La Extorsión Digital como delito transnacional: La responsabilidad penal de las plataformas digitales y la automatización delictiva

Digital Extortion as a Transnational Crime: The Criminal Liability of Digital Platforms and Criminal Automation

Alvaro Daniel Lujan Zúñiga
Estudiante Investigador
Universidad Católica Sedes Sapientiae
Los Olivos, Perú
https://orcid.org/0009-0002-5308-8184

https://doi.org/10.59659/rifed.v13.2025.ch06

Resumen

En este trabajo se analizará el delito de extorsión como un fenómeno penal complejo, el cual requiere repensar las categorías dogmáticas clásicas del Derecho Penal a la luz de los avances tecnológicos y dentro del entorno digital actual. Se plantea la discusión sobre si este delito debe considerarse de naturaleza común cometido por medios digitales o si encaja dentro del ámbito de los delitos informáticos. Adicionalmente, se estudiará la necesidad de incorporar una perspectiva ética en el diseño y funcionamiento de algoritmos de los sistemas informáticos, pues se considera que muchas plataformas digitales pueden llegar a ser instrumentalizadas para facilitar conductas delictivas sin asumir responsabilidad penal alguna. La investigación se desarrolla desde una perspectiva interdisciplinaria, articulando y fusionando elementos del derecho penal, la ética tecnológica y el derecho internacional. Metodológicamente, se ha determinado conveniente emplear el enfoque cualitativo (teórico-dogmático), así como revisión doctrinal, análisis normativo comparado y estudios de casos. El trabajo está estructurado en tres partes académicas: (i), revisión del tipo penal de extorsión y su ejecución mediante medios digitales; (ii), el análisis de la imputación objetiva para determinar la posible responsabilidad de las plataformas tecnológicas. Se espera contribuir a una discusión crítica sobre la necesidad de adaptar categorías dogmáticas frente a los nuevos avances tecnológicos y escenarios digitales, además, de explorar propuestas normativas que permitan una respuesta jurídica

más eficiente a la extorsión digital.

Palabras clave
Extorsión Digital, Ciberdelincuencia, Ética Algorítmica, Automatización delictiva, responsabilidad penal, Automatización delictiva.

Abstract

This paper analyzes the crime of extortion as a complex criminal phenomenon, which requires a rethinking of the classic dogmatic categories of criminal law in light of technological advances and within the current digital environment. It raises the question of whether this crime should be considered a common crime committed through digital means or whether it falls within the scope of cybercrime. Additionally, it will explore the need to incorporate an ethical perspective in the design and operation of computer system algorithms, since it is considered that many digital platforms can be exploited to facilitate criminal conduct without assuming any criminal liability. The research is conducted from an interdisciplinary perspective, articulating and merging elements of criminal law, technological ethics, and international law. Methodologically, it has been determined appropriate to employ a qualitative (theoretical-dogmatic) approach, as well as a doctrinal review, comparative normative analysis, and case studies. The paper is structured in three academic parts: (i) a review of the criminal offense of extortion and its execution through digital means; (ii) the analysis of objective imputation to determine the potential liability of technology platforms. The aim is to contribute to a critical discussion on the need to adapt dogmatic categories to new technological advances and digital scenarios, in addition to exploring regulatory proposals that allow for a more efficient legal response to digital extortion.

Keywords
Digital Extortion, Cybercrime, Algorithmic Ethics, Criminal Automation, Criminal Liability, Criminal Automation.

INTRODUCCIÓN

Desde la creación de la teoría de la imputación objetiva, los delitos han pasado por una evolución que ha propiciado la creación de nuevas formas de interpretación penal, surgiendo nuevas conductas humanas contrarias a las leyes. En la era de la revolución digital, han nacido nuevas formas de cometer delitos, como la extorsión digital. Consecuentemente, las nuevas tecnologías de la información, han traído consigo nuevos contextos digitales, como las plataformas digitales y las redes sociales, lo que ha propiciado que las personas puedan utilizarlas como herramientas o instrumentos para la comisión de delitos, pues brindan anonimato y mantenerse al margen de cualquier responsabilidad penal y/o persecución. Esta situación, plantea interrogantes urgentes respecto a la imputación objetiva, la dogmática penal y el rol de los algoritmos en la facilitación de conductas ilícitas que, por desarrollarse dentro de un entorno digital sin barreras físicas, trascienden las fronteras de los países convirtiéndose en un delito trasnacional, lo que a su vez plantea la interrogante: ¿la extorsión digital es un delito común o especial?

METODOLOGÍA

La presente investigación analiza el delito de la extorsión cometido a través de medios digitales desde una perspectiva interdisciplinaria y se enfoca en los desafíos que implica su calificación penal, los vacíos que pueden estar presentes en la tipificación de este delito y también estudiar la necesidad de integrar una ética algorítmica que impida la instrumentalización de sistemas digitales y automatizados para fines delictivos, con la utilización la revisión bibliográfica y un enfoque cualitativo.

Capítulo I
El delito de extorsión y su evolución hacia el contexto digital

La extorsión es un delito que ha sido modificado en numerosas ocasiones dentro de la legislación penal peruana. Estas modificaciones se pueden explicar, según Salinas (2018) por el incremento de realización de este delito en la sociedad, por lo que obligó al legislador ejercer medidas destinadas a tranquilizar a los ciudadanos. Sin embargo, proponemos que este fenómeno también se puede explicar por la constante evolución típica del delito a través del tiempo, ya que desde su primera modificación en el año 1998 coincide con el inicio de los cambios en las dinámicas sociales que trajeron consigo las nuevas tecnologías cibernéticas en los campos de la economía y de la comunicación. La apertura de los medios digitales trajo consigo un nuevo medio para cometer este delito, por ejemplo, mediante correos electrónicos o mensajes de texto, además se facilitó tener acceso a información personal de los usuarios por terceros. Pero primero, analizaremos la tipicidad objetiva de este delito, pues al ser uno de tipo que se puede realizar por una variedad de medios, se debe determinar la conducta típica del sujeto activo para ser encuadrada correctamente en la norma penal.

