REVISTA JURÍDICA DE LA FACULTAD DE DERECHO Y CIENCIAS SOCIALES | UNT
ISSN : 3072 - 8169 | VOL. 1, NÚM. 1, AÑO 2025

Ciberinstigación: convergencias y divergencias en la configuración de la participación criminal digital entre Argentina y Perú

Cyber-instigation: convergences and divergences in the configuration of digital criminal participation between Argentina and Peru

Jorge Pérez López y Edin Romero Romero*

Autores:
Jorge Pérez López y Edín Romero Romero
Universidad Nacional Mayor de San Marcos, Perú.

Recibido: 13/08/2025
Aceptado: 01/10/2025

Citar como:
PÉREZ LÓPEZ, Jorge y ROMERO ROMERO, Edin (2025): "Ciberinstigación convergencias y divergencias en la configuración de la participación criminal entre Argentina y Perú", *Revista Jurídica de la Facultad de Derecho y Ciencias Sociales UNT, Vol. 1, Núm. 1*.

Resumen: El presente estudio examina la ciberinstigación como modalidad contemporánea de participación criminal, adaptada a los entornos digitales y caracterizada por el anonimato, la masividad de los mensajes y su alcance transnacional. A través de un análisis comparado entre Argentina y Perú se identifican similitudes y diferencias en la regulación, interpretación y persecución de esta conducta. Ambos sistemas conciben la instigación como la inducción dolosa que determina a otro a cometer un delito, exigiendo la concurrencia de un nexo causal entre el acto instigador y el ilícito. No obstante, Argentina presenta una formulación más precisa en sus artículos 45 y 209 del Código Penal y una mayor elaboración jurisprudencial, mientras que Perú, aunque equipara la pena a la autoría, artículo 24 del Código Penal, carece de un desarrollo doctrinal sólido en entornos digitales. El trabajo describe las principales manifestaciones de la ciberinstigación, que van desde redes sociales y foros en la dark web hasta aplicaciones de mensajería cifrada, plataformas de videojuegos, metaversos y entornos descentralizados. Asimismo, se examina su incidencia en delitos como estafas masivas, radicalización, tráfico de material ilícito, ciberacoso y ataques a infraestructuras críticas. Se abordan también los desafíos probatorios derivados del cifrado, el uso de pseudónimos y la descentralización, destacando que Argentina cuenta con protocolos técnicos y formación

* Jorge Pérez López. Docente ordinario de la Universidad Nacional Mayor de San Marcos, Perú. Correo electrónico: jperezlopez0804@gmail.com ORCID: 0000-0002-4695-389X.
**Edin Romero Romero. Estudiante avanzado de Derecho en la Universidad Nacional Mayor de San Marcos, Perú. Miembro Principal del Taller de Estudios Penales-UNMSM. Correo electrónico: edin.romero@unmsm.edu.pe ORCID: 0009-0007-7290-7612.

pericial más robusta, mientras Perú depende en mayor medida de la cooperación internacional. Finalmente, se proponen medidas para fortalecer la respuesta penal, incluyendo la tipificación autónoma de la ciberinstigación, la armonización normativa, el desarrollo de protocolos probatorios especializados, la capacitación de operadores jurídicos y la intensificación de la cooperación judicial internacional.

Palabras claves: ciberinstigación, derecho penal, evidencia digital, criminalidad transnacional

Abstract: This study examines cyber-instigation as a contemporary form of criminal participation, adapted to digital environments and characterized by anonymity, mass dissemination of messages, and transnational reach. Through a comparative analysis between Argentina and Peru, similarities and differences are identified in the regulation, interpretation, and prosecution of this conduct. Both systems define instigation as the intentional inducement that determines another to commit a crime, requiring the existence of a causal link between the instigating act and the offense. However, Argentina presents a more precise formulation in Articles 45 and 209 of its Criminal Code and a more developed body of case law, while Peru, although equating the penalty to that of the perpetrator under Article 24 of its Criminal Code, lacks a solid doctrinal framework in digital contexts. The paper describes the main manifestations of cyber-instigation, ranging from social networks and dark web forums to encrypted messaging applications, video game platforms, metaverses, and decentralized environments. It also examines its impact on crimes such as large-scale fraud, radicalization, trafficking of illicit materials, cyberbullying, and attacks on critical infrastructure. The study further addresses evidentiary challenges arising from encryption, the use of pseudonyms, and decentralization, highlighting that Argentina has more robust technical protocols and expert training, while Peru relies more heavily on international cooperation. Finally, the paper proposes measures to strengthen the criminal justice response, including the autonomous criminalization of cyber-instigation, regulatory harmonization, the development of specialized evidentiary protocols, training for legal practitioners, and the intensification of international judicial cooperation.

Keywords: cyber-instigation, criminal law, digital evidence, transnational crime

I. INTRODUCCIÓN

La era digital ha transformado radicalmente los escenarios en los que se ejercen los delitos, ampliando las fronteras geográficas y multiplicando las formas de intervención criminal. Esto ha configurado nuevos retos para el Derecho Penal, especialmente en cuanto a su capacidad para adaptarse a modos de comisión delictiva basados en herramientas informáticas y entornos virtuales. En este contexto, la figura de la ciberinstigación emerge como un elemento clave dentro de la participación criminal digital, entendida como la incitación o el impulso para la comisión de delitos a través de medios electrónicos.

La ciberinstigación se distingue por características particulares como el anonimato del instigador, la masividad y el alcance global de los mensajes, lo cual dificulta la aplicación de categorías jurídicas clásicas que requieren imputación subjetiva clara y la demostración de un nexo causal directo. Por ello, resulta

indispensable un análisis crítico que identifique y compare las respuestas legislativas y jurisprudenciales en diferentes sistemas jurídicos con realidades y normativas semejantes, pero no idénticas.

Argentina y Perú representan casos paradigmáticos en Latinoamérica para examinar esta problemática, dada su relevancia en la región y las particularidades en sus marcos normativos y prácticas probatorias en materia de instigación digital. El presente artículo busca contribuir a la comprensión de las convergencias y divergencias doctrinales y prácticas en ambos países, así como proponer lineamientos para fortalecer la persecución penal en un contexto caracterizado por su complejidad técnica y transnacionalidad.

De esta manera, se pretende aportar elementos relevantes para la actualización y armonización de las normativas penales regionales y para el desarrollo de protocolos investigativos que respondan a los desafíos de la criminalidad digital contemporánea.

II. MARCO GENERAL DE LA INSTIGACIÓN

II.1. Concepto dogmático y elementos estructurales de la instigación

La instigación, en el derecho penal, se configura como una institución de participación delictiva que se distingue dogmáticamente de la autoría y coautoría. En efecto, la doctrina define al autor como aquel sujeto que realiza el hecho punible de manera directa y autónoma, de modo que se puede afirmar que el delito es suyo[1]. Por su parte, los coautores son los que realizan de manera conjunta y de mutuo acuerdo un hecho[2], es decir, cometen el delito entre todos.

Partiendo de estas nociones fundamentales, corresponde delimitar el concepto de la instigación. Esta se entiende como la acción mediante la cual una persona, de manera intencional y con ánimo de inducir, determina dolosamente a otro la comisión del injusto[3]. Por lo tanto, se trata de una forma de participación mediata en el delito, en la que el instigador no ejecuta materialmente la conducta típica, pero si influye decisivamente en la voluntad del autor.

Desde una perspectiva dogmática, la instigación requiere la concurrencia de tres elementos: a) la determinación psíquica del autor, es decir, que su decisión haya sido efectivamente influenciada por el instigador; b) el dolo de instigar, entendido como el conocimiento y la voluntad de inducir a otro a delinquir; y c) una

[1] MIR (2015). Para esto se tiene en cuenta que el "concepto ontológico" es cuestionable, ya que la filosofía analítica ha manifestado que las cosas no tienen una esencia necesaria, implicada en sí mismas, sino que son concebidas a través de la mediación convencional del lenguaje. Además, se considera que el concepto de una cosa depende del significado convencional de las palabras con las que son designadas.

[2] Esta definición ha sido aceptada en la doctrina alemana como Jescheck, Welzel; en España, Rodríguez Morillo.

[3] HURTADO Y PRADO (2011). La persona instigada es determinada por el instigador para que ejecute una infracción, el instigador no comente la infracción ni tampoco forma parte de su ejecución, ya que se limita a influir psicológicamente en otra persona, esto con el objetivo de que este incurra en un hecho punible.

relación de causalidad entre la instigación y la conducta del autor, de modo que esta no se habría producido sin la intervención del instigador. Lo desarrollamos seguidamente.

a) La determinación psíquica: El instigador provoca en la mente del autor material la decisión de cometer el hecho delictivo, esto implica una creación de la voluntad criminal ajena. Para Mir Puig, esta influencia debe ser objetivamente imputable como la causa de la decisión delictiva, es decir, debe poder atribuírsele el incremento en el riesgo para el bien jurídico protegido[4].

b) El dolo de instigar: El instigador actúa con conocimiento y voluntad respecto al resultado delictivo. El dolo abarca no solo al conocimiento del tipo penal al cual se induce sino también a la intención de que dicho delito se realice a través del sujeto instigado. Según Enrique Bacigalupo, el instigador es quien crea el dolo en la cabeza del autor y dirige su voluntad hacia la comisión del delito[5].

c) La relación de causalidad: Existe un nexo causal entre la conducta del instigador y la perpetración del hecho delictivo. Para que exista instigación, el influjo psíquico debe ser la causa eficaz que determina la realización del ilícito penal por tercera persona. Sin este nexo, la conducta no puede ser imputada al instigador como responsable directo.

La confluencia de estos elementos distingue la instigación de otras formas de participación como la complicidad o coautoría, siendo característica la inducción mental a cometer un hecho punible. En consecuencia, la ausencia de cualquiera de estos elementos desvirtúa la figura y puede descalificar la conducta como mera exhortación o expresión protegida.

II.2 Distinciones conceptuales: instigación vs. coautoría, complicidad e incitación pública a delinquir

Para la correcta aplicación de estas instituciones, es imprescindible delimitar claramente la figura de la instigación frente a otros modos de participación criminal y conductas que pueden parecer similares. A efectos de distinguir las diferentes formas de participación delictiva, se presenta el siguiente cuadro comparativo, elaborado conforme a los criterios doctrinarios más aceptados[6].

[4] MIR (2015).
[5] BACIGALUPO (1994) p. 181.
[6] Véase Cuadro 1: Diferencias entre instigación, coautoría, complicidad e incitación pública.

