, están las autoridades gubernamentales que deben regular en estricto las acciones que deben tener los proveedores de servicios en línea o internet, dando protocolos y reglamentos más específicos para priorizar y evitar la vulneración de datos y no afectar la identidad de las personas; de otro lado, estan las autoridades de la administración de justicia que persiguen y sancionan los delitos de ciberdelincuencia (entre ellos las que afectan la identidad de las personas, como la suplantación de identidad, entre otros), buscando efectivizar sanciones penales mas ejemplares, conllevando asimismo, que éstas autoridades estén y tengan mayor logística y tecnología para identificar a los autores de estos delitos.

OBJETIVO ESPECÍFICO 3

Delimitar la manera en que la legislación peruana favorece a la ciberseguridad como antídoto a los delitos cibernéticos.

8. ¿Tiene pleno conocimiento del bien jurídico que protege el derecho a la identidad?

   El bien jurídico protegido serían sus datos personales.

9. ¿Conoce las políticas y legislaciones existentes que protegen el derecho a la identidad personal y cómo se aplican en el Perú?

   Existe la Ley 30096 – Ley de Delitos Informáticos, que tiene por objeto prevenir y sancionar las conductas ilícitas que afectan los sistemas y datos informáticos. Los ciberdelitos contra los datos y los sistemas informáticos comprenden el acceso ilícito, los atentados a la integridad de los datos informáticos y de los sistemas informáticos, y el abuso de mecanismos y dispositivos informáticos. El acceso ilícito (artículo 2º) es cometido por quien, deliberada e ilegítimamente, accede a todo o parte de un sistema informático, siempre que se realice con vulneración de medidas de seguridad establecidas o excediendo lo autorizado.¿Cuáles son los principales derechos asociados al derecho a la identidad personal y cómo se ven vulnerados por la ciberdelincuencia?

MARIA LIZBET BENITES CUADROS
Fiscal Provincial Penal
10° Fiscalia Provincial Corporativa Penal
4° Despacho - Distrito Fiscal del Callao

Los derechos asociados al derecho a la identidad, son el derecho a su nombre, nacionalidad, y con ello sus derechos básicos a la salud, educación.

10. ¿Conoce las políticas y legislaciones existentes que protegen el derecho a la identidad personal ante la vulneración por medios cibernéticos?
    En el Perú se tiene la norma legal 30096, que regula todos los delitos de ciberdelincuencia que se presentan en la sociedad.

11. ¿Cuáles son los derechos y responsabilidades de los individuos en la protección de su propia identidad personal frente a la ciberdelincuencia?

    El derecho de una persona en la protección de su identidad en este tipo de delitos, es que las entidades bancarias y telefonías sean más recelosos en los accesos o permisos para poder realizar compras o transferencias vía internet.
    Y las responsabilidades de los usuarios es que al momento de usar las redes sociales o páginas de internet, utilicen una red confiable, accedan a enlaces originales y comprueben la seguridad, tener claves fortalecidas, no usar claves como fecha de nacimiento o que sean sencillas de acceder, optar por múltiples opciones de validación en las cuentas virtuales, instalar a sus dispositivos antivirus.

12. ¿Cuáles son las estrategias legales y sociales se pueden implementar para prevenir y abordar la vulneración del derecho a la identidad personal?
    Difundir con mayor frecuencia las alertas a la población sobre el uso de las redes para realizar alguna operación.

Nombre del entrevistado	Sello y firma
Maria Lizbet Benites Cuadros	MARIA LIZBET BENITES CUADROS Fiscal Provincial Penal 10° Fiscalía Provincial Corporativa Penal 4° Despacho - Distrito Fiscal del Callao