La extorsión está tipificada en el artículo 200 del Código Penal Peruano, convirtiéndolo en un delito común, pues se encuentra en el Título V referente a los delitos contra el patrimonio, por lo que analizaremos lo que se establece en su primer párrafo:

> **Artículo 200.- Extorsión**
>
> 200.1. El que mediante violencia o amenaza obliga a una persona o a una institución pública o privada a otorgar al agente o a un tercero una ventaja económica u otra ventaja indebida u otra ventaja de cualquier otra índole será reprimido con pena privativa de la libertad o menor a diez ni mayor de quince años […]. (Código penal peruano, 1991)

De acuerdo a la imputación objetiva, las acciones son la utilización de la violencia o amenaza para obligar a una persona o institución pública o privada (sujeto pasivo) para que esta otorgue una ventaja económica u otra de cualquier otra índole de manera indebida, es decir, ilegítimamente. En esta primera parte del artículo se hace referencia a la extorsión genérica o básica, puesto que se configura cuando el agente activo, utilizando la violencia o amenazando a la víctima o sujeto pasivo, la obliga a entregarle o a otra persona, una ventaja de índole patrimonial o de otra naturaleza en contra de su voluntad. (Salinas, 2018, p.497)

En esta primera parte, la norma se limita a identificar a los sujetos y la acción típica o verbo rector que configuran el delito de la extorsión, por lo que, desde un punto de vista dogmático, la extorsión implica la coacción ilegítima ejercida sobre la voluntad de la víctima, una afectación directa a la libertad de autodeterminación y lo que trae como consecuencia negativa que menoscaba el patrimonio o la disposición de derechos. Para Roxín (1997), el delito de la extorsión es uno en que se necesita la intensión de enriquecerse o hacerlo a favor de otro de manera injusta, por lo que para lograr esta finalidad es necesaria la utilización de medios coercitivos para obligar a la víctima a disponer de sus bienes patrimoniales. Del mismo modo, Jescheck (2014) concluye que este delito tiene como característica fundamental la amenaza que condiciona a la víctima a cometer actos contrarios a sus intereses patrimoniales, lo que consiste en un propósito económico por parte del agente o autor del delito, por lo que es distinto al robo, ya que no existe un apoderamiento físico directo, sino un desplazamiento de bienes por coacción.

Las siguientes modificaciones incorporaron los numerales 222.2, 200.3, 200.4, 200.5 y 200.6, y para el desarrollo y comprensión de la evolución de este delito, es necesario mencionar que la ley también determina la comisión mediante la utilización de imágenes del entorno familiar o de otro como el empresarial, laboral o social de la víctima para ser difundidos directa o indirectamente. (Código penal, 1991, art. 206)

Estas modificaciones y agregados fueron realizados mediante el Decreto Legislativo 982, publicado el 22 de julio de 2007, y otros, por lo que es posible hacer la afirmación que la tipificación de la conducta delictiva ha experimentado una evolución jurídico – social, tanto en relación al contexto como con el agente activo. Esta evolución puede responder a que el legislador consideró conveniente adaptar la norma a las nuevas formas delictivas, modos más complejos de operar y la diversificación de actores involucrados. Bajo el análisis histórico legal de la extorsión, en sus inicios este se entendía como una amenaza o uso de la violencia para obtener dinero o algún bien, sin embargo, el tipo penal se ha extendido al surgimiento de otras formas de coacción más complejas, como el engaño, el ardid, la simulación de contratos (Código penal, 1991, art. 200.2) o el uso de imágenes de índole familiar, laboral o empresarial (200.6.f). Los contantes cambios que ha sufrido la norma sustantiva, además de la deficiente precisión por parte del legislador, se manifiesta en el desorden, ampliación excesiva y falta de prevención hacia el futuro, este método de control penal solo se enfoca en el intento de disminuir el acto delictivo a través de la represión y no ataca el origen del problema en el ámbito social. (Cabrera, 2014, citado en Bonifacio, 2019)

La evolución normativa de este delito en el ordenamiento penal peruano refleja un intento de adaptación frente a las transformaciones sociales, culturales y tecnológicas que han modificado y ampliado las formas en que se comete este ilícito. Esto evidencia la necesidad de ampliar la compresión del tipo penal, incorporando nuevas modalidades comisivas que, si bien conservan la esencia de la coacción patrimonial, ahora se manifiestan en contextos cada vez más complejos, como el entorno digital. Esta progresión normativa y dogmática permite advertir cómo la extorsión ha dejado de ser un delito exclusivamente físico o presencial por la diversificación de métodos extorsivos, para convertirse, en muchos casos, en un fenómeno virtual que desafía los marcos tradicionales del derecho penal, por lo que es necesaria una política criminal más sofisticada y contextualizada frente a un fenómeno delictivo en expansión.

Capítulo 2
Extorsión Digital: plataformas digitales y automatización delictiva

La conducta típica del criminal que busca beneficiarse patrimonialmente de la víctima mediante el empleo de coacción, violencia o amenaza, configura la extorsión. La finalidad es la obtención de dinero o bienes de manera ilegítima, se llega a este objetivo por distintos medios y utilización de diversas herramientas. Como se ha desarrollado, la norma penal ha sufrido modificaciones y agregados posteriores en razón de los nuevos medios que surgieron a través del tiempo. Por ello, la categorización de la extorsión mediante medios digitales plantea una disyuntiva en el ámbito jurídico: ¿nos encontramos ante un delito común dentro de un nuevo medio o ante un acto de criminalidad en entornos informáticos que exige un tratamiento normativo especial?, para responder esta incógnita no solo basta con el análisis teórico, sino también es necesario el análisis de casos concretos que han sucedido en la realidad práctica. En el 2024 una entidad bancaria importante sufrió la vulneración de sus bases de datos y se filtraron datos personales de una gran cantidad de ciudadanos. En un artículo periodístico titulado "Robo de datos en Interbank al descubierto: así operó el hacker para extraer información de clientes del banco", Paucar (2024) narró que un acontecimiento alarmante se produjo el 30 de octubre de 2024, en materia de los servicios digitales de la entidad bancaria Interbank del Perú, ya que sus servicios experimentaron interrupciones significativas. Paralelamente, un individuo bajo el seudónimo de "kzoldiyck" afirmó que obtuvo acceso no autorizado a los sistemas del banco, sustrayendo aproximadamente 3.7 terabytes de información y datos sensibles de alrededor de tres millones de clientes. La información personal comprometida consistía en nombres completos, números de tarjetas, números de teléfono, fechas de nacimiento, documentos de identidad y detalles de transacciones bancarias. El ciberdelincuente intentó extorsionar al banco Interbank, exigiendo un pago de 4 millones de dólares a cambio de no divulgar la información personal de los clientes robada o vender la data sustraída. Ante la negativa del banco a cumplir

con las demandas, el atacante comenzó a liberar fragmentos de los datos en foros de la dark web, exponiendo la información personal de los clientes afectados.