Cuadro1. Diferencias entre instigación, coautoría, complicidad e incitación pública

Figura	Rasgo distintivo principal	Descripción y ejemplo
Instigación	Determinación psíquica a otro para cometer delito	El instigador induce mentalmente al autor material. A induce a B a robar a C.
Coautoría	Participación directa y conjunta	Los sujetos planifican y ejecutan el delito en concierto. A y B planifican y realizan un fraude a C.
Complicidad	Ayuda o asistencia sin control sobre la decisión delictiva	Facilitar herramientas o medios para el delito. A provee un vehículo a B para huir después de robar a C.
Incitación pública	Llamado dirigido a colectividad indeterminada	Mensajes públicos que promueven delitos sin individualizar destinatarios. Esta situación generalmente se da a través de llamadas en redes (se abordará en desarrollo).

Fuente: Elaboración propia.

La instigación supone un dominio sobre la voluntad ajena que es más directo y específico que la mera complicidad; igualmente, se diferencia de la incitación pública a delinquir, la cual se caracteriza por estar dirigida a un público amplio y no necesariamente culmina en un delito específico. La instigación requiere además que el delito se cometa, o al menos se inicie la ejecución, para que la responsabilidad se configure plenamente.

II.3. Regulación de la instigación en el Código Penal argentino

El artículo 45 del Código Penal argentino establece que: “Los que tomasen parte en la ejecución del hecho o prestasen al autor o autores un auxilio o cooperación sin los cuales no habría podido cometerse, tendrán la pena establecida para el delito. En la misma pena incurrirán los que hubiesen determinado directamente a otro a cometerlo”[7].

Este precepto reconoce explícitamente que el instigador es quien, no ejecutando personalmente el delito, induce o determina a otro a su comisión. En el artículo 209 se sanciona, por la sola instigación, con prisión de dos a seis años según la gravedad del delito y las demás circunstancias establecidas en el artículo 41. Incluso, la sanción puede ser de 10 años si el instigador fuese un militar que en tiempo de conflicto armado incite la sustracción al servicio militar[8].

La jurisprudencia argentina ha interpretado que para sancionar la instigación se debe acreditar un vínculo claro, específico y efectivo entre la acción del instigador y la conducta del autor material; Además, se exige la demostración del dolo, es decir, de la intención consciente de generar la decisión delictiva en el

[7] ARGENTINA, Código Penal, artículo 45.
[8] ARGENTINA, Código Penal, art. 209 y 209 bis.

tercero, tal como lo resolvió la Suprema Corte de Justicia de la Provincia de Buenos Aires en el caso *Altuve*[9].

Además, mediante la doctrina establece que la instigación debe ser más que un simple estímulo: debe tratarse de una "determinación directa", representando una causa eficiente que genera el resultado delictivo[10]. El marco normativo argentino busca así evitar imputaciones por manifestaciones ambiguas o generales que no configuran influencia causal efectiva.

II.4. Regulación de la instigación en el Código Penal peruano

En el Código Penal peruano, el artículo 24 dispone: El que, dolosamente, determina a otro a cometer el hecho punible será reprimido con la pena que corresponde al autor[11].

Esta disposición normativa configura a la instigación como una forma de participación delictiva, equiparable en sanción a la autoría, siempre que se acredite una determinación dolosa del instigador sobre el autor material. La jurisprudencia suele requerir prueba concreta de la influencia efectiva y causal del instigador sobre la persona que ejecuta el delito, resaltando la dificultad de probar el nexo psíquico y la intención delictiva en ambientes digitales o anónimos.

El sistema jurídico peruano demanda que la instancia acusadora demuestra la relevancia causal del acto de instigación para la comisión del delito, así evita condenas basadas en meras presunciones o conjeturas. Este enfoque pone en relieve las dificultades probatorias que surgen en la investigación penal, sobre todo en casos de ciberinstigación, donde el anonimato y la masividad de los mensajes complican la identificación y la imputación exacta.

La jurisprudencia peruana, establece que la instigación supone determinar a otro a la comisión de un hecho delictivo; cuya conducta reprochable penalmente “es haber puesto a disposición del autor razones de peso para tomar una decisión criminal”[12]; dado que únicamente dependerá del autor la ejecución y/o consumación del hecho delictivo. De otro lado, no solo la autoría inmediata sino también la coautoría son formas de autoría; en cuyos supuestos existe dominio sobre el desarrollo de la acción criminal (dominio del hecho) según lo resuelto por la Corte Suprema peruana en la causa Nº 1045-2019[13].

[9] SUPREMA CORTE DE JUSTICIA DE LA PROVINCIA DE BUENOS AIRES, 23/12/2020, causa P. 131.348, *Altuve, Carlos Arturos/ Recurso extraordinario de inaplicabilidad de ley*.
[10] ZAFFARONI (2006).
[11] PERÚ, Código Penal, artículo 24.
[12] GARCÍA (2019), p. 774.
[13] PERÚ, CORTE SUPREMA DE JUSTICIA DE LA REPÚBLICA, SALA PENAL TRANSITORIA, Recurso de Nulidad N.º 1045-2019, Lima, 22/06/2021.

III. LA CIBERINSTIGACIÓN: PARTICULARIDADES Y DESAFÍOS EN EL MUNDO DIGITAL

III.1. Definición y características de la ciberinstigación

En base a lo desarrollado anteriormente, se puede definir a la ciberinstigación como la acción de incitar, inducir o estimular a uno o varios sujetos (la pluralidad de instigados se da principalmente por usar medios digitales de alcance masivo) a cometer delitos, valiéndose de medios electrónicos como redes sociales, plataformas de mensajería, y herramientas de comunicación digital. Este fenómeno trasciende la simple traslación de la instigación tradicional al plano digital, ya que introduce características singulares que complejizan su análisis y tratamiento jurídico. Entre sus características están las siguientes:

a) El anonimato: El entorno digital habilita el uso de identidades apócrifas, pseudónimos y tecnologías de ocultación, dificultando enormemente la identificación fidedigna de los instigadores. Delincuentes y grupos organizados operan desde cualquier parte del mundo, servidos por infraestructuras como la web oscura, plataformas cifradas y servicios de anonimización, eludiendo la acción policial y judicial mediante técnicas avanzadas que obstruyen la trazabilidad de sus acciones.

b) La masividad**:** A diferencia de la instigación tradicional, en el ciberespacio un mensaje puede replicarse y multiplicarse instantáneamente, alcanzando a miles o millones de usuarios en cuestión de segundos. Esta masividad aumenta el potencial lesivo de la conducta e introduce desafíos inéditos para delimitar la conexión causal entre el acto de instigación y concretos hechos ilícitos, dadas la pluralidad y heterogeneidad de posibles destinatarios.

c) El alcance global: Las Tecnologías de la Información y la Comunicación (TIC) han eliminado restricciones geográficas y temporales, permitiendo que los instigadores actúen desde jurisdicciones remotas y accedan a víctimas en diversos puntos del planeta. El ciberespacio proporciona un ámbito donde las operaciones ilícitas pueden desplegarse transnacionalmente, aprovechando lagunas normativas, diferencias legales y falencias en la cooperación internacional, consolidando la transnacionalidad de la ciberinstigación.

III.2 Formas de manifestación de la ciberinstigación

La ciberinstigación despliega una amplia diversidad de manifestaciones cuya comprensión es trascendental para una adecuada tipificación y su respectiva persecución penal. Se tiene a las siguientes manifestaciones:

a) Redes sociales

Las principales plataformas, como Facebook, X, Instagram y TikTok, permiten la rápida diseminación de mensajes incitadores. No solo se observan convocatorias explícitas a saqueos o disturbios, sino también la creación de

eventos virales que buscan desbordar la capacidad de respuesta de las autoridades. En la viralización desempeñan un papel trascendental los algoritmos de amplificación, los cuales contribuyen a que contenidos peligrosos ganen visibilidad, mientras que la generación de comunidades cerradas refuerza la identidad grupal y disminuye la resistencia moral ante la comisión de ilícitos, ya que, pese a las políticas de seguridad implementadas por las diversas redes sociales, estas suelen resultar insuficientes o son fácilmente eludidas.

En Argentina durante diciembre de 2017, se viralizó un evento titulado "Saqueos de Navidad 2017" en Facebook, alcanzando a cientos de usuarios. Este tipo de convocatorias, aunque a veces disfrazadas de "juegos" o "simulaciones", tienen efectos concretos en la organización de delitos contra la propiedad. Investigaciones como las de Marina Prieto han demostrado que los muros abiertos y publicaciones públicas permitieron una coordinación informal entre usuarios, constituyendo una forma digital de instigación y organización delictiva[14].

En Perú durante el estado de emergencia provocado por las intensas lluvias e inundaciones en marzo de 2017, se identificó un caso paradigmático del uso de redes sociales como medio para instigar conductas delictivas. En particular, la Policía Nacional del Perú detectó a un sujeto que, a través de publicaciones en Facebook, incitaba a la comisión de saqueos, generando grave perturbación de la tranquilidad pública. Este hecho motivó la intervención del Ministerio del Interior y dio lugar a la apertura de una investigación penal, conforme a los presupuestos del delito de perturbación del orden público, con una pena estimada de hasta seis años de privación de libertad[15].

Si bien se desarrolla, de manera similar, mediante X a través del uso de hashtags como "#saqueos" o "#rebelión" se puede amplificar la difusión de mensajes delictivos, ya que el *retuit* o la etiqueta contribuyen a la divulgación masiva de la ofensa, lo que puede agravar la responsabilidad penal del emisor. La política oficial de X prohíbe expresamente la incitación a la violencia, incluyendo llamados a cometer delitos, acosar grupos protegidos o difundir instrucciones para actos violentos, es decir, la plataforma reconoce que la naturaleza abierta y viral de los hashtags puede facilitar la coordinación de acciones ilícitas, conforme a lo establecido en las Políticas de seguridad de la red social X[16].

Una de las redes sociales con mayor visualización es TikTok, en el caso de esta plataforma, son diversos los retos virales o "*challenges*" que han promovido conductas peligrosas, las cuales pueden considerarse formas contemporáneas de instigación pública. Entre ellos destacan el *Blackout Challenge*[17], el *Clonazepam*

[14] PRIETO (2013).
[15] LA REPÚBLICA (2017).
[16] X (2025).
[17] *Blackout Challenge*: reto viral en el que se incita a los participantes, en su mayoría menores de edad, a provocar asfixia voluntaria mediante diversos métodos (cintas, cinturones, manos), con el fin de experimentar una breve pérdida de conciencia o euforia. Esta práctica ha sido relacionada con varios casos de muerte por hipoxia cerebral, y su difusión ha generado alertas internacionales por parte de organizaciones de salud y protección infantil, El Universal (2022).

