REBAZA, ALCÁZAR & DE LAS CASAS

Informativo Penal

Modificatorias legislativas relevantes de abril en material penal

Entra en vigencia Ley 32314 que modifica el Código Penal y la Ley 30096, Ley de delitos informáticos, para incluir el uso de la Inteligencia Artificial en la comisión de delitos

Mediante este informativo, remitimos a nuestros clientes la relación de las modificaciones legislativas más relevantes publicadas en el mes de abril en materia penal, a fin de que puedan disponer de esta información a su interés.[1]

Respecto del Código Penal, la Ley 32314 publicada el 29 de abril de 2025, introduce modificaciones relevantes en los artículos 46, 129-M, 132, 196-A, 217, 218, 219, 220, 220-A, 220-B y 220-C del Código Penal. Así mismo, incorpora el numeral 5 al artículo 11 de la Ley 30096, Ley de Delitos Informáticos.

Estas modificaciones se centran en cuestiones relacionadas con la incorporación **del uso de la Inteligencia Artificial** en la comisión de delitos.

[1] La información ha sido extraída conforme al Diario El Peruano y al Sistema Peruano de Información Jurídica – SPIJ.

I. Código Penal

Modificatoria	Comentarios
Artículos 46, literal e) del numeral 2 y se incorpora a este el literal ñ) [...] 2. Constituyen circunstancias agravantes, siempre que no estén previstas específicamente para sancionar el delito y no sean elementos constitutivos del hecho punible, las siguientes: [...] e) Emplear en la ejecución de la conducta punible medios de cuyo uso pueda resultar peligro común, así como el **uso indebido de inteligencia artificial o de tecnologías similares o análogas**; [...] ñ) Cuando para la realización de la conducta punible **se utilice la inteligencia artificial o tecnologías similares o análogas**.	Se reconoce como **agravante el uso indebido de IA o tecnologías similares para cometer delitos**, lo que refleja una preocupación por el potencial nocivo de estas herramientas. Se diferencia entre el **uso indebido** (e) y el **uso directo** como medio (ñ). **Ejemplo:** Una empresa privada ofrece asesoría automatizada a una serie de usuarios para lo cual implementan un algoritmo de inteligencia artificial que recomienda de forma deliberada la compra de acciones de una compañía en la que ellos tienen intereses, inflando artificialmente su precio en el mercado. **Aplicación de agravantes:** • **Literal e)**: Se empleó IA como medio para ejecutar el delito económico. Generó peligro común, al comprometer a un número indeterminado de víctimas y al sistema económico en su conjunto. • **Literal ñ)**: La conducta fue especialmente lesiva por el uso de tecnología que dificultaba detectar el engaño.

Artículo 129-M, primer párrafo

El que posee, promueve, fabrica, distribuye, exhibe, ofrece, comercializa, publicita, publica, importa, exporta o manipula por cualquier medio objetos, libros, escritos, imágenes, videos o audios, **o utiliza tecnologías basadas en inteligencia artificial, incluidas las falsificaciones profundas ('deepfakes') o cualquier contenido multimedia generado por inteligencia artificial,** con fines relacionados con la pornografía infantil o realiza espectáculos en vivo de carácter sexual, en los cuales participen menores de dieciocho años de edad, será sancionado con pena privativa de libertad no menor de seis ni mayor de diez años y con ciento veinte a trescientos sesenta y cinco días multa.
[...].

Tipifica como delito la **utilización de IA**, incluidos deepfakes, en el contexto de pornografía infantil. Se incorpora una nueva modalidad tecnológica en la explotación sexual de menores, ampliando el alcance penal.

Ejemplo: Una persona utiliza un programa de inteligencia artificial para **crear videos falsos (*deepfakes*)** en los que **parecen participar menores de edad en actos sexuales**, aunque en realidad **las imágenes fueron generadas digitalmente** a partir de rostros reales de adolescentes tomados de redes sociales. Luego, **comercializa estos videos en la dark web** a cambio de criptomonedas.

Aplicación del artículo 129-M:

- La persona **utiliza tecnología basada en inteligencia artificial para generar contenido pornográfico infantil**, incluso si no hay una víctima que haya sido filmada directamente.
- El uso de *deepfake* **no elimina la tipicidad penal**, ya que el artículo **expresamente incluye los contenidos generados por IA** con fines de pornografía infantil.