El delito de extorsión ha evolucionado con el progreso tecnológico en las áreas digitales de comunicación y conexión de las redes sociales y/o plataformas digitales dedicadas al comercio de bienes y servicios. Es por ello que ya no se puede perseguir e investigar como un delito común cuando se comete mediante medios que no son comunes, este fenómeno de evolución criminal supone una forma más compleja y especializada de persecución penal, porque el uso de herramientas tecnológicas ha permitido que su comisión sea más rápida, inmediata, accesible y, sobre todo, envuelta en la protección del anonimato. Esta transformación, representa un desafío adicional cuando la víctima es un ciudadano que solo utiliza los medios tecnológicos, pero no sabe de su funcionamiento interno, ni cuenta con los medios necesarios para poder protegerse en el ámbito digital y esto lo sitúa en una posición de vulnerabilidad extrema. A diferencia de grandes empresas privadas o entidades estatales, los ciudadanos comunes no poseen los medios para protegerse eficazmente ante el ataque de su privacidad o de sus datos personales, ni cuentan con mecanismos reales para poder identificar al extorsionador, además existe la posibilidad de que su situación de vulnerabilidad digital se agrave aún más cuando la víctima es un menor de edad o persona adulta mayor. Dentro de este contexto, se han identificado las prácticas delictivas más utilizadas por los cibercriminales para obtener de sus víctimas algún dato personal o de índole íntimo que le sirva como insumo para obtener algún beneficio indebido:

Por ello, en el desarrollo de este trabajo, nos enfocaremos en el análisis de la modalidad denominada “sextorsión”, que según Goicochea (2018) es la práctica que se realiza a través de redes sociales y tecnologías de la información consistente en amenazar a una persona con publicar y difundir, a través de la red, material audiovisual en donde se vea comprometida su privacidad, ya sea porque se le muestra realizando actos

sexuales o pornográficos. Este material audiovisual puede ser obtenido por el cibercriminal al acceder ilícitamente a la información que la víctima almacena en algún dispositivo informático o mediante la práctica del sexting, en donde los delincuentes contactan a sus víctimas a través de las redes sociales, se ganan su confianza y, mediante engaños y argucias, los convencen para que envíen fotografías o videos de sí mismos desnudos, con poca ropa o realizando actos sexuales. Posteriormente, proceden con amenazarlo en difundir el material comprometedor si no cumple con las exigencias, de índole económico, patrimonial o incluso sexuales.

La modalidad de cómo engañar a la víctima para que proporcione material íntimo al delincuente consistía en ganarse la confianza de la víctima por medio de las redes sociales y utilizando perfiles falsos, poco a poco se convencía a la víctima para entrar en una videollamada en donde se grababa el material privado. Sin embargo, con el avance en la creación y diseño de las aplicaciones digitales, ahora el delincuente puede simular tener problemas de audio o imagen en la videollamada y hacer que la víctima instale en su dispositivo una aplicación mal intencionada que permite tener completo acceso a información privada almacenada, una vez que el delincuente obtiene los datos bancarios, contactos, imágenes o videos, procede a extorsionar a la víctima, amenazándola con difundir el material entre sus familiares, amigos o conocidos y esto la deja en una posición de vulnerabilidad extrema, sin la posibilidad de defenderse (Flores, et al., 2015).

Este tipo de extorsión se realiza dentro del ámbito digital y tecnológico, evoluciona, se simplifica y se especializa cada día más, sin embargo, las medidas legislativas y de control, aún son lentas y deben pasar por numerosos procedimientos burocráticos para tener validez y ser promulgadas. Así, en la actividad legal, se puede llegar a la conclusión de que la sextorsión no utiliza la violencia física como lo tipifica la norma, sino que se utiliza la coacción psicológica y la amenaza a la privacidad, por lo que se estaría frente a otros tipos de violencia, además el entorno digital agrava el daño potencial y la viralización del contenido.

Sin embargo, esta modalidad de extorsión digital no es la única, también se encuentra la modalidad de uso extorsivo de datos personales mediante la modalidad del phishing que consiste en la utilización de correos electrónicos falsos que simulan ser de entidades gubernamentales o comerciales verdaderas para inducir a la víctima que digite sus datos personales como contraseñas, códigos y credenciales de acceso, con la finalidad de utilizarlos para suplantar la identidad en línea; por lo que constituye un delito cibernético altamente negativo y tiene impactos severos en el patrimonio de los usuarios, ya que el robo de sus contraseñas y datos bancarios permiten al delincuente realizar transacciones comerciales en línea, como compras o depósitos no autorizados por el titular y vaciar su dinero. Además del impacto negativo psicológico y patrimonial de la víctima, esta práctica afecta a la confianza y credibilidad de las entidades financieras, resultando en un delito pluriofensivo (Cervieri & Pavón, 2025). Adicionalmente, este delito puede desembocar en la extorsión, pues si el delincuente no tiene la posibilidad de disponer del patrimonio de la víctima, puede intentar amenazarlo o coadyuvarlo para que se realice sus exigencias, como se vio en el ejemplo del ataque que se realizó a la entidad bancaria Interbank, en donde el ciberdelincuente amenazó con revelar y divulgar datos bancarios de miles de usuarios y clientes del banco si no cumplían con pagarle una cantidad de dinero exorbitante.

En el delito de extorsión, se han identificado cinco procesos que el delincuente realiza para conseguir que la víctima acceda a realizar sus requerimientos indebidos. Según Goicoechea (2018), la primera etapa, cuando la extorsión se da mediante redes sociales o telefónicas, consiste en que el delincuente selecciona a sus potenciales víctimas (perfiles de Facebook, Instagram o números telefónicos), de manera aleatoria y masiva, aunque también puede tener como criterio la capacidad económica y la reputación del usuario, es decir, si es una persona famosa que tiene que cuidar de su reputación e identidad digital, resultará más sencillo que acceda a sus exigencias. En la segunda etapa, es cuando se trata de ganar la confianza de la víctima, mediante comunicación presencial (este tipo de