Challenge[18] y el *Rompecráneos*[19] ampliamente difundidos y, en muchos casos, dirigidos a menores de edad como señala el medio especializado Maldita.es (2023). Estos contenidos tienden a normalizar conductas potencialmente delictivas, tales como lesiones, intoxicaciones, daños a la propiedad o exposición al peligro, y al estar disponibles públicamente, pueden configurar una instigación abierta a la comisión de hechos punibles[20].

b) Foros y comunidades especializadas en la "deep web" y "dark web"

En el internet que navegamos a diario es apenas la punta del iceberg, ya que detrás de los buscadores como Google existe un universo mucho más grande y menos visible: espacios que no aparecen en los resultados y que requieren accesos especiales.

Entre los cuales se distinguen dos conceptos que suelen confundirse; por un lado, la internet profunda y por el otro, la internet oscura, cada una con funciones y características propias. Entre lo más llamativo de estas áreas se encuentran foros de la web profunda y foros de la web oscura, que son utilizados como medios para reunir a diversas comunidades en línea[21].

La web profunda, conocida como deep web, es un instrumento útil, necesario y legal para la operatividad de internet, es la parte del internet a la cual no se puede acceder desde los motores de búsqueda tradicionales, debido a está protegido detrás de firewalls[22] o muros de pago, es decir, requiere credenciales de inicio de sesión específicas. Es importante tener en cuenta que la web profunda no es intrínsecamente maliciosa. De hecho, el contenido en esta parte de internet es completamente legítimo, como: cuentas personales de correo electrónico, registros médicos, redes privadas incluidas VPN e intranets, páginas de cuentas bancarias, entre otras[23].

---

[18] *Clonazepam Challenge*: desafío que consiste en ingerir dosis no prescritas del medicamento clonazepam, un ansiolítico de uso controlado, para grabar y viralizar en redes sociales los efectos de somnolencia, desinhibición o pérdida de conciencia. El consumo en contextos no médicos ha derivado en intoxicaciones graves e internamientos hospitalarios, y representa una conducta especialmente peligrosa entre adolescentes, BIOCHILE (2018).

[19] *Rompecráneos* (también conocido como *Skull-Breaker Challenge*): consiste en hacer que una persona salte (generalmente en medio de dos individuos), para luego ser derribada sorpresivamente con un golpe en las piernas, provocando su caída violenta hacia atrás. Este “juego” ha generado lesiones craneales, conmociones cerebrales, Telemundo (2020).

[20] MALDITA.ES (2023).

[21] CLYBE (2025).

[22] Para KASPERSKY (*s/f)*: “Un firewall es un sistema de seguridad de red de las computadoras que restringe el tráfico de Internet entrante, saliente o dentro de una red privada. Este software o esta unidad de hardware y software dedicados funciona bloqueando o permitiendo los paquetes de datos de forma selectiva. Normalmente, su finalidad es ayudar a prevenir la actividad maliciosa y evitar que cualquier persona (dentro o fuera de la red privada) pueda realizar actividades no autorizadas en la web”.

[23] CLYBE (2025).

La web oscura, conocida como dark web, es un subconjunto de la web profunda, es donde se intensifican el anonimato y el secreto[24]. Aunque la web oscura suele asociarse con actividades ilícitas, su uso no es exclusivamente delictivo, ya que periodistas, activistas la utilizan para comunicarse y compartir información sin temor a la censura.

Sin embargo, también se ha constituido como un espacio donde circulan datos robados, dentro de ellos usuarios, contraseñas o información de tarjetas de crédito, así como la compraventa de drogas, armas y esquemas de fraude. Lo cierto es que, la dark web también brinda un espacio para las personas que están preocupadas por la privacidad o desea discutir temas sensibles sin temor a ser vigilados por las autoridades[25].

Por otro lado, el internet al cual se puede acceder mediante el motor de búsqueda como Google, Yahoo!, Bing, entre otros, es conocido como surface web o clear web. A diferencia de la web visible, la *deep web*, también conocida como web invisible o web oculta, abarca cerca del 90 % de Internet. Allí se encuentran contenidos que, siendo fiables y legales, no son indexables y rastreables por los buscadores, como correos electrónicos, cuentas y depósitos bancarios, servicios de video bajo demanda (Netflix, Amazon, HBO), música en streaming (Spotify, Apple Music, Amazon Music) o sitios de contactos como Ashley Madison y Meetic[26].

En la red oscura existen foros clandestinos, que se organizan por temáticas como hacking, narcotráfico, pornografía infantil, venta de armas o fraudes, los cuales funcionan como puntos de encuentro seguros para que delincuentes intercambien información, coordinen acciones y difundan guías para delinquir, amparados en el anonimato que brindan redes como Tor. Entre los más conocidos destacan: XSS, especializado en hacking y ransomware; Foros de infracción, centrado en la compraventa de datos robados; Temor, con formato similar a Reddit y orientado a la coordinación criminal; y Foros oscuros, con membresías exclusivas que perpetúan el comercio ilícito.

En estos foros, la ciberinstigación se manifiesta de múltiples maneras: desde la difusión de guías para cometer fraudes, estafas o ataques informáticos, hasta la convocatoria y organización de ataques cibernéticos, incluso en el mundo físico. Además, se incluye el intercambio de software y herramientas ilícitas (mediante la venta o préstamo de malware, exploits, acceso a bases de datos falsos o herramientas de phishing que incrementan la comisión de hechos delictivos), la propagación de ideologías extremistas que promueven violencia y terrorismo, y el

[24] Está intencionalmente oculta de los motores de búsqueda y requiere un software especial como Tor (The Onion Router) para ingresar a él. Los sitios en la web oscura suelen usar nombres de dominio "(...).onion", que incorpora una capa de anonimato tanto para los usuarios como para los administradores. Tor es una red de anonimato y un navegador asociado que permite a los usuarios navegar por Internet de forma privada y segura, ocultando su dirección IP y cifrando su tráfico a través de una red distribuida de servidores voluntarios llamados nodos. Su nombre proviene de The Onion Router (el enrutador cebolla), haciendo referencia a su método de encriptación en capas, que protege la identidad y la actividad de los usuarios ante proveedores de servicios de Internet, administradores de red y terceros (Arimetrics, *s/f*).

[25] RODRÍGUEZ (2025).

[26] FISCALÍA GENERAL DEL ESTADO (2023).

comercio de bienes ilegales como drogas, armas o datos robados, uniendo la instigación con la acción delictiva. Todos estos espacios, no son los únicos, facilitan la logística delictiva al complementar la instigación con operaciones concretas.

En América Latina, específicamente en Argentina y Perú se ha registrado la presencia e influencia de estos foros, con actividades delictivas, en la dark web. Ante lo cual ambos países han ido adaptando su legislación. En el caso del primero, está presente la Ley de delitos informáticos, Ley de Grooming, Ley de protección de datos personales, Convenio de Budapest sobre cibercrimen; mientras que en el segundo, está presente la Ley de delitos informáticos. Con esto se entiende que ambos países han impulsado acciones contra foros y mercados clandestinos ligados a la distribución de pornografía infantil, tráfico de drogas y fraudes digitales, colaborando internacionalmente para desmantelar redes que operan en estas plataformas.

Por ejemplo, recientemente en Argentina se desplegó un megaoperativo, a cargo de la Policía Federal Argentina, denominado "Protección de las Infancias IV" el cual logró desmantelar una red que utilizaba la dark web para la producción y distribución de material de abuso infantil, involucrando la detención de numerosos sujetos y la incautación de dispositivos digitales asociados a la comisión del delito[27].

El carácter oculto, descentralizado y técnico de estos foros pone en jaque al derecho tradicional, demandando investigaciones especializadas, cooperación internacional y marcos legales adaptados para sancionar la ciberinstigación. Esta resulta especialmente efectiva al dirigirse a personas con intención criminal, protegidas por entornos que favorecen la impunidad. Así, los foros de la deep y dark web son piezas clave para comprender y enfrentar la ciberinstigación, al facilitar su origen, organización y expansión a escala global.

c) Aplicaciones de mensajería instantánea y cifrada

Las aplicaciones de mensajería instantánea y cifrada, como WhatsApp, Signal, Telegram, entre otras, constituyen hoy en día uno de los principales canales para la comunicación digital a nivel global. Sin embargo, también son utilizadas para la comisión y coordinación de delitos a través de la ciberinstigación, debido a su combinación de accesibilidad, rapidez y mecanismos avanzados de privacidad y seguridad que dificultan la acción de persecución.

Estas aplicaciones usan generalmente un cifrado de extremo a extremo, lo que significa que los mensajes enviados están encriptados desde el dispositivo del emisor hasta el receptor, sin posibilidad de que ni siquiera la empresa proveedora acceda al contenido. Esto asegura la privacidad y confidencialidad de las comunicaciones, pero también plantea un reto significativo para la persecución penal, pues las autoridades no pueden interceptar directamente los mensajes sin acceso físico a los dispositivos implicados o sin la colaboración del usuario[28].

[27] ARGENTINA.GOB.AR (2024).
[28] BELCIC y CORRIGAN (2024).

Telegram, a diferencia de WhatsApp y Signal, no activa el cifrado de extremo a extremo en todos los chats, sino solo en una función opcional llamada "chat secreto", lo que en la práctica puede generar zonas de menor seguridad y mayor vulnerabilidad al rastreo en conversaciones convencionales[29]. A pesar de ello, su popularidad y características de privacidad la hacen muy utilizada para actividades ilícitas. Es más, las aplicaciones cifradas se han convertido en espacios clave para la organización criminal, ya que, a través de grupos y canales, públicos o privados, permiten coordinar estafas, fraudes y actos violentos a gran escala. En ellos circulan guías, enlaces y videos que instruyen sobre delitos específicos, mientras que bots integrados —especialmente en Telegram— amplifican automáticamente la difusión de contenidos ilícitos. El cifrado, el registro con números virtuales y el uso de dispositivos dedicados protegen la identidad de los instigadores, dificultando su localización[30]. A ello, se suman versiones adulteradas de apps legítimas (versiones troyanizadas), infectadas con malware para interceptar comunicaciones, manipular datos y robar información, potenciando delitos informáticos de alta complejidad.