Este tipo penal busca cerrar la puerta a quienes intenten escudarse en que "no hay una víctima real", reconociendo que la **representación sexual de menores, aunque sea sintética**, fomenta una cultura de explotación y puede derivar en daños reales.

Artículo 132, tercer párrafo

[...]
Si el delito se comete por medio del libro, la prensa u otro medio de comunicación social, **o mediante tecnologías de inteligencia artificial, falsificaciones profundas ('deepfakes') u otros contenidos generados mediante inteligencia artificial que difundan información falsa o denigrante que cause daño a la reputación o a la imagen**, la pena será privativa de libertad no menor de uno ni mayor de tres años y de ciento veinte a trescientos sesenticinco días-multa.

Agrava la difamación **si se usa IA o deepfakes** para difundir información falsa o denigrante. Se actualiza el tipo penal frente a nuevas formas de vulnerar la reputación en **entornos digitales.**

Ejemplo: Una persona incómoda con un periodista que investiga un caso de corrupción decide **crear un video deepfake** en el que el periodista aparece **recibiendo sobornos de un empresario vinculado a contratos estatales**. El video, completamente falso, pero muy realista, es difundido por redes sociales y enviado a medios digitales, generando un daño a la imagen y reputación profesional de la periodista, quien pierde oportunidades laborales y enfrenta ataques en línea.

Aplicación del artículo 132, tercer párrafo:

- Se trata de una **difamación agravada** porque:
- Se usa **tecnología de inteligencia artificial** (deepfake).
- Se **difunde información falsa y denigrante**.
- Esta información **causa un daño concreto a la reputación o imagen** de la víctima.
- La pena se agrava respecto de la difamación simple, precisamente porque **se emplea un medio tecnológicamente avanzado que amplifica el alcance y el daño**.

Artículo 196-A, para incorporar el numeral 7

La pena será privativa de libertad no menor de cuatro ni mayor de ocho años y con noventa a doscientos días-multa, cuando la estafa:

[...]

7. Se realice mediante la manipulación de la voz, imagen, audio o movimiento corporal de terceros, **utilizando inteligencia artificial o tecnologías análogas** de forma que cause un perjuicio económico a la víctima.

Establece como agravante el uso de IA para **manipular elementos personales** (voz, imagen, etc.) y causar un perjuicio económico. Reacciona frente a **fraudes sofisticados** usando tecnologías emergentes.

Ejemplo: Una persona utiliza una herramienta de inteligencia artificial para **reproducir la voz de un gerente de una empresa** (mediante *voice cloning*) y **llama al área de tesorería haciéndose pasar por él**. En la llamada, instruye al encargado para que **realice una transferencia bancaria urgente** a una cuenta determinada, supuestamente para cerrar un negocio estratégico.

El trabajador, al reconocer la voz del gerente, **confía en la instrucción y transfiere S/ 80,000**, los cuales son desviados a una cuenta fraudulenta.

Aplicación del artículo 196-A, numeral 7:

- Se trata de una **estafa agravada** porque:
- Se **manipuló la voz** de un tercero (el gerente).
- Se utilizó **inteligencia artificial para simular credibilidad**.
- Se **causó un perjuicio económico directo a la víctima (la empresa)**.

Este tipo penal busca proteger contra fraudes tecnológicos que **usan IA para simular la identidad de una persona y generar confianza**, con el fin de obtener ilícitamente dinero o bienes.

Artículo 217, primer párrafo

Será reprimido con pena privativa de libertad no
menor de dos ni mayor de seis años y con treinta a noventa días-multa, el que, con respecto a una obra, una interpretación o ejecución artística, un fonograma o una emisión o transmisión de radiodifusión, o una grabación audiovisual o una imagen fotográfica, **de autoría humana**, expresada en cualquier forma, realiza alguno de los siguientes actos sin la autorización previa y escrita del autor o titular de los derechos:
[...].

Reafirma la protección de **obras de autoría humana** y exige consentimiento expreso para su uso, diferenciándolas implícitamente de obras generadas por IA. Resalta el **valor del elemento humano** en la creación.