contacto se suele realizar mediante encuentros o "citas") o sin contacto directo (cuando el medio comisivo de este delito son las redes sociales o tecnologías de la información) y se puede decir que es el más conveniente para el delincuente, pues le resulta más sencillo comunicarse con la víctima sin los obstáculos geográficos, de manera inmediata y anónima, lo que a su vez, ocasiona que la investigación y persecución policial, se complique y se sea más difícil, pues al no existir fronteras geográficas, se convierte en un delito transnacional. En la tercera etapa, es cuando se lleva a cabo la amenaza, mediante violencia verbal y psicológica reiterada para lograr intimidar a la víctima y hacerla sentir indefensa. El tipo de amenaza está sujeta a la información que posee el extorsionador, ya sean datos personales, fotografías o videos íntimos otorgados por la misma víctima, etc, y pueden ser amenazas de divulgar el material íntimo, realizar transacciones bancarias sin su consentimiento, quitarle la vida, agredirla, secuestrarla, atentar contra sus familiares o destrozar su identidad digital y reputación, con el objetivo de que la víctima se encuentre en una posición de indefensión y bajo un estrés tan fuerte que no piense en pedir ayuda por el miedo constante, por lo que estos factores emocionales y circunstanciales logran que la víctima realice las instrucciones del extorsionador por la desesperación de querer salir de esa situación. Esta fase del proceso comisivo del delito es el determinante para saber si es que la víctima realizará las exigencias, pues si reacciona de manera sumisa y temerosa ante la amenaza, el extorsionador seguirá con la amenaza, pero le dará instrucciones para que, dependiendo el objetivo del delincuente, la víctima realice el pago u otra acción indebida. Si, por el contrario, la víctima no se deja intimidar y se enfrenta al extorsionador y se dispone a denunciar el delito, se inicia la negociación. La quinta y última fase consiste en el pago y cobro de lo exigido, en este punto, el delincuente tiene control total sobre la víctima y se asegura de mantenerla bajo su poder, pudiendo continuar con la extorsión y pedirle de manera sistemática dinero u otro tipo de beneficio.

Con la identificación de las fases de realización de este delito se

puede concluir que las plataformas digitales de comunicación y tecnologías de la información han traído consigo nuevas formas de cometer delitos comunes mediante medios digitales, brindando a los delincuentes anonimato, inmediates y facilidad extrema, así como la seguridad de que no serán descubiertos de manera sencilla, pues los obstáculos geográficos superados por las redes sociales e internet, paradójicamente se han convertido en obstáculos para su investigación, identificación y persecución, ya que el delito ha evolucionado en uno de naturaleza trasnacional.

Adicionalmente, el avance de la tecnología en la rama de la inteligencia artificial, amerita que se incluya un factor importante en la comisión de este delito: la utilización de la inteligencia artificial para la comisión, incluso más rápida y especializada, de delitos como la extorsión digital y su implicancia en la dinámica digital de los usuarios. La primera etapa de realización consiste en la identificación de la víctima, en redes sociales y espacios digitales se suele hacer aleatoriamente, y la segunda etapa consiste en la comunicación con la víctima para ganar su confianza con el objetivo de que el extorsionador consiga material comprometedor para poder intimidar y amenazar al extorsionado. Sin embargo, la inteligencia artificial es una herramienta que tiene su auge en este siglo, definida como una ciencia que busca la implementación de conocimientos, valores y pensamiento humanos a las máquinas, es decir, dotar de inteligencia como potencial humano para que sean capaces de conocer, comprender y razonar, con el objetivo de que ciertos procesos puedan ser realizados por las máquinas. Por ello, desde su desarrollo hasta la actualidad, la inteligencia artificial está presente en muchos campos del trabajo humano, por ejemplo, en el tratamiento de lenguajes expertos, sistemas informáticos de información, robótica, aprendizaje y demás áreas (Escolano et al,. 2003).

El avance de esta herramienta en todos los campos de la vida humana, supone también la posibilidad de que se use para la realización de delitos, pues la creación de aplicaciones y plataformas digitales impulsadas por IA o bots pueden dar paso a su utilización para fines ilícitos. Por

ejemplo, existe el fenómeno denominado DeepFake, por su traducción al español "profundo" y "falso", respectivamente, este término se refiere a la utilización del aprendizaje por parte de las máquinas para realizar tareas sin intervención humana en el proceso, permitiendo la creación de materiales manipulados (Heidari et al., 2023). Según, Ramos (2024), esta práctica consiste en alterar medios audiovisuales y del material original y hace posible la sustitución del rostro de una persona en el cuerpo de otra, se puede manipular el físico y partes específicas del cuerpo, también es posible la manipulación de audios y videos en donde aparecen personas hablando y haciendo declaraciones falsas que nunca dijeron.

Según un artículo periodístico de Castro (2024), titulado "Telegram en la mira: bots crean y difunden contenido explícito hecho por la IA", se narra que la plataforma de comunicación instantánea Telegram, alberga en sus sistemas a bots (programadas de software automatizados) que son capaces de utilizar DeepFakes para generar contenido explícito. Estos bots son programas alojados en los sistemas de la aplicación de mensajería capaces de generar contenido explícito sin consentimiento de las personas a partir de una fotografía o videos, pueden reemplazar el rostro de una persona en el cuerpo de otra, además de hacer desaparecer la ropa de una persona retratada en una fotografía o desnudarla y crear videos falsos en donde se realizan actos explícitos de índole sexual. Según el portal de noticias, menciona que una investigación de la revista WIRED, reveló que la plataforma Telegram, alberga cincuenta bots dedicados a esta actividad y que la cantidad de usuarios que interactúan con estos es de aproximadamente cuatro millones e incluso alcanzan los cuatrocientos mil usuarios mensuales. El funcionamiento de estos bots es muy sencillo, pues el usuario de estos programas ilegales solo tiene que subir al sistema una fotografía de alguien para que la inteligencia artificial proceda a desnudar a la persona. Estas prácticas ilícitas que van en contra de los derechos de imagen y de la intimidad de las personas, se pueden realizar a través de Telegram, pues su algoritmo está diseñado con la finalidad de brindar privacidad de sus usuarios y no revisar la

función que estos bots pueden realizar, por lo que se encuentra en una investigación por parte de los Estados Unidos de Norteamérica.