Se han detectado en Argentina diversos grupos cerrados de Telegram dedicados a realizar estafas bancarias, fraudes electrónicos y diversos delitos. En estos canales, administradores e instigadores comparten enlaces de phishing, códigos maliciosos, técnicas para engañar a usuarios o para acceder a productos ilegales mediante el buscador de dicha aplicación y operadores financieros. Por ejemplo, un caso importante involucró la creación de canales privados, por el cual se ofrecían drogas sintéticas como MDMA, LSD y ketamina, con instrucciones de compra y entrega (Ministerio Público Fiscal). Esta modalidad de ciberinstigación, mediante difusión masiva y anonimato, evidencia cómo el instigador digital induce a terceros a cometer hechos delictivos sin contacto directo.

En Perú, se ha detectado el uso de Telegram como medio para instigar delitos informáticos, especialmente estafas y extorsiones. La Agencia Andina evidenció cómo cibercriminales enviaban enlaces fraudulentos desde cuentas previamente comprometidas, se apoderan de la cuenta de otra persona, induciendo a las víctimas (contactos de la cuenta comprometida) a entregar sus códigos de verificación[31]. Esta forma de ciberinstigación, basada en la manipulación de la confianza digital, conocida también como ingeniería social, facilita el acceso ilícito a información privada.

d) Plataformas de videojuegos y sistemas de chat alternativos

Durante los últimos años, los entornos digitales asociados al ocio interactivo, especialmente los videojuegos en línea multijugador (MMORPG, shooters) y las plataformas de comunicación como Discord y Twitch, se han convertido en blancos ideales para la planeación y ejecución de conductas delictivas. Aunque concebidos originalmente como medios de entretenimiento, su

[29] REVISTA CLOUD (2024).
[30] SALVADOR (2024) p. 101.
[31] ANDINA (2025).

capacidad para propiciar interacciones sincrónicas, privadas y, en muchos casos, anónimas, ha facilitado su instrumentalización para fines criminales, generando verdaderos puntos ciegos para la persecución penal tradicional[32].

En el caso de los videojuegos en línea, se han documentado prácticas como la extorsión digital entre jugadores, la distribución de malware mediante archivos modificados o enlaces compartidos en chats personales, y el acoso sexual (tratando de acercase al *grooming*), especialmente en comunidades con una mayor presencia de menores. Algunos de ellos son *World of Warcraft*, *Call of Duty* o *Valorant* han sido usados para planificar ataques coordinados, difundir mensajes de odio y manipular a usuarios vulnerables. Esta dinámica adquiere relevancia en la instigación encubierta hacia menores de edad, determinada por un proceso de manipulación psicológica gradual, carente de órdenes explícitas, pero con una evidente intención de influir emocional y cognitivamente en la víctima (Calderón, 2025)[33].

En esa misma línea, para Dergarabedian[34], Discord es un caso paradigmático, ya que su programación descentralizada y poca supervisión institucional favorecen la producción de servidores privados con canales de texto, voz y video, en los que proliferan actividades ilícitas como *doxing* (difusión de datos personales), "porno venganza", distribución de *malware* (incluyendo *infostealers* como RedLine o Lumma) e instigación a conductas delictivas, tanto en el ámbito digital como en el físico. En Argentina, esta descentralización dificulta la identificación del instigador, diluye la trazabilidad penal y, en consecuencia, incrementa la impunidad.

Asimismo, Twitch, aunque orientada a la transmisión audiovisual, también ha reconocido conductas inadecuadas vinculadas a su comunidad, incluyendo amenazas de violencia masiva, explotación sexual infantil y participación en grupos organizados de odio. En 2021, implementó una política de sanción extraplataforma, reconociendo la interconexión entre entornos digitales y la necesidad de respuestas integrales frente a la instigación transmedia, es decir, la aplicación de sanciones en contra de ofensas graves que presenten un riesgo de seguridad sustancial para su comunidad, incluso si tales acciones ocurren completamente fuera de Twitch. Por ejemplo, la violencia letal, extremismo violento, amenazas de violencia masiva, explotación sexual de menores y pertenencia a grupos de odio[35].

e) Nuevas tendencias

La rápida transformación tecnológica ha dado lugar a entornos virtuales que desafían los esquemas tradicionales de imputación penal. Entre estos, las redes descentralizadas, los metaversos y los contenidos sintéticos generados por inteligencia artificial —como los conocidos *deepfakes*— crean nuevas formas de mantener el anonimato, simular situaciones y coordinar actividades delictivas, lo

[32] DÍAZ, RESTREPO & GONZÁLEZ (2024).
[33] CALDERÓN (2025).
[34] DERGARABEDIAN (2021).
[35] TWITCH (2021).

que pone a prueba los mecanismos tradicionales que se utilizan para identificar a quienes son responsables.

Las redes descentralizadas, que funcionan con arquitectura *peer-to-peer* y utilizan blockchain, permiten que las personas interactúen sin intermediarios, dificultando rastrear quienes están detrás de las conductas ilegales. En el Perú, se han detectado casos de estafas usando plataformas con criptomonedas y contratos inteligentes, donde las identidades de los autores y los fondos permanecen ocultos, haciendo que sea difícil para las autoridades actuar de manera efectiva[36]. En Argentina, también se ha comprobado que en comunidades en redes como Mastodon o Element, se difunden contenidos ilegales —como discursos de odio o material sensible— y las autoridades tienen poca capacidad para intervenir directamente[37].

Por otro lado, los metaversos son entornos en los que los usuarios interactúan en tiempo real usando avatares, creando nuevas formas de acoso, fraudes y hasta la explotación de menores. En Argentina, se han reportado casos en plataformas como *Second Life* y *VRChat*, donde adultos crean perfiles falsos de jóvenes para establecer vínculos afectivos y obtener material íntimo, sin que haya contacto físico, lo que constituye delitos de riesgo (Bendinelli, 2024). En Perú, aplicaciones de realidad aumentada como *Pokémon Go* han sido usadas para organizar encuentros con fines delictivos, aprovechando la geolocalización y las interacciones en espacios públicos[38].

Finalmente, los *deepfakes*[39] son una amenaza en crecimiento en el ámbito legal, ya que permiten crear imágenes, audios y videos falsos que parecen reales. En Perú, ya se han reportado casos donde se usan vídeos manipulados para extorsionar, simulando declaraciones de figuras públicas o familiares, causando daños económicos y psicológicos graves (Mendoza, 2024)[40]. En Argentina, un fallo de la Cámara Penal de Zárate-Campana reconoció que contenidos creados por inteligencia artificial —sin víctimas reales— pueden considerarse delitos contra la

[36] El uso creciente de criptomonedas ha sido acompañado por un aumento significativo en esquemas de fraude digital, especialmente mediante plataformas descentralizadas que dificultan la identificación de los autores. Según la opinión de expertos en ciberseguridad, las amenazas más comunes incluyen el *phishing*, la suplantación de identidad y el uso de malware, todo ello facilitado por la ausencia de regulación y trazabilidad en estos entornos. MEZA (2025).

[37] DERGARABEDIAN (2021).

[38] El autor estudia el fenómeno de los Deepfakes y sus consecuencias jurídicas respecto del delito de suplantación de identidad en el Perú. TORRES (2024)

[39] Los *deepfakes* son medios sintéticos generados mediante técnicas de aprendizaje profundo (*deep learning*). Incluyen imágenes, vídeos y grabaciones de audio manipulados para retratar a alguien diciendo o haciendo algo que en realidad nunca dijo o hizo. Estas tecnologías identifican y aprenden de grandes cantidades de datos para generar medios falsos de apariencia realista.

[40] En Perú, se han reportado casos en los que delincuentes utilizan videos falsos generados mediante técnicas de *deepfake* para simular declaraciones de figuras públicas, como Bill Gate, con el fin de insertar malware, robar datos personales o inducir transferencias económicas fraudulentas. Esta modalidad, que combina simulación audiovisual y manipulación informática, ha sido identificada como una amenaza creciente en el país, especialmente en esquemas de extorsión y fraude digital.

integridad sexual de menores, según el artículo 128 del Código Penal (Melián, 2025)[41].

III.3. Ciberdelitos en los que la instigación digital cobra especial relevancia

La ciberinstigación —entendida como la acción de promover, orientar o facilitar la realización de conductas delictivas a través de medios digitales— adquiere especial protagonismo en la génesis, propagación y agravamiento de ciertos hechos delictivos, tanto hechos que surgen del entorno digital como tradicionales que se adaptan a las nuevas tecnologías. A continuación, se desarrollan los principales tipos penales donde esta figura resulta especialmente relevante:

a) Estafas informáticas y fraudes masivos

En América Latina, las estafas informáticas han ido evolucionando y complejizando con el transcurrir del tiempo, donde la instigación colectiva digital cumple un rol central. Muchas de estas estafas, como el *phishing, vishing, QRishing, carding* y el *SIM swapping*, ya no solo las hacen de manera individual, sino que comparten, enseñan y coordinan en grupos cerrados en plataformas como Telegram, formando verdaderas comunidades delictivas.

En Argentina, la Unidad Fiscal Especializada en Ciberdelincuencia (UFECI) reportó en 2024 que recibieron 34.468 denuncias, lo que significa un aumento del 21,1% en comparación con el año anterior. La mayoría de estos casos, el 63%, fueron fraudes en línea, incluyendo usurpación de identidad, accesos ilegales y campañas de phishing[42]. Estos delitos suelen darse a través de canales privados de mensajería donde se comparten scripts automatizados, tutoriales y métodos para reclutar personas que actúan como "mulas digitales" para hacer transferencias ilegales o suplantar identidades.

En Perú, la Dirección de Investigación de Ciberdelincuencia de la Policía Nacional (PNP) registró 4.349 denuncias por delitos informáticos en lo que va de 2025, con proyecciones de duplicarse respecto al año anterior. Las modalidades más frecuentes incluyen *phishing* (291 casos), *carding* (218), *Thief Transfer* (108), *SIM swapping* (11) y *QRishing*, una técnica emergente que utiliza códigos QR falsos para redirigir a sitios maliciosos[43].

[41] En Argentina, el uso de inteligencia artificial para generar *deepfakes* con contenido sexualizado de menores ha motivado propuestas legislativas para reformar el artículo 128 del Código Penal. En el caso citado por Melián (2025), se describe cómo se utilizó la imagen facial de una menor, combinada digitalmente con el cuerpo de otra persona, para producir material pornográfico falso. Este tipo de manipulación, aunque no involucre a una víctima “real” en el sentido tradicional, configura una representación sexualizada que vulnera gravemente la integridad de los menores. El proyecto de reforma propone incluir expresamente estas prácticas como delitos, reconociendo el uso de IA como medio típico de comisión (Proyecto de Ley 4411-D-2023).