Ejemplo: Una empresa crea un video publicitario para redes sociales. Para ello, **toma sin autorización un videoclip musical de un artista independiente**, quien lo había publicado previamente en YouTube. El videoclip incluye una interpretación artística del propio autor (voz y guitarra), y es incorporado al anuncio sin su conocimiento.

Aunque la empresa alegue que usó solo unos segundos y que aplicó filtros con inteligencia artificial para "modificarlo", lo cierto es que **no obtuvo el consentimiento previo, ni escrito, del autor**.

Aplicación del artículo 217, primer párrafo:

- Se infringe el derecho del autor **sobre una obra de autoría humana (interpretación musical)**.
- El uso fue **sin autorización escrita**, requisito que el artículo exige expresamente.
- Aunque la empresa usó IA para editar la obra, **la protección sigue vigente** porque se trata de una creación **humana**, lo que el artículo busca proteger especialmente frente al uso indebido o apropiación.

Este tipo penal busca dejar claro que el uso de obras humanas no puede eludirse con modificaciones tecnológicas o filtros: **el consentimiento sigue siendo obligatorio**.

Artículo 218, literales a) y d)

La pena será privativa de libertad no menor de cuatro ni mayor de ocho años y con noventa a ciento ochenta días multa cuando:

a. Se dé a conocer al público una obra **de autoría humana**, inédita o no divulgada, que haya recibido en confianza del titular del derecho de autor o de alguien en su nombre, sin el consentimiento del titular.
[...]
d. Se fabrique, ensamble, importe, exporte, modifique, venda, alquile, ofrezca para la venta o alquiler, o ponga de cualquier otra manera en circulación dispositivos, sistemas tangibles o intangibles, esquemas o equipos capaces de soslayar otro **dispositivo destinado a impedir o restringir la realización de copias** de **obras de autoría humana**, o a menoscabar la calidad de las copias realizadas, o capaces de permitir o fomentar la recepción de un programa codificado, radiodifundido o comunicado en otra forma al público, por aquellos que no están autorizados para ello.
[...].

Se sanciona con severidad el **uso indebido de obras recibidas en confianza** y la comercialización de **dispositivos que burlen medidas de protección**. Enfatiza la protección de obras frente al uso no autorizado.

Ejemplo para el literal a) –*Divulgación de obra recibida en confianza sin autorización:*
Una diseñadora gráfica entrega en confianza a su amigo un borrador completo de su libro ilustrado, aún **no publicado**, para que le dé su opinión. Sin su consentimiento, él **lo sube a una plataforma digital y lo difunde públicamente** donde se ve afectado por una serie de descargas. La autora no solo pierde el control sobre su obra inédita, sino también posibles contratos de edición.

Aplicación del literal a):

- Se divulgó una obra **de autoría humana, inédita**, sin consentimiento.
- La obra fue **recibida en confianza**, y se rompió esa relación.
- Configura una **agravante específica**: el uso indebido de obras confidenciales.

Ejemplo para el literal d) –*Comercialización de sistemas que burlan protección*
Una persona **vende en línea un software que permite romper los sistemas de protección DRM** (gestión de derechos digitales) de plataformas de streaming, para descargar películas sin pagar. Publicita el software como una forma de "guardar tus películas favoritas sin restricciones".

Aplicación del literal d):

- Se **fabrica y pone en circulación** un sistema intangible (software).
- Su fin es **soslayar medidas de protección** que impiden la copia o distribución no autorizada de obras de autoría humana.
- Constituye una forma agravada de infracción, pues **facilita la piratería tecnológica**.

Ambos supuestos muestran cómo se protege **no solo el contenido**, sino también las **relaciones de confianza y las barreras tecnológicas** que garantizan el respeto por los derechos de autor.