Esta práctica cada vez más creciente, pone en evidencia que las plataformas digitales son herramientas creadas para facilitar el comercio, el aprendizaje, la comunicación o las relaciones sociales, sin embargo, también pueden convertirse en herramientas destinadas a la comisión de delitos transnacionales y graves. Según Popova (2020), la utilización de esta tecnología para la creación de contenidos inapropiados genera un problema, en cuanto supone la ilegalidad del contenido producido. Así mismo, la creación de este contenido falso en donde se presenta a las personas en situaciones comprometedoras y de forma inexacta, supone una amenaza y grave afectación a su reputación, integridad personal e imagen. Es por ello, que, dentro de las fases de comisión de la extorsión, vemos necesario actualizar esa información teniendo en cuenta este fenómeno, pues ahora con los bots generativos de imágenes falsas y trucadas, al delincuente solo le bastaría con conseguir una fotografía de su víctima (generalmente se puede tener acceso a fotografías de las personas en sus redes sociales), tal como lo sostiene Liberos et,. al (2013), las redes sociales son un medio de comunicación que permiten el acceso a datos presentes en sus sistemas de almacenamiento, tales como blogs, fotografías, música, videos y demás. En este contexto digital, resulta muy fácil para el criminal cargarla a los programas malintencionados y generar una imagen explícita para poder extorsionar a su víctima (sextorsión), esto no solo facilita la labor criminal, sino que también genera la especialización y automatización del delito, pues ya no son necesarias acciones destinadas a ganarse la confianza de la víctima y se puede proceder a la extorsión de manera más rápida, sencilla y eficiente.

Capítulo 3
Responsabilidad Penal de las plataformas digitales

La evolución de las tecnologías de la información y las redes sociales tienen como consecuencia muchos beneficios económicos, culturales y sociales. Sin embargo, también pueden ser utilizadas por personas mal intencionadas que buscan un beneficio ilegítimo realizando conductas ilegales, pues hacen uso de las herramientas y avances que brinda la tecnología para perpetrar sus actos delictivos y poder conseguir ventajas y beneficios económicos. El avance de los programas de computadora y las nuevas formas de comunicación más eficaces, rápidas y sencillas, han traído consigo el surgimiento de las plataformas digitales, que, según Constantinides et al. (2018, como se citó en Bonina et al., 2021), son "un conjunto de recursos digitales, ya sean servicios o contenidos, que facilitan las interacciones entre sus participantes" [traducción propia] (p. 871). Consecuentemente, se puede decir que las plataformas digitales son programas diseñados para facilitar el intercambio de servicios y contenidos entre sus usuarios, contribuyen a la interacción rápida y sencilla entre ofertantes y demandantes, así como facilitan las transacciones comerciales y/o brindar soportes digitales para la comunicación a través de las redes sociales, como Facebook, Instagram, etc. Las plataformas digitales se podrían entender como mercados y espacios públicos a los que se accede a través de la red de internet, siendo un espacio de encuentro virtual, en donde se crea una identidad, reputación y conducta digital. Al ser un espacio virtual, es decir, fuera de la realidad concreta, exige nuevas formas de interpretación por parte del Derecho Penal, en son de los avances tecnológicos y la creación de espacios virtuales que eliminan las fronteras territoriales y jurisdiccionales de los países.

Por ello, la responsabilidad penal de las plataformas digitales constituye un problema importante; su regulación debe ser sólida y clara en términos jurídicos y tecnológicos, pues el Derecho debe trascender a un nuevo espacio virtual en donde la libertad para cometer delitos

es mayor. La responsabilidad penal de las personas, debe pasar por los filtros de la imputación objetiva, ya que son necesarios para atribuirle responsabilidad penal de las personas, pues según Bramont, esta teoría necesita que la acción humana produzca un riesgo o lo aumente más allá de las fronteras que permite la ley, el riesgo debe realizarse en el resultado y todo esto debe estar dentro de la protección de la norma (2008, p. 187). En ese sentido, en ámbitos virtuales y del ciberespacio, esta teoría deberá ser actualizada manteniendo sus fundamentos principales como el sujeto, la acción, el nexo causal y el resultado lesivo a un bien jurídico, teniendo en cuenta que el comportamiento de la plataforma digital frente a la posible comisión de los delitos dentro de su espacio virtual, cumpla con los requisitos de la imputación objetiva y de la teoría de la adecuación. Primero, debemos mencionar que los espacios virtuales son programados a través de algoritmos y códigos que determinan sus funciones y alcances, siendo esto una ventaja enorme porque se puede programar una plataforma digital de tal manera que no permita la comisión de delitos a través de sus sistemas o que por lo menos los prevenga y denuncie. Por lo que, la responsabilidad de las plataformas digitales en el ámbito penal, se debe analizar desde una perspectiva múltiple: la forma en cómo se han programado (los algoritmos y lenguajes de programación), la detección de conductas que pueden ser antijurídicas (a través de revisión de datos e información almacenados en sus sistemas internos) y la detección de usuarios que intenten cometer delitos a través de sus servicios digitales. Estos elementos son necesarios porque, la forma en cómo están creadas las plataformas (lo que permiten hacer, lo que previenen y lo que prohíben) es fundamental para regular las acciones de los usuarios (siempre en observancia de la libertad de expresión y comunicación). En la realidad material, en donde el Derecho es el instrumento político-social de regulación y determinación del comportamiento de los ciudadanos, en las realidades virtuales, los algoritmos y códigos pueden ser el principal regulador de comportamiento de los usuarios, mediante medidas de prevención y sanción dentro de la misma plataforma, esto se convierte en una enorme ventaja de prevención y erradicación de los delitos info-

máticos, por el contrario, si la misma arquitectura y programación de las plataformas digitales no contempla procesos destinados a la observancia de los principios éticos y de prevención básicos, la empresa propietaria y desarrolladora puede ser responsable penalmente, así como los programadores.

La teoría de la imputación ampliamente utilizada en los sistemas legales de todo el mundo, sostiene que una persona es responsable de un delito cuando con su actuar crea un riesgo no permitido que es mayor al socialmente permitido y por consecuencia el resultado es lesivo para un bien jurídico (Roxin, 1997, p. 366), por lo que al extrapolar este principio rector de la imputación penal hacia el ámbito y entorno digital se llega a un problema, pues el control humano y el funcionamiento automatizado de las plataformas digitales, bots, aplicaciones de computadora e inteligencia artificial, pueden afectar la claridad y conceptos de la imputación objetiva, en tanto que las pruebas empíricas destinadas a determinar la responsabilidad penal pueden resultar ineficaces o débiles. Por ejemplo, existen plataformas que permiten la difusión de materiales audiovisuales ilícitos y peligrosos que van en contra de la sociedad y sus intereses, por lo que resultará necesario determinar la responsabilidad de estas plataformas o de las personas que han diseñado los algoritmos, para determinar si es que el modelo estructural de la plataforma carece de medidas de prevención o detección de contenidos potencialmente ilícitos y como consecuencia generaron un riesgo no permitido concreto que ha desembocado en un resultado lesivo para los usuarios. Pero también surge la interrogante sobre el rol que cumplen las plataformas digitales (pueden ser de índole comercial, comunicacional, educativa o de entretenimiento, entre muchas otras) pero independientemente de su finalidad, deben tener un rol más activo en cuanto a la observancia de las leyes e ir un paso más allá al cumplir con la prevención y detección de actos ilegales que se pueden dar a través de las mismas plataformas digitales. Entonces, la teoría del rol normativo del sujeto cobra relevancia para fundamentar la responsabilidad de las plataformas. Según Jakobs, el rol normativo del