[42] UNIDAD FISCAL ESPECIALIZADA EN CIBERDELINCUENCIA (2025).

[43] CHAUCA (2025).

Este panorama revela un patrón de ciberinstigación estructurada, donde los grupos cerrados en Telegram y redes sociales no solo difunden contenido delictivo, sino que fomentan activamente la comisión de delitos, generando una forma de autoría mediata digital. En palabras de Miucci[44], "los ciberatacantes hacen un trabajo de inteligencia previa, perfilan a la víctima y diseñan mensajes muy creíbles, con un objetivo claro: que la persona haga clic o ejecute una acción específica"[45].

b) Delitos de odio, radicalización y terrorismo digital

El mundo virtual ha cambiado por completo la forma en que ocurren fenómenos como la radicalización de ideas, la promoción del odio y el terrorismo. Esto se debe a que en línea se pueden difundir mensajes violentos a gran escala, de manera anónima y que cruzan fronteras. En este escenario, la ciberinstigación ayuda a ampliar, organizar y mantener vivo este tipo de conductas delictivas, muchas veces motivadas por motivos raciales, religiosos o políticos.

La Organización de las Naciones Unidas (ONU) ha alertado que las redes sociales facilitan una propagación sin precedentes del odio, lo que puede llevar desde una mayor polarización social hasta crímenes atroces. En su informe de 2023, el Secretario General señaló que "la incitación al odio en línea no es solo una amenaza para la convivencia democrática, sino un precursor directo de la violencia física"[46]. Las agresiones digitales incluyen ataques coordinados contra comunidades vulnerables, la difusión de memes que banalizan o exaltan el odio y la violencia, y campañas internacionales de desinformación impulsadas por cuentas anónimas o bots para manipular la opinión pública y afectar la estabilidad democrática[47].

En Argentina, el Código Penal contempla la instigación al delito (artículo 209) y la apología del crimen (artículo 213), pero no regula específicamente la instigación digital al odio o al terrorismo. En Perú, la Ley Nº 30096 sobre delitos informáticos tampoco aborda la ciberinstigación como figura autónoma, aunque podría interpretarse como una forma agravada de instigación cuando se utiliza tecnología para amplificar el daño.

c) Tráfico de material ilícito

El tráfico de materiales ilegales en el mundo digital, como pornografía infantil, drogas y armas, se basa en esquemas donde los propios usuarios se incentivan mutuamente. Estas comunidades en línea, muchas de ellas en foros especializados y canales cifrados, comparten consejos sobre cómo mantener sus identidades ocultas, encriptar mensajes y usar sistemas de pago que no dejan rastro, como criptomonedas o tokens anónimos.

[44] MIUCCI (2025).
[45] EL COMERCIO (2025).
[46] ONU (2023)
[47] ORGANIZACIÓN DE LAS NACIONES UNIDAS (2023).

En 2024, según el *Crypto Crime Report 2025* de Chainalysis, se detectaron transacciones ilícitas que sumaron más de 45 mil millones de dólares, relacionadas con actividades como ransomware, hackeos, estafas y lavado de dinero. Aunque esta cifra representa solo el 0.14% del total de transacciones en cripto, expertos advierten que el valor real podría superar los 55 mil millones debido a que constantemente aparecen nuevas direcciones vinculadas a delitos[48].

En Perú, el uso legítimo de criptomonedas también ha llevado a investigaciones penales por supuesto lavado de activos, incluso en casos donde no hay pruebas claras de delito o acuerdo entre las partes. Como explica Yandira Sapa en LP Derecho, personas sin antecedentes han sido acusadas solo por operar en plataformas como Binance o por recibir transferencias de terceros en sus cuentas bancarias[49]. Esto muestra una especie de zona gris legal, donde la falta de regulaciones claras sobre los activos digitales genera inseguridad jurídica y un riesgo real de que personas inocentes terminen siendo criminalizadas.

El Poder Judicial en Perú ha detectado un aumento muy preocupante en el lavado de activos usando plataformas virtuales, sobre todo en casos como la tala ilegal y el tráfico de especies protegidas. Según el juez supremo Víctor Prado Saldarriaga, esta forma de lavado se ha triplicado desde que empezó la pandemia[50]. Lo que la hace diferente es que se utilizan billeteras digitales anónimas para guardar y mover dinero ilegal de manera sencilla y rápida. Para hacer frente a esto, en 2024, la Superintendencia de Banca y Seguros (SBS) emitió la Resolución SBS N.º 02648-2024, que busca poner en marcha un sistema para prevenir el lavado de dinero en servicios de activos virtuales (PSAV). Esta norma pide a las empresas que gestionan estos servicios que tengan medidas para identificar a los beneficiarios, gestionar los riesgos y registrar cualquier movimiento sospechoso para que las autoridades puedan actuar a tiempo.

d) Ciberacoso, hostigamiento y *doxxing*

El acoso cibernético, el hostigamiento en línea y el doxxing —que es cuando publican sin permiso datos personales— son formas de violencia que se han vuelto más comunes, intensas y sofisticadas. Muchas veces, estas acciones se organizan desde grupos cerrados en redes sociales o foros donde los usuarios pueden mantenerse en el anonimato. Cuando se hacen a gran escala y de manera coordinada, estas prácticas pueden tener graves consecuencias físicas, psicológicas y daños a la reputación de las víctimas

Según ONU Mujeres, el doxxing afecta a más de la mitad de las mujeres que usan internet, y el 73% de las periodistas han sufrido violencia digital en su trabajo[51]. Estas cifras muestran un patrón constante de agresiones en contra de mujeres públicas, incluyendo amenazas, difamación, suplantación de identidad y ataques a su seguridad en línea.

[48] JIMENEZ (2025).
[49] SAPA (2025).
[50] PODER JUDICIAL (2023).
[51] ABIUSO Y LÓPEZ (2024).

La violencia digital no se queda solo en el mundo virtual. Diversos estudios han evidenciado que este tipo de violencia puede estar muy vinculada con problemas como el malestar psicológico, ideas suicidas y autolesiones, especialmente en adolescentes y mujeres jóvenes. Por ejemplo, en Colombia, se reportaron casos en los que intentos de suicidio estaban relacionados directamente con el acoso en redes sociales[52].En México, un estudio con más de 1,600 adolescentes reveló que quienes sufrían ciberacoso tenían niveles mucho más altos de pensamientos suicidas y malestar emocional, siendo las chicas las que más sufrían estos efectos[53].

Jurídicamente, el doxxing presenta sus propios retos. En Perú, aún no está definido como un delito separado, pero puede considerarse una violación del derecho a la intimidad, según lo establece la Constitución (artículo 2.6), o bien como acoso bajo la Ley Nº 30364. En Argentina, tampoco hay un delito específico para esto, pero puede subsumirse en delitos de amenazas, injurias o daños informáticos Ley Nº 26388. Por otra parte, la ciberinstigación en estos casos muchas veces se manifiesta como un linchamiento virtual, donde los agresores animan a otros usuarios a sumarse a campañas de odio, difamación o exposición pública. Esta instigación colectiva, muchas veces anónima, genera una responsabilidad difusa que complica los métodos tradicionales para imputar penalmente a los responsables.

e) Ataques contra infraestructuras críticas

Los ataques a infraestructuras esenciales, como las redes eléctricas, hospitales, transporte y servicios financieros, se han vuelto más frecuentes y sofisticados. Hoy en día, estos ataques representan una de las mayores amenazas en el mundo digital. Incluyen campañas de *ransomware*, sabotajes cibernéticos y ataques de denegación de servicio (DDoS). Muchas veces, estos ataques se planifican en foros cerrados y canales cifrados donde se dice a quienes podrían realizarlos qué blancos atacar, qué técnicas usar y cómo actuar.

En este escenario, la ciberinstigación cumple un papel importante al distribuir tareas, coordinar acciones y repartir la responsabilidad entre los involucrados. En lugar de que un solo atacante realice todo el ataque, los líderes del grupo actúan como cerebros logísticos en el mundo virtual, dando instrucciones sin participar directamente en el ataque. Según el “Informe sobre ransomware 2025” de Akamai Technologies, ha quedado claro que la estrategia del triple extorsión se ha consolidado, combinando: cifrado de datos, amenazas de hacer públicos los datos y ataques DDoS para paralizar servicios críticos. Grupos como Dragon RaaS y Stormous usan este método, que forma parte del modelo Ransomware-as-a-Service (RaaS). Esto permite que personas sin conocimientos técnicos avanzados puedan lanzar ataques sofisticados, facilitando así que más actores puedan participar en estas actividades ilegales[54].

[52] ESCOBAR ECHAVARRÍA y otros (2017).
[53] DOMÍNGUEZ MORA (2019)
[54] AKAMANI TECHNOLOGIES (2025).

Durante el primer trimestre de 2025, se registraron más de 2.000 víctimas de ransomware en sitios donde se publican filtraciones de datos, un aumento del 126 % en comparación con el mismo período en 2024[55]. Estos ataques afectan no solo a empresas privadas, sino también a hospitales, redes eléctricas y sistemas de transporte, generando crisis que afectan derechos fundamentales como la salud, la seguridad y el acceso a servicios básicos.

Desde el punto de vista legal, determinar quién es responsable en estos casos es complicado. Como señala Gorjón Barranco[56], en España los artículos 264 y 264 del Código Penal castigan el sabotaje cibernético cuando afecta infraestructuras críticas, y el artículo 573.2 lo considera un delito grave con fines terroristas. Sin embargo, identificar al instigador digital es difícil, especialmente cuando opera desde otros países o en redes descentralizadas.

En Perú, aunque no existe una ley específica para el sabotaje a infraestructuras críticas, la Ley Nº 30096 sobre delitos informáticos cubre el acceso no autorizado, daños e interferencias en sistemas digitales. Aun así, la doctrina penal no tiene criterios claros para responsabilizar en casos de ciberinstigación organizada, por lo que es necesario revisar cómo se atribuye culpa y participación en el ámbito digital.

f) Delitos emergentes: *sextorsión* grupal, *ransomware as a service* y delitos en el metaverso

La transformación del ciberespacio ha dado lugar a nuevas formas de criminalidad digital que son cada vez más sofisticadas, mantienen el anonimato y cruzan fronteras fácilmente. Problemas como la sextorsión en grupo, el modelo *Ransomware-as-a-Service* (RaaS) y las actividades delictivas en el metaverso muestran un escenario donde la ciber-instigación colectiva juega un papel central en la planificación, realización y difusión de conductas ilegales.