Artículo 219. Plagio

Será reprimido con pena privativa de libertad no menor de tres ni mayor de seis años y noventa a ciento ochenta días multa, el que, con respecto a una **obra de autoría humana**, la difunda como propia, en todo o en parte, copiándola o reproduciéndola textualmente, **o tratando de disimular la copia mediante ciertas alteraciones, atribuyéndose o atribuyendo a otro, la autoría o titularidad ajena.**

Se penaliza el plagio de obras humanas, incluso si se intentan disimular los copiados. **Esto delimita claramente la autoría humana frente a los contenidos generados por IA.**

Ejemplo: Una estudiante universitaria presenta como tesis final una monografía que **copió casi íntegramente de un artículo académico** publicado por un investigador reconocido en una revista indexada. Para evitar ser descubierta, **modifica ligeramente la redacción y cambia el orden de algunos párrafos**, pero **mantiene las ideas, estructura y ejemplos originales** sin citar al autor. Luego, la presenta como si fuera de su autoría ante la universidad.

Aplicación del artículo 219:

- La obra copiada es de **autoría humana**.
- Se ha **copiado total o parcialmente** el contenido.
- Se han hecho **alteraciones menores para disimular la copia**, lo que **no excluye la configuración del delito**.
- La infractora **se atribuye falsamente la autoría**, lo cual constituye **plagio penalmente sancionado**.

Artículo 220, para incorporar el literal f)

Será reprimido con pena privativa de libertad no
menor de cuatro ni mayor de ocho años y noventa a trescientos sesenticinco días-multa:
[...]
f. Si el agente obtiene una **ventaja patrimonial** derivada de la explotación de la obra objeto del comportamiento descrito en el artículo 219.

Se sanciona al que obtenga beneficio económico por explotar una **obra plagiada**. Reforzamiento del carácter patrimonial del derecho de autor, desincentivando su vulneración.

Ejemplo: Un influencer con miles de seguidores en redes sociales **publica un libro digital (e-book)** que en realidad **es una copia parcial de una novela escrita por un autor peruano**, disponible solo en bibliotecas universitarias. El influencer hace leves modificaciones en los nombres de personajes y escenarios, pero mantiene la historia, diálogos y estilo. **Vende el e-book a través de su página web y obtiene ingresos significativos** por cada descarga.

Aplicación del artículo 220, literal f):

- La obra plagiada es de **autoría humana**.
- Hay una **infracción al artículo 219** (plagio).
- Se **obtuvo una ventaja patrimonial** (ingresos por ventas del e-book).
- Se configura una **agravante específica**: el beneficio económico derivado del plagio.