sujeto es el papel o función que debe cumplir dentro de un contexto y sistema social, porque una persona que vive y se desarrolla dentro de la sociedad no puede ser un sujeto aislado de las normas sociales y preceptos culturales, por lo tanto cumple una función y ocupa un lugar específico y sus acciones son evaluadas de acuerdo a su rol y de las normas que lo regulan; pues lo contrario sería un comportamiento anti normativo, contraviniendo a lo socialmente permitido (1998, p. 103). Por ejemplo, un médico pertenece a un ámbito y espacio dentro de la sociedad, por lo que su actuar en ejercicio de su deber estará condicionado – dentro de las libertades propias del ser humano – por las normas de la buena praxis y del Derecho Médico, y en general por todas las demás que se relacionan con ser un sujeto respetuoso del Derecho de los demás, lo mismo sucedería con un albañil, profesor o político, por lo que en el caso de las plataformas digitales, este rol normativo cobra una importancia vital, no porque la plataforma sea un sujeto físico, sino porque la plataforma es en sí misma el espacio, ámbito y medio donde se desarrollan los usuarios, por lo que tiene la responsabilidad y el rol de prevenir, detectar y denunciar actos ilícitos que puedan cometer sus usuarios, pero además debe ser capaz de que el diseño de su espacio virtual no propicie la comisión de delitos. Ahora bien, en el contexto de las plataformas digitales, los programadores y demás involucrados, deben asumir el rol dentro de la sociedad (tal como los médicos, ingenieros, profesores, etc) y estar determinados por las normas que regulan este ámbito, mismas que deben incluir deberes de monitoreo, control y reacción frente al comportamientos de sus usuarios que puedan generar riesgos no permitidos y lesionen derechos protegidos legalmente. Finalmente, dentro de este marco de responsabilidad de las plataformas digitales, las teorías de la imputación objetiva ofrecen herramientas teóricas que se pueden llevar hacia el ámbito y espacio virtual de las plataformas, pues resultan importantes y útiles para determinar el rol, acción y responsabilidad de los sujetos involucrados en el ciberespacio, permitiendo distinguir a intermediarios técnicos, agentes y programadores, que por sus acciones u omisiones contribuyen a la producción del resultado lesivo. Para desarrollar el tema de la responsabilidad penal de

las plataformas digitales, primero es necesario estudiar la teoría del delito en tres tipos de comisión: delitos dolosos, culposos y en los de omisión.

Responsabilidad penal de las plataformas digitales en delitos dolosos de comisión

Primero, recordemos el rol del Derecho Penal en la sociedad, pues según Mir Puig, este se consagra como uno de los medios de control social – existen otros medios de control social dentro de las dinámicas de los ciudadanos como las profesiones o las familias – pero posee formalidad a diferencia de los otros, ya que su función principal es evitar comportamientos que sean lesivos mediante la advertencia de castigar e imponer sanciones punitivas en caso que los ciudadanos realicen tales comportamientos (2011, p.40). Por ello, el Derecho penal es un medio de control social a través de toda la maquinaria judicial y engranajes normativos, entendiéndolo como una máquina enorme destinada a prevenir delitos, investigarlos y castigar a los infractores de la ley, así como reinsertarlos en la sociedad, pero con el surgimiento de la realidad virtual y entornos digitales, resulta necesario que también se convierta en un medio de control social digital.

En ese sentido, los delitos dolosos de comisión se encuentran tipificados en la norma sustantiva y en ella se determina a los sujetos, los supuestos de hecho, comportamiento y correspondiente castigo. Según Bramont, las conductas que resultan lesivas pueden ser dolosas o culposas, la diferencia radica en que las conductas dolosas se caracterizan porque el sujeto encaminó sus acciones con el pleno conocimiento de que sus actos dañan un bien jurídico y tuvo la intención de hacerlo, por lo que destinó su comportamiento (tipo objetivo) y voluntad (tipo subjetivo) para perpetrar la lesión al bien jurídico y en la culpa está presente la negligencia o la imprudencia (2008, p. 203). En el contexto digital, se deberá analizar la conducta de la plataforma digital – como sistema automatizado con intervención humana – y analizar si es que infringe la ley penal (tipo objetivo) y si existía conocimiento y voluntad de cometer

el delito (tipo subjetivo)[3]. La conducta de la plataforma se puede analizar con la fiscalización de sus diseños y algoritmos para determinar si han sido diseñados para prevenir y evitar actos delictivos o, por el contrario, han sido diseñados justamente con el objetivo de cometer delitos de manera automatizada o con negligencia deliberada. Así mismo, determinar si se creó un riego relevante o lo aumentó más allá de lo permitido legalmente, a saber, el riesgo puede ser creado cuando se evitan normas técnicas, legales y de buena praxis en el diseño de los algoritmos o el riesgo puede ser aumentado cuando los programadores sabían que el actuar de la plataforma, por acción u omisión, permitía que se cometan delitos. Por ejemplo, cuando la aplicación digital esconde su verdadera finalidad bajo una red social y que solo busca la obtención de datos personales, imágenes o información sensible de los usuarios para poder extorsionarlos posteriormente de manera automatizada o hacerlos pagar por servicios fantasmas y estafarlos, es decir, su diseño algoritmo está creado para la comisión activa de delitos con o nula intervención humana. En estos casos, las plataformas digitales, al no ser personas naturales ni jurídicas, no pueden ser responsables penalmente, sino que la responsabilidad recaería en los programadores de la plataforma (como los programadores de bots, impulsados por inteligencia artificial, creados para desnudar a las personas con una simple fotografía y que se aloja en la plataforma digital Telegram). Así mismo, en el caso de las plataformas digitales que son impulsadas por la inteligencia