La sextorsión en grupo implica que varias personas coaccionan sexualmente a una víctima, muchas veces usando plataformas cerradas, compartiendo fotos o videos íntimos, y amenazando con difundirlo. En el metaverso, esta práctica ha tomado dimensiones nuevas: en enero de 2024, se reportó un caso donde una joven fue abusada sexualmente por un grupo de adultos en su avatar en un entorno virtual, causando daños psicológicos similares a los de una agresión física[57]. Las autoridades británicas iniciaron una investigación, aunque reconocieron que la legislación actual no contempla la agresión sexual en entornos virtuales, lo que evidencia una grave laguna normativa.

El modelo RaaS permite que ciberdelincuentes sin conocimientos técnicos específicos puedan acceder a kits de *ransomware* desarrollados por terceros, pagando suscripciones, tarifas únicas o compartiendo beneficios. Según Holdsworth y Kosinski[58], el ransomware representa alrededor del 20 % de todos los

[55] MODINI (2025)
[56] GORJÓN BARRANCO (2022)
[57] MVS Noticias (2024).
[58] HOLDSWORTH Y KOSINSKI (2024).

delitos cibernéticos, con virus como LockBit y BlackBasta que se difunden mediante este sistema, que ofrece soporte técnico, foros privados y pagos en criptomonedas. Esta estructura descentralizada hace difícil determinar quién es responsable, ya que quien realiza el ataque no siempre es el creador del malware.

El metaverso ha abierto un nuevo campo donde las leyes aún no alcanzan a regular. Se detectan cada vez más casos de suplantación de identidad, robo de activos digitales como NFTs y criptomonedas, y ataques a avatares. Según Trend Micro, el darkverse —una versión criminal del metaverso— facilita actividades ilícitas usando tokens de acceso, ubicaciones físicas específicas y un gran nivel de anonimato, lo que complica mucho el trabajo de las autoridades para vigilar y arrestar a los responsables[59]. Los delitos que ocurren en el metaverso incluyen: Robo de NFTs y monedas digitales, lavado de dinero usando bienes virtuales, extorsión con ataques DDoS y ransomware, y ataques a avatares con impactos psicológicos reales. La relación entre el mundo virtual y lo físico, donde lo virtual afecta directamente la economía y las emociones, hace necesaria una nueva forma de entender quién puede ser penalmente responsable, especialmente en casos de conspiración colectiva y sistemas legales fragmentados.

IV. ANÁLISIS COMPARADO DE LOS DESAFÍOS PROBATORIOS EN LA CIBERINSTIGACIÓN

IV.1. Identificación y atribución de responsabilidad al instigador digital

a) Manejo del anonimato y pseudonimato en Perú y Argentina

La ciberinstigación a menudo funciona escondiendo la identidad, lo que dificulta la imputación penal directa. Aunque proteger el anonimato y la pseudonimia está respaldado por derechos importantes como la privacidad y la libertad de expresión, estos aspectos se convierten en obstáculos cuando se usan para promover delitos.

Por un lado, el Perú ha ratificado el *Convenio de Budapest* sobre ciberdelincuencia, lo que habilita mecanismos de cooperación internacional y técnicas de rastreo digital[60]. Sin embargo, no existe una regulación específica sobre el uso de redes como Tor o VPN en contextos delictivos. La persecución penal se basa en rastrear técnicamente y trabajar con proveedores de servicios. Los casos judiciales sobre ciberinstigación aún son escasos, y la doctrina penal no ha desarrollado criterios sobre la imputación bajo anonimato.

Por otro lado, en Argentina el informe de Derechos Digitales destaca el tratamiento jurídico del anonimato y la pseudonimia, incluyendo el uso de herramientas como Tor y su admisibilidad como evidencia[61]. Además, se han desarrollado propuestas metodológicas para la identificación de autoría en redes sociales mediante análisis multidimensional del discurso. Asimismo, existe debate

[59] TREND MICRO (2022).
[60] MINISTERIO PÚBLICO FISCALÍA DE LA NACIÓN (2021).
[61] FALIERO E IGLESIAS (2018).

sobre el rol de plataformas digitales en la preservación de datos que permitan la identificación del instigador.

Es decir, mientras Perú se apoya en tratados internacionales y técnicas convencionales de rastreo IP, Argentina va más allá, integrando disciplinas como la lingüística forense y discutiendo sobre la responsabilidad de las plataformas digitales. No obstante, ambos países emplean software especializado para el análisis forense, como EnCase, FTK y Autopsy, y técnicas avanzadas de extracción y preservación, lo que permite reconstruir eventos digitales y vincular a los responsables con los mensajes de instigación.

b) Herramientas y técnicas de investigación forense digital en ambos países

Superar el velo del anonimato requiere herramientas forenses capaces de reconstruir la actividad digital del presunto instigador, preservando la cadena de custodia y garantizando la legalidad del procedimiento.

En el caso peruano la Unidad Especializada en Ciberdelincuencia del Ministerio Público aplica técnicas de análisis de metadatos, recuperación de archivos y rastreo de actividad en redes sociales. Aunque, enfrenta limitaciones en infraestructura, escasa formación especializada y dependencia de cooperación internacional para acceder a datos alojados fuera del país.

En el caso argentino, se han implementado guías técnicas para la obtención y preservación de evidencia digital, incluyendo el allanamiento remoto y el uso de hash para verificar integridad[62]. Además, existe una capacitación continua mediante diplomaturas, como las ofrecidas por UCASAL y UNT forman peritos en análisis forense digital, con énfasis en herramientas open source y comerciales. Aplicando técnicas de recuperación de datos móviles, análisis de blockchain y reconstrucción de actividad en la nube.

En este caso, Argentina presenta una institucionalización más avanzada del análisis forense digital, con formación especializada y protocolos técnicos consolidados. Perú, aunque alineado con estándares internacionales, enfrenta desafíos estructurales que limitan la eficacia investigativa.

IV.2. Obtención, preservación y validez de la prueba digital

La prueba digital constituye el eje probatorio en los casos de ciberinstigación. Su correcta obtención, preservación y validación jurídica son fundamentales para garantizar el debido proceso, especialmente cuando se trata de evidencias como mensajes cifrados, direcciones IP, logs de actividad o archivos en la nube. En contextos de anonimato y autoría difusa, la cadena de custodia y los peritajes informáticos adquieren un valor determinante.

[62] BENDINELLI (2024)

a) Cadena de custodia de la evidencia electrónica en la práctica peruana y argentina

La cadena de custodia es el conjunto de procedimientos técnicos y legales que aseguran la integridad, autenticidad y trazabilidad de la evidencia digital desde su recolección hasta su presentación en juicio.

En el Perú, la Resolución N.º 729-2006-MP-FN establece el reglamento de cadena de custodia para elementos materiales y evidencias digitales, incluyendo su recolección, embalaje, rotulado, almacenamiento y análisis técnico. Además, el protocolo exige que cada muestra sea identificada con lugar, fecha, responsable y características técnicas, garantizando la trazabilidad desde el levantamiento hasta el análisis forense[63].

La doctrina penal argentina ha desarrollado una visión más técnica y casuística sobre la cadena de custodia digital. Enrique Stel destaca que "sin una correcta cadena de custodia, la evidencia digital no puede ser acreditada, perseguida ni condenada"[64]. Se exige la preservación de metadatos, la aplicación de hash criptográficos y la documentación detallada de cada intervención sobre el dispositivo o archivo digital.

Mientras que Perú cuenta con un marco normativo formal, pero enfrenta desafíos operativos en la implementación. Argentina, en cambio, ha desarrollado una doctrina técnica más robusta, con énfasis en la confiabilidad y la pericia especializada.

b) La función de los peritajes informáticos en los procesos judiciales

El peritaje informático es el análisis técnico de evidencias digitales realizado por expertos certificados, con el fin de determinar su autenticidad, origen, manipulación y relevancia jurídica.

En el caso peruano, los peritos informáticos del Poder Judicial están certificados para intervenir en casos penales, civiles y administrativos. Su labor incluye recuperación de datos, análisis de logs, autenticación de mensajes y reconstrucción de actividad digital[65]. Y en casos de ciberinstigación, su rol es clave para vincular al presunto instigador con la evidencia digital, especialmente cuando se opera bajo pseudonimato o en redes cifradas.

Mientras que, en el caso de Argentina, los peritos informáticos judiciales actúan como asesores técnicos en tribunales, elaborando informes periciales que autentican correos, mensajes de WhatsApp, redes sociales y sitios web[66]. Además, se emplean técnicas OSINT, análisis de blockchain y reconstrucción de actividad en sistemas operativos, lo que permite atribuir responsabilidad incluso en entornos descentralizados.

[63] Ministerio Público del Perú (2006).
[64] STEL (2020).
[65] DURIVA (2024).
[66] PERITOS INFORMÁTICOS (2024).

IV.3. Desafíos en la cooperación judicial internacional

La ciberinstigación transnacional plantea desafíos complejos en materia de cooperación judicial, especialmente cuando los delitos se cometen desde jurisdicciones distintas, bajo anonimato y mediante plataformas descentralizadas.

La atribución de responsabilidad penal depende no solo de la identificación técnica del instigador, sino también de la coordinación entre sistemas jurídicos, la compatibilidad normativa y la ejecución efectiva de medidas probatorias.

a) Mecanismos de asistencia mutua entre Argentina y Perú en casos de ciberinstigación transnacional

Existe entre Argentina y Perú el Acuerdo de Asistencia Judicial en Materia Penal[67] en 1999, vigente desde 2001, que establece mecanismos de cooperación para investigaciones, enjuiciamientos y procedimientos penales. Este acuerdo contempla:

- Localización e identificación de personas y bienes
- Intercambio de pruebas y documentos
- Ejecución de registros e inspecciones
- Recepción de testimonios e interrogatorios
- Embargo, secuestro y decomiso de bienes
- Participación de autoridades extranjeras en diligencias probatorias

Aunque el acuerdo no menciona expresamente delitos informáticos, su redacción permite incluirlos. Sin embargo, la ejecución de medidas coercitivas (como interceptación de comunicaciones o allanamientos digitales) requiere que el hecho esté tipificado como delito en ambos países y que exista consentimiento expreso o autorización judicial.

b) Conflictos de jurisdicción y ley aplicable en el ciberespacio

La naturaleza del ciberespacio plantea retos sustantivos a las nociones clásicas de territorialidad y soberanía. En este entorno, una conducta delictiva puede gestarse en un país, ejecutarse técnicamente desde otro y producir efectos sobre víctimas situadas en diversas jurisdicciones. Este carácter transnacional genera conflictos en la determinación de la competencia y complica la identificación de la ley aplicable.