Artículo 220-A. Elusión de medida tecnológica
Efectiva

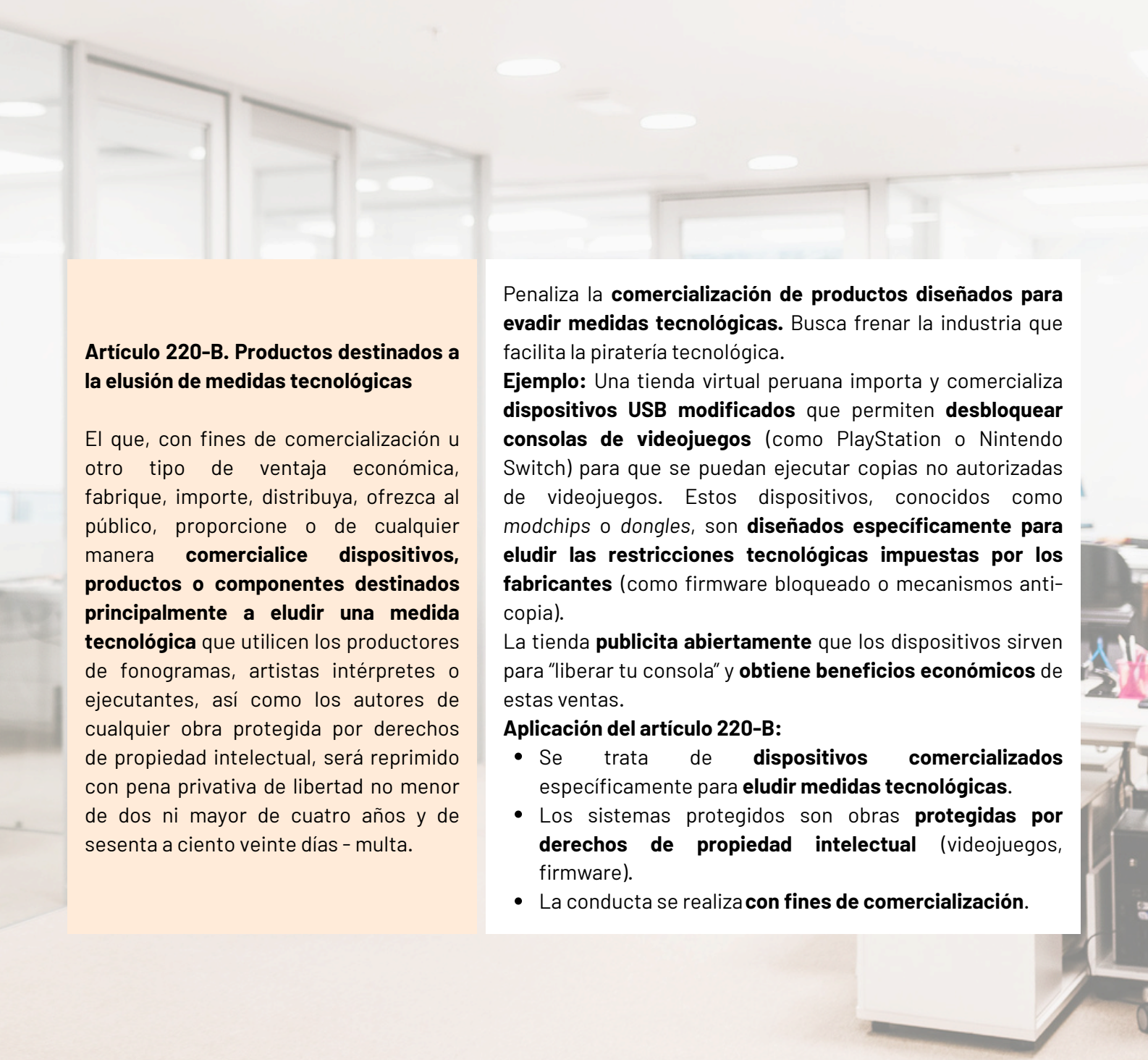
El que, con fines de comercialización u otro tipo de ventaja económica, **eluda sin autorización cualquier medida tecnológica efectiva** que utilicen los productores de fonogramas, artistas, intérpretes o ejecutantes, así como los autores de cualquier obra protegida por derechos de propiedad intelectual, será reprimido con pena privativa de libertad no menor de dos ni mayor de cuatro años y de sesenta a ciento veinte días - multa.

Se penaliza la **elusión de medidas tecnológicas que protegen obras o fonogramas**. Protege los sistemas **DRM (Digital Rights Management)** y otras barreras digitales tales como **códigos de región** en DVDs o Blu-rays, **c**ifrado **de archivos** o de transmisiones de streaming, **sistemas anti-copia** en consolas o discos y **restricciones de acceso** basadas en autenticación o licencias frente a usos no autorizados.

Ejemplo: Un programador crea y comercializa en línea una aplicación que **desbloquea los archivos protegidos de una popular plataforma de streaming de música**, permitiendo a los usuarios **descargar las canciones sin pagar** y sin las restricciones que impone la plataforma (como cifrado o autenticación). La aplicación **elude deliberadamente los sistemas de protección DRM** implementados por la plataforma y **genera ingresos a través de suscripciones y publicidad**.

Aplicación del artículo 220-A:

- Se elude una **medida tecnológica efectiva** (DRM, cifrado, autenticación).
- El autor **no tiene autorización** del titular de los derechos (la plataforma y/o los autores).
- El acto se realiza **con fines de comercialización** y/o para obtener una **ventaja económica**.



Artículo 220-B. Productos destinados a la elusión de medidas tecnológicas

El que, con fines de comercialización u otro tipo de ventaja económica, fabrique, importe, distribuya, ofrezca al público, proporcione o de cualquier manera **comercialice dispositivos, productos o componentes destinados principalmente a eludir una medida tecnológica** que utilicen los productores de fonogramas, artistas intérpretes o ejecutantes, así como los autores de cualquier obra protegida por derechos de propiedad intelectual, será reprimido con pena privativa de libertad no menor de dos ni mayor de cuatro años y de sesenta a ciento veinte días - multa.