En el contexto digital, los delitos dolosos de comisión pueden ser: extorsión en redes sociales, difusión de material pornográfico infantil o íntimo sin consentimiento, suplantación de identidad, etc. Sin embargo, estos delitos deben estar correctamente tipificados en la norma sustantiva, es decir, en una ley que recoja todos los tipos penales para que se pueda cumplir, en primer lugar, con la función seleccionadora consistente en determinar las conductas que sucedan dentro de la sociedad consideradas graves y relevantes para el Derecho Penal. En segundo lugar, su función garantizadora, que establece que una persona solo puede ser sancionada

si su conducta está tipificada en un tipo penal. En tercer lugar, la función indiciaria, consistente describir de manera general las acciones típicas para poder distinguir aquellas que son punibles de aquellas que, por características especiales, no lo son al existir causas de justificación que llevan a la antijuricidad del hecho. Por último, la función motivadora, pues es de suma importancia motivar a las personas para que no cometan delitos, constituyendo una manera de prevención mediante la intimidación con imponer un castigo (Bramont, 2008, p.171). De todas las funciones desarrolladas, consideramos que, para el contexto digital, la función garantizadora es de suma urgencia, pues los delitos informáticos no se encuentran expresamente regulados o presentes en códigos únicos, sino que se encuentran desperdigados, pues se intenta regular las conductas en el ámbito virtual desde distintos puntos de partida, desde el área comercial, desde los derechos de autor, defensa del consumidor, etc. Sin embargo, hay que reconocer que los avances en tipificar las conductas, ya se vienen desarrollando en leyes y convenios internacionales tales como la Ley de Delitos Informáticos N°30096 en el Perú que, recientemente, incluyó la incidencia y el uso de la Inteligencia Artificial como agravante en la comisión de delitos informáticos, la protección especial a los menores de edad y la coordinación interinstitucional, el Convenio de Budapest conocido como el Convenio de la Ciberdelincuencia, etc. artificial, se puede dar el caso que cuando la plataforma modifica y promueve la comisión de delitos, colabora con grupos criminales (proporcionándoles logística, herramientas de hackeo, deepfakes, etc.) y sus algoritmos promueven contenidos ilícitos, entonces se estaría frente a conductas dolosas presentes en la misma estructura y programación de la plataforma.

Responsabilidad penal de las plataformas digitales en los delitos culposos y de omisión

La culpa y la omisión en el Derecho Penal son semejantes, pues en ambos está presente el riesgo permitido (a diferencia de los delitos de comisión dolosa en donde el riesgo es creado por el mismo sujeto), es el sujeto que por sus acciones determina el resultado sin querer hacerlo.

En otras palabras, para que se le impute a una persona un delito culposo, este debió actuar necesariamente con negligencia, imprudencia o sin haber agotado todo lo que estuvo a su alcance (impericia) para evitar el resultado lesivo. Así, Bramont señala que los comportamientos humanos culposos serían aquellos en donde el sujeto lesionó el bien jurídico cuando no quería hacerlo, es entonces una situación en donde la conducta del agente incumple lo que el ordenamiento jurídico le exhorta; ser cuidadoso (2008, p. 224 – 227). Así mismo, Roxin critica esta concepción de la culpa, pues no basta con esperar que el sujeto actúe de una manera normativamente impuesta y actúe de otra por negligencia o desconocimiento para imponerle una culpa, sino que existe una largo trecho entre el querer hacer y el poder hacer, por ello, cuando la situación amerita un deber de cuidado para evitar un daño jurídicamente relevante, el sujeto puede tener la intensión de encaminar sus actos para evitar tal daño pero el entorno lo supera, venciéndolo y resultando el daño igualmente (1997, p.801). Sin embargo, en este apartado no corresponde discutir y dilucidar estos aspectos de la culpabilidad, sino que la misma norma determina cuáles son los delitos culposos, por ejemplo, Silva dice que "la culpa surge cuando un deber de cuidado impuesto por la norma se incumple sin voluntad de causar daño" (2001) y Bramont señala que "los delitos culposos deben ser declarados de forma expresa en la norma, siguiendo el sistema de números clausus" (2008, p.224).

Por lo que, en el caso de las empresas desarrolladoras de plataformas digitales e inteligencia artificial, estas pueden ser responsables (desarrolladores, directivos, programadores, etc.) de un delito penal por la comisión culposa del tipo. En ese sentido, cuando se viola el deber de cuidado determinado por códigos de conducta, reglamentos internos, principios de la ética algorítmica y demás cuerpos normativos, ya sea por imprudencia, negligencia o la inobservancia de las reglas propias de la materia, se habría incurrido en la realización culposa del delito porque como creadores (posición de garante objetivo) del ámbito virtual de su plataforma, tienen la capacidad de actuar frente a un ilícito pero si lo

ignoran, infligen el deber de cuidado objetivo y el resultado es consecuencia de la negligencia técnica o funcional. Por ejemplo, pongamos el contexto de la existencia de una plataforma digital que funciona como una red social en donde los usuarios pueden hacer transmisiones en vivo de su vida cotidiana y demás actividades, pero entre todos los creadores de contenido, existe un grupo dedicado a transmitir abusos sexuales a menores de edad o grabaciones ocultas a personas violando su intimidad. Ciertos usuarios han reportado este tipo de cuentas a la misma empresa propietaria de la plataforma, pero las cuentas dedicadas a estas actividades no han sido eliminadas de manera eficaz. Entonces, la empresa propietaria sería responsable de manera culposa si es que se logra probar que los algoritmos de programación contaban con filtros automatizados o moderadores humanos dedicados a dar de baja este tipo de cuentas, pero no estaban correctamente capacitados o eran ineficientes. En el caso de la responsabilidad por omisión, los delitos son cometidos por la inacción del garante que tiene el deber de cuidado, es decir la empresa responsable de la plataforma y todos los involucrados en esta labor. Por ejemplo, la posible comisión por omisión, sería cuando las entidades financieras crean sus plataformas digitales para que sus clientes puedan realizar transacciones en menor tiempo y ahorrando gastos operativos, sin embargo, la empresa encargada de esta plataforma no hace la labor obligatoria de actualizar sus sistemas y protocolos de protección ante ataques cibernéticos a pesar de que tienen el conocimiento de la vulnerabilidad de la plataforma, por lo que los hackers atacan la plataforma y logran extraer datos personales y bancarios de miles de clientes, ocasionando pérdidas millonarias y la filtración de los datos sensibles, entonces su responsabilidad penal estaría determinada por su inacción si es que se llega a probar que no actuaron pesa a tener conocimiento del riesgo de ataque, es decir, inobservaron las reglas que los obligaban a actuar con diligencia lo que ocasionó el resultado negativo, entonces se estaría frente a una omisión impropia, ya que la empresa tiene la posición de garante que lo faculta y obliga a actuar para evitar la comisión del delito, adicionalmente, también cabe la posibilidad de estar frente a omisión propia, cuando la pla-

taforma no realiza la eliminación de contenido ilegal, de odio o que promueve la violencia, a pesar de que tiene la obligación de hacerlo por ley.