En el contexto peruano, Mendoza[68], sostiene que el ciberespacio “modifica la probabilidad de definición del lugar de procesamiento o castigo del hecho”, lo que deriva en una indeterminación jurisdiccional y, en algunos casos, en el abandono de investigaciones por la ausencia de una atribución territorial precisa. Por su parte, en el ámbito argentino, la doctrina identifica al ciberespacio como un “metapaís posgeográfico”, cuya naturaleza exige abordar las relaciones jurídicas desde una perspectiva supranacional. En esta línea, se considera que “las

[67] Gobierno del Perú y Biblioteca de Tratados de Cancillería Argentina.
[68] MENDOZA (2022).

consecuencias jurídicas de la tecnología han superado los límites locales", demandando así respuestas coordinadas entre Estados[69].

En este marco, se advierten tres desafíos centrales: i) determinar el lugar de comisión del delito, especialmente en casos de instigación digital. ii) establecer la competencia judicial sin transgredir la soberanía de otro Estado, y iii) aplicar de forma efectiva las normas penales nacionales frente a conductas transfronterizas que carecen de una regulación específica.

V. CONCLUSIONES

El análisis de la ciberinstigación en el contexto jurídico-penal de Argentina y Perú permite constatar que se trata de un fenómeno criminal complejo, caracterizado por su anonimato, masividad y alcance transnacional, lo que lo distingue sustancialmente de la instigación tradicional. Estas particularidades generan retos específicos para su tipificación, investigación y sanción, así como para la preservación de derechos fundamentales como la libertad de expresión y la privacidad.

En el plano dogmático, ambos países coinciden en concebir la instigación como una forma de participación criminal que exige: a) determinación psíquica del autor, b) dolo de instigar y c) nexo causal entre la inducción y el delito cometido. Sin embargo, las diferencias surgen en el grado de precisión legislativa y en la interpretación jurisprudencial. Argentina, mediante sus artículos 45 y 209 del Código Penal, introduce exigencias expresas sobre la "determinación directa" y cuenta con precedentes que afinan su alcance; mientras que el Perú, aunque equipara la pena de la instigación a la autoría, artículo 24 del Código Penal, presenta mayor escasez de desarrollo jurisprudencial en entornos digitales.

En el ámbito probatorio, ambos sistemas afrontan dificultades para identificar al instigador digital, especialmente por el uso de pseudónimos, cifrado extremo a extremo y plataformas descentralizadas. Si bien los dos países han adoptado herramientas de informática forense, Argentina presenta una institucionalización más robusta en cuanto a protocolos técnicos, formación de peritos y uso de metodologías multidisciplinarias, mientras que Perú se apoya más en cooperación internacional y en estándares generales del Convenio de Budapest.

En lo operativo, se observa que las manifestaciones de la ciberinstigación abarcan desde redes sociales, foros en la dark web y aplicaciones de mensajería cifrada, hasta nuevos entornos como metaversos y redes descentralizadas. Los delitos en que cobra mayor relevancia incluyen estafas masivas, delitos de odio y radicalización, tráfico de material ilícito, ciberacoso, ataques contra infraestructuras críticas y conductas emergentes como el Ransomware-as-a-Service o la sextorsión grupal.

Finalmente, a través de la investigación comparada se muestra que, aunque existen bases normativas y operativas comunes, la ausencia de un tipo penal autónomo de ciberinstigación y de protocolos probatorios especializados limita la

[69] MONTOTO (1999).

eficacia de la persecución penal. A esto se suma la necesidad de armonizar marcos legislativos, reforzar la cooperación judicial y adoptar un enfoque adaptado a la naturaleza cambiante de la criminalidad digital.

VI. PROPUESTAS

1) Tipificación autónoma de la ciberinstigación: Se debe incorporar en los Códigos Penales de ambos países un tipo específico que regule la instigación cometida a través de medios digitales, incluyendo circunstancias agravantes por uso de tecnologías de cifrado, plataformas masivas o alcance transnacional. Además, diferenciar la ciberinstigación de figuras próximas como, la complicidad o la incitación pública, evitando solapamientos normativos. Además, se debe promover, en el marco del Convenio de Budapest y foros regionales como la OEA, criterios uniformes sobre definición, elementos y sanciones de la ciberinstigación. Y facilitar que la cooperación internacional se active sin obstáculos de doble incriminación, asegurando que las conductas sean punibles en jurisdicciones vinculadas.

2) Protocolos especializados de investigación y preservación de evidencia digital: Se debe establecer guías técnicas comunes para la obtención, preservación y análisis de pruebas electrónicas, incluyendo el uso obligatorio de valores hash, documentación exhaustiva de la cadena de custodia y estándares de autenticación de mensajes cifrados. Asimismo, desarrollar unidades de respuesta rápida para intervenciones digitales urgentes, especialmente en delitos en curso. Asimismo, se debe capacitar jueces, de manera frecuente, fiscales y peritos en técnicas avanzadas de análisis de blockchain, OSINT, lingüística forense y rastreo en redes cifradas. Además, crear laboratorios forenses especializados en entornos virtuales emergentes (metaversos, redes descentralizadas) para identificar conductas y actores relevantes.

3) Cooperación judicial y operativa efectiva: Se propone fortalecer la cooperación judicial y operativa entre Argentina y Perú mediante la revisión y ampliación de acuerdos bilaterales que incluyen expresamente los delitos informáticos y habiliten medidas como el allanamiento digital remoto, el intercambio inmediato de metadatos y la participación conjunta en diligencias virtuales. Ello debe complementarse con la creación de canales seguros de comunicación interinstitucional y el establecimiento de equipos conjuntos de investigación (ECI) para casos de carácter transnacional. Paralelamente, resulta esencial impulsar campañas de alfabetización digital dirigidas a usuarios vulnerables —como menores y adultos mayores—, orientadas a la detección temprana de intentos de ciberinstigación y la denuncia oportuna de conductas sospechosas.

La ciberinstigación constituye uno de los retos más urgentes para el derecho penal contemporáneo. Su naturaleza mutable, capacidad de alcance masivo y facilidad para el anonimato demandan que las respuestas jurídicas sean ágiles,

coordinadas y técnicamente sofisticadas. Argentina y Perú comparten desafíos y oportunidades: ambos pueden fortalecer sus marcos normativos, mejorar su capacidad probatoria y potenciar su cooperación bilateral. En un escenario donde los límites entre lo virtual y lo real se diluyen, la efectividad de la persecución penal dependerá de la adaptabilidad del sistema de justicia a la dinámica acelerada de la criminalidad digital.

VII. BIBLIOGRAFÍA

ABIUSO, Marina Y LOPEZ, Julia (2024). *Violencia y acoso digital: Herramientas de acción para periodistas*, Red de Editoras de Género, UNFPA, UNICEF, PNUD y ONU.

AKAMAI TECHNOLOGIES (2025). Ransomware: Nuevas tácticas de extorsión. Recuperado de https://t21.pe/ransomware-nuevas-tacticas-extorsion. Fecha de consulta: 14/08/2025.

ANDINA (2025). Advierten de nueva modalidad de estafa y extorsión a usuarios de Telegram. Disponible en: https://andina.pe/agencia/noticia-atencion-advierten-nueva-modalidad-estafa-y-extorsion-a-usuarios-telegram-930476.aspx. Fecha de consulta: 10/08/2025

ARGENTICA.GOR.AR (2024). Operación protección de la infancia IV: rescatamos a 70 menores víctimas de trata y abuso sexual. Disponible en: https://www.argentina.gob.ar/noticias/operacion-proteccion-de-la-infancia-iv-rescatamos-70-menores-victimas-de-trata-y-abuso. Fecha de consulta: 11/08/2025

ARIMETRICS, (*s/f*). Qué es Tor. Disponible en: https://www.arimetrics.com/glosario-digital/tor. Fecha de consulta: 11/08/2015.

BACIGALUPO ZAPATER, Enrique (1994): *Lineamientos de la Teoría del delito* (Buenos Aires, Editorial Hammurabi, tercera edición).

BELCIC, Ivan y CORRIGAN, Caroline (2024). Las mejores aplicaciones de mensajería cifrada. Disponible en: https://www.avg.com/es/signal/secure-message-apps. Fecha de consulta: 11/08/2025

BENDINELLI, Maximiliano (2024). “La evidencia digital en la lucha contra el ciber crimen: desafíos en su obtención, preservación y uso en Argentina”. *Cuadernos Argentinos de Ciencias Forenses*, Año 2, N.º 1: pp. 62-73.

CALDERÓN, Camila (2025). Ciberdelincuencia en Perú: los casos más comunes, cuáles son las técnicas utilizadas y qué hacen las operadoras.

Disponible: https://www.infobae.com/peru/2025/02/21/ciberdelincuencia-en-peru-los-casos-mas-comunes-cuales-son-las-tecnicas-utilizadas-y-que-hacen-las-operadoras/. Fecha de consulta: 10/08/2025

CHAUCA ALENDEZ, Nicol (2025). Códigos QR, phishing y robo de cuentas: delitos informáticos en Perú podrían duplicarse este 2025. Disponible en: https://www.infobae.com/peru/2025/08/13/codigos-qr-phishing-y-robo-de-cuentas-delitos-informaticos-en-peru-podrian-duplicarse-este-2025/. Fecha de consulta: 14/08/2025.

CLYBE (2025). Los 10 mejores foros de la Dark Web y la Deep Web de 2025. Disponible en: https://cyble.com/knowledge-hub/top-10-dark-web-forums/. Fecha de consulta: 11/08/2025.

DERGARABEDIAN, César (2021). Discord: una plataforma atractiva para cibercriminales". Disponible en: https://www.iprofesional.com/tecnologia/346070-discord-una-plataforma-atractiva-para-cibercriminales. Fecha de consulta: 10/08/2025

DOMÍNGUEZ MORA, Raquel. Y VARGAS JIMÉNEZ, Esperanza y CASTRO CASTAÑEDA, Remberto y MEDINA CENTENO, Raúl, y HUERTA ZÚÑIGA, Claudia Gregoria (2019). "Ciberacoso como factor asociado al malestar psicológico e ideación suicida en adolescentes escolarizados mexicanos", *Acta Universitaria*, Vol. 29 N.° 1: pp. 205–218.