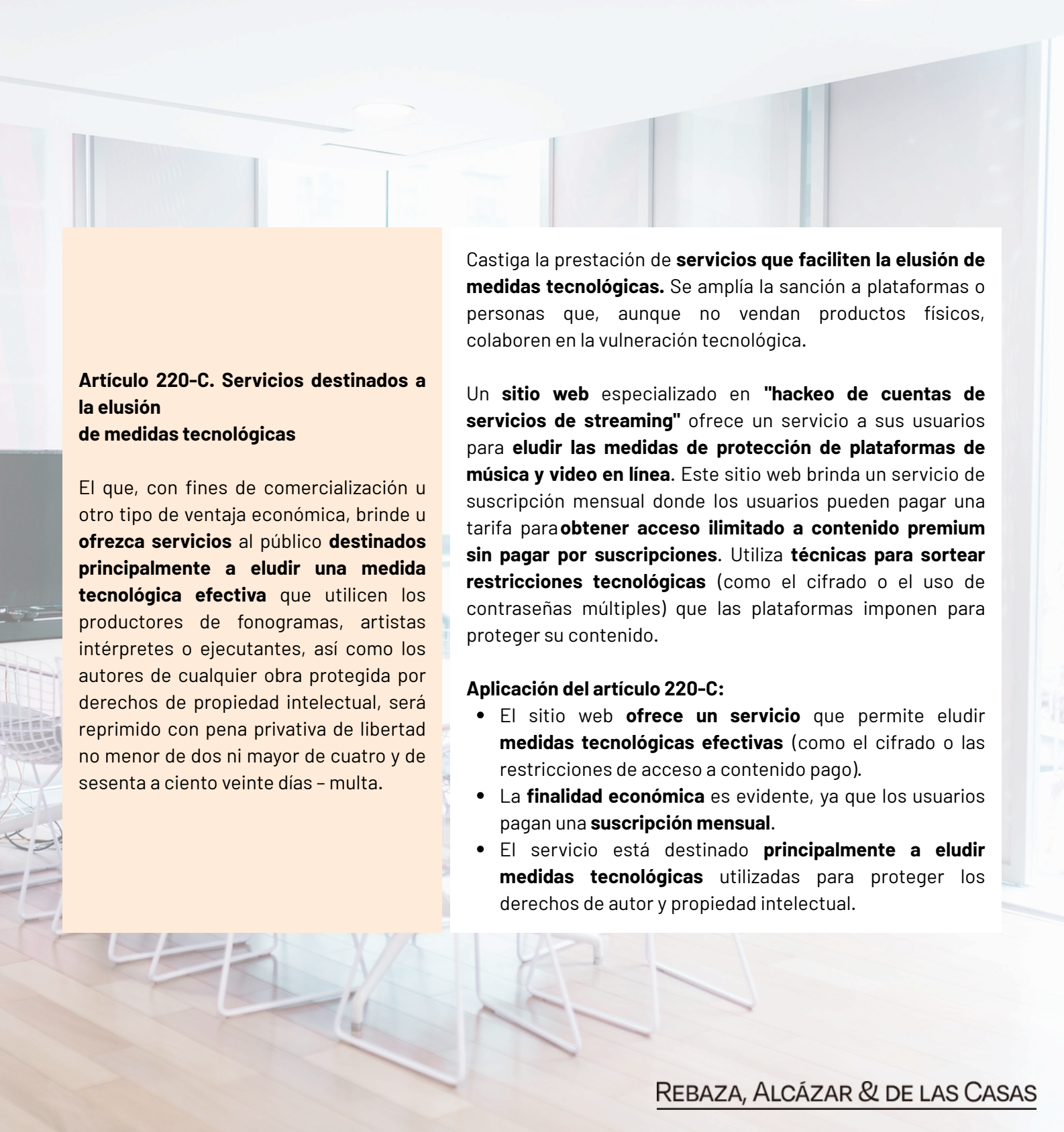
Penaliza la **comercialización de productos diseñados para evadir medidas tecnológicas.** Busca frenar la industria que facilita la piratería tecnológica.

Ejemplo: Una tienda virtual peruana importa y comercializa **dispositivos USB modificados** que permiten **desbloquear consolas de videojuegos** (como PlayStation o Nintendo Switch) para que se puedan ejecutar copias no autorizadas de videojuegos. Estos dispositivos, conocidos como *modchips* o