RESULTADOS

Después del análisis bibliográfico, doctrinario y jurisprudencial desarrollados en el presente trabajo se llegó a las siguientes conclusiones:

El delito de extorsión común ha evolucionado hacia un delito más complejo denominado extorsión digital, pues es posible cometer este delito a través de plataformas digitales que no han sido creadas para cometer delitos, pero que los delincuentes utilizan por brindarles anonimato, inmediates y mayor alcance. También existe la posibilidad de que personas o grupos criminales creen plataformas digitales destinadas exclusivamente para la comisión de la extorsión, automatizando el delito a través de algoritmos diseñados para extorsionar a una amplia cantidad de personas. También que las empresas y personas jurídicas pueden ser responsables penalmente, ya sea por comisión dolosa, culposa u omisión, por los delitos cometidos a través de sus plataformas digitales. La inteligencia artificial puede tener responsabilidad penal derivada del diseño de sus algoritmos si es que no se la programa con valores éticos y principios necesarios para evitar el daño al ser humano. Por último, el delito de extorsión debe ser tipificado en la norma especial de delitos digitales como Extorsión Digital, ya que no se puede investigar y perseguir por medios tradicionales, porque constituye un delito complejo que requiere especialización para su persecución eficiente. Se recomienda la actualización de la normativa referente a los delitos digitales, la creación de medios especializados de control y persecución, así como la creación de obligaciones para los desarrolladores de plataformas digitales como deberes de cuidado específicos y determinar sus posiciones de garantes, todo esto con la posibilidad de continuar con la lege ferenda en la materia.

Referencias bibliográficas

Bonifacio, S. (2019). *El incremento de los casos de extorsión agravada y su relación con los delitos contra el patrimonio – Lima 2015* [Tesis de maestría, Universidad Nacional Federico Villarreal]. Repositorio UNFV. https://repositorio.unfv.edu.pe/handle/20.500.13084/3518

Bonina, C., Koskinen, K., Eaton, B., & Gawer, A. (2021). *Digital platforms for development: Foundations and research agenda. Information Systems Journal*, 31(5), 869–902. https://doi.org/10.1111/isj.12326

Bramont, L. (2008). *Manual de derecho penal: Parte general* (4.ª ed.). Editorial y Distribución de Libros.

Castro, A. (2024, octubre 26). *Telegram en la mira: Bots crean y difunden contenido explícito hecho por IA.* La República. https://larepublica.pe/tecnologia/actualidad/2024/10/26/cuidado-con-el-nuevo-problema-en-telegram-bots-crean-contenido-explicito-con-ia-1615484

Cervieri, V., & Pavón, C. (2025). *El phishing como delito de triple impacto: Marcas, datos personales y afectación del patrimonio.* Revista de Actualidad Mercantil, (9), 21–29. https://revistas.pucp.edu.pe/index.php/actualidadmercantil/article/view/30902

Congreso de la República del Perú. (1991, abril 8). *Código Penal: Decreto Legislativo N.º 635.* https://spij.minjus.gob.pe

Escolano, F., Cazorla, M., Alfonso, I., Colomina, O., & Lozano, M. (2003). *Inteligencia artificial: Modelos, técnicas y áreas de aplicación.* https://books.google.com

Flores, R., Urano, A., Hayashi, N., Gu, L., Remorin, A., Zhu, J., Lin, P., & Costoya, J. (2015). *Sextortion in the Far East.* Trend Micro. https://documents.trendmicro.com/assets/wp/wp-sextortion-in-the-

far-east.pdf

Francescutti, P. (2021). *Vidas mediáticas: Entre lo masivo y lo individual. InMediaciones de la Comunicación,* 16(2), 237–242. https://doi.org/10.18861/ic.2021.16.2.3164

Goicoechea, M. (2018). *La extorsión: Un estudio desde la fenomenología y la psicopatología* [Trabajo de grado, Universidad del País Vasco]. Repositorio UPV/EHU. https://addi.ehu.es/handle/10810/29756

Heidari, A., Jafari, N., Dag, H., & Unal, M. (2023). *Deepfake detection using deep learning methods: A systematic and comprehensive review*. WIREs Data Mining and Knowledge Discovery. https://doi.org/10.1002/widm.1520

Jakobs, G. (1997). *Derecho penal: Parte general, fundamentos y teoría de la imputación.* https://proyectozero24.com

Jescheck, H. (2014). *Tratado de derecho penal: Parte general* (Vol. I). https://proyectozero24.com

Liberos, E., Núñez, A., Bareño, R., García, R., Gutiérrez, J., & Pino, G. (2013). *El libro de marketing interactivo y la publicidad digital.* https://books.google.com

Mir Puig, S. (2011). *Derecho penal: Parte general* (9.ª ed.). https://www.pensamientopenal.com.ar

Morán, A. (2022). *Responsabilidad penal de la inteligencia artificial (IA): ¿La próxima frontera?* Revista IUS, 15(48), 290–323. https://doi.org/10.35487/rius.v15i48.2021.706

Paucar, L. (2024, noviembre 14). *Robo de datos en Interbank al descubierto: Así operó el hacker para extraer información.* Infobae.

Poder Ejecutivo. (2007, julio 21). *Decreto Legislativo N.º 982.* Diario Oficial El Peruano. https://www.leyes.congreso.gob.pe/Documentos/DecretosLegislativos/00982.pdf

Popova, M. (2020). *Reading out of context: Pornographic deepfakes, celebrity and intimacy.* Porn Studies, 7(4), 367–381. https://doi.org/10.1080/23268743.2019.1675090

Ramos, F. (2024). *Deepfake: Análisis de sus implicancias tecnológicas y jurídicas en la era de la inteligencia artificial. Derecho Global: Estudios sobre Derecho y Justicia*, 9(27), 359–387. https://doi.org/10.32870/dgedj.v9i27.754

Roxin, C. (1997). *Derecho penal: Parte general. Fundamentos. La estructura de la teoría del delito.* https://img.lpderecho.pe

Salinas, R. (2018). *Derecho penal: Parte especial.* https://proyectozero24.com

Silva, J. (2001). *La expansión del derecho penal: Aspectos de la política criminal en las sociedades postindustriales.* https://es.scribd.com