DURIVA (2024). Perito en sistemas informáticos en Perú. Disponible en: https://duriva.com/servicio-pericial/perito-en-sistemas-informaticos-en-peru/. Fecha de consulta: 12/08/2025.

EL COMERCIO (09/08/2025): "¿Por qué seguimos cayendo en el phishing? La trampa más vieja de internet aún domina en el Perú y ni las empresas se salvan". Disponible en: https://elcomercio.pe/tecnologia/ciberseguridad/por-que-seguimos-cayendo-en-el-phishing-la-trampa-mas-vieja-de-internet-aun-domina-en-peru-y-ni-las-empresas-se-salvan-noticia/. Fecha de consulta: 14/08/2025.

ESCOBAR ECHAVARRÍA, Juliana y MONTOYA GONZÁLEZ, Laura Elisa y RESTREPO BERNAL, Diana y MEJÍA RODRÍGUEZ, David (2017). "Ciberacoso y comportamiento suicida. ¿Cuál es la conexión? A propósito de un caso", *Revista Colombiana de Psiquiatría,* Vol. 46, N.° 4: pp. 247-251.

FALIERO, Johanna e IGLESIAS, Rodrigo (2018). Informe de investigación operación y uso de herramientas de privacidad y anonimato en Argentina. (Buenos Aires, Derechos Digitales).

FISCALÍA DE LA NACIÓN. (2006). Resolución de la Fiscalía de la Nación N.º 729-2006-MP-FN.

FISCALÍA GENERAL DEL ESTADO (2023): *Deep web: nuevas criminalidades*, en *Boletín de derecho penal IUS Criminale* (Quito, Fiscalía General del Estado). RODRÍGUEZ ZAMBRANO, Henry (2025). 'Dark web': una amenaza oculta y latente en América Latina

GARCÍA CAVERO, Percy (2019*): Derecho penal. Parte general*, (Lima, Editorial Ideas Soluciones).

GORJÓN BARRANCO, María Concepción (2022). "Sabotaje informático a infraestructuras críticas: análisis de la realidad criminal recogida en los artículos 264 y 264 bis del Código Penal. Especial referencia a su comisión con finalidad terrorista", *Revista de Derecho Penal y Criminología*, Vol. 3, N.º 25: pp 77-124.

HOLDSWORTH, Jim y KOSINSKI, Matthew (2024). ¿Qué es el ransomware como servicio (RaaS)? Disponible en: https://www.ibm.com/es-es/think/topics/ransomware-as-a-service. Fecha de consulta: 12/08/2025.

HURTADO POZO, José y PRADO SALDARRIAGA, Víctor (2011): *Manual de Derecho Penal. Parte General*, Tomo II (Lima, Ediciones Idemsa).

JIMENEZ ROMERO, Katha (2025). Chainalysis reveló que el crimen cripto marcó cifra récord de USD 45 mil millones en 2024. Disponible en: https://es.cointelegraph.com/news/chainalysis-revealed-that-crypto-crime-set-record-high-of-usd-45-billion-in-2024. Fecha de consulta: 14/08/2025.

KASPERSKY (*s/f*). ¿Qué es un firewall? Definición y explicación. Disponible en: https://latam.kaspersky.com/resource-center/definitions/firewall. Fecha de consulta: 11/08/2025.

LA REPÚBLICA (18/03/2017): "Facebook: La PNP identificó al sujeto que incitaba a cometer saqueos". Disponible en: https://larepublica.pe/sociedad/857612-la-pnp-identifico-al-sujeto-que-incitaba-en-facebook-cometer-saqueos. Fecha de consulta: 02/08/2025.

MALDITA.ES (2023): *Qué se sabe de los retos virales peligrosos que circulan en TikTok*. Disponible en: https://maldita.es/sociedad/20230413/retos-virales-tiktok-challenge. Fecha de consulta: 01/08/2025.

MARIANA DÍAZ, Correa y RESTREPO RAMOS, Santiago y GONZÁLEZ GARCÍA, Daniela (2024): "Videojuegos online multijugador como entornos digitales posibilitadores de la interacción digital", Centro de Estudios en Diseño y Comunicación, Cuaderno 214: pp. 169 – 183.

MELIÁN, Guadalupe. (2025). Deepfakes: algoritmos que delinquen. Disponible en: https://elanalista.com.ar/deepfakes-algoritmos-que-delinquen. Fecha de consulta: 10/08/2025

MENDOZA MALPARTIDA, Hugo. (2022). El ciberespacio y la problemática de la aplicación espacial de la ley penal: el ciberdelito y su jurisdiccionalidad. Disponible en: https://lpderecho.pe/el-ciberespacio-y-la-problematica-de-la-aplicacion-espacial-de-la-ley-penal-el-ciberdelito-y-su-jurisdiccionalidad/. Fecha de consulta: 12/08/2025.

MENDOZA RIOFRÍO, Marcela (2024). Deepfakes: una realidad ante la que estar alerta. Disponible en: https://ebiz.pe/noticias/deepkfakes-una-realidad-ante-la-que-estar-alerta. Fecha de consulta: 10/08/2025

MEZA CAPCHA, Evelin (2025). Criptomonedas: las tres amenazas más comunes y cómo protegerte, según expertos. Disponible en: https://www.infobae.com/peru/2025/08/01/criptomonedas-las-tres-amenazas-mas-comunes-y-como-protegerte-segun-expertos. Fecha de consulta: 10/08/2025

MINISTERIO PÚBLICO FISCAL (*s/f)*. "Narcomenudeo: cae usuario que vendía drogas sintéticas por telegram y secuestran gran cantidad de estupefacientes. Disponible en: https://mpfciudad.gob.ar/noticias/narcomenudeo-cae-usuario-que-vendia-drogas-sinteticas-por-telegram-y-secuestran-gran-cantidad-de-estupefacientes. Fecha de consulta: 10/08/2025

MIR PUIG, Santiago (2015): *Derecho Penal*. *Parte General* (Montevideo, Editorial B de F Ltda, décima edición).

MODINI, Tomás (2025). La evolución del ransomware: por qué 2025 se convirtió en el año más peligroso. Recuperado de: https://www.innovaciondigital360.com/cyber-security/la-evolucion-del-ransomware-por-que-2025-se-convirtio-en-el-ano-mas-peligroso/. Fecha de consulta: 14/08/2025.

MONTOTO GUERREIRO, José Luis (1999). Ciberespacio: aproximación a temas de jurisdicción y ley aplicable. Disponible en: https://www.saij.gob.ar/doctrina/dacf000113-montoto_guerreiro-ciberespacio_aproximacion_temas_jurisdiccion.htm. Fecha de consulta: 12/08/2025.

MVS NOTICIAS (03/01/2024). "Delitos en el Metaverso: El avatar de una joven es abusado por un grupo de hombres adultos". Disponible en: https://mvsnoticias.com/tendencias/ciencia-tecnologia/2024/1/3/delitos-en-el-

metaverso-el-avatar-de-una-joven-es-abusado-por-un-grupo-de-hombres-adultos-620757.html. Fecha de consulta: Fecha de consulta: 14/08/2025.

PRADO SALDARRIAGA, Víctor Roberto (2023). *Lavado de activos virtuales. Nueva tipología del crimen organizado en Perú,* (Lima, Editorial Gaceta Jurídica).
PRIETO, Marina Lucía (2013): "Construcciones sociales en Facebook. Saqueos durante una huelga policial (Argentina, 2013)", Revista Ágora de heterodoxias, vol. 4, N° 2: pp. 129-138.

RAÚL ZAFFARONI, Eugenio (2006): *Manual de Derecho Penal. Parte general,* (Buenos Aires, Editorial Ediar, segunda edición).

REVISTA CLOUD (2024). Telegram y el cifrado de extremo a extremo. Disponible en: https://revistacloud.com/telegram-y-el-cifrado-de-extremo-a-extremo/. Fecha de consulta: 11/08/2025

SALVADOR RAMÍREZ, Catalina Tania, (2024). "La impunidad en los delitos informáticos. Una problemática de poco interés para legisladores, jueces y fiscales". *Revista de Investigación de la Corte Superior de Justicia de Huánuco*, Vol. 7, N.° 9: pp. 91-115.

SAPA ORURO, Yandira (2025). ¿Trading o delito? Cómo el uso legítimo de criptomonedas puede llevarte a una investigación penal en Perú. Disponible en: https://lpderecho.pe/trading-delito-como-uso-legitimo-criptomonedas-llevarte-investigacion-penal-peru/. Fecha de consulta: 14/08/2025.

STEL, Enrique. (2020). La cadena de custodia de la evidencia digital. Disponible en: https://prisioneroenargentina.com/la-cadena-de-custodia-de-la-evidencia-digital/. Fecha de consulta: 12/08/2025.

SUPREMA CORTE DE JUSTICIA DE LA PROVINCIA DE BUENOS AIRES, 23/12/2020, causa P. 131.348, *Altuve, Carlos Arturo s/ Recurso extraordinario de inaplicabilidad de ley*.

TORRES MALCA, Harold Alexis (2024). El fenómeno de los deepfakes y sus consecuencias legales frente al delito de suplantación de identidad en el Perú. Tesis para optar el grado académico de bachiller en Derecho en la Facultad de Derecho y Humanidades de la Universidad Señor de Sipán.

TREND MICRO (2022). Darkverse: el lado oscuro del metaverso. Disponible en: https://www.revistaciberseguridad.com/2022/09/darkverse-el-lado-oscuro-del-metaverso/. Fecha de consulta: 12/08/2025.

UFECI, (2025). Informe 2024 Casos y modalidades reportadas a UFECI. Ministerio Público Fiscal.

UNESCO. (2023). Encuesta sobre el impacto de la desinformación y el discurso de odio en línea. UNESCO.

X (2025): *Políticas de seguridad*. Disponible en: https://help.x.com/es/rules-and-policies/x-rules. Fecha de consulta: 01/08/2025.

VIII. LEGISLACIÓN CITADA

ARGENTINA, *Código Penal de la Nación* (29/10/1921).

PERÚ, *Código Penal* (/ /1991).

IX. JURISPRUDENCIA CITADA

PERÚ, CORTE SUPREMA DE JUSTICIA DE LA REPÚBLICA, SALA PENAL TRANSITORIA, Recurso de Nulidad N.º 1045-2019, Lima, 22/06/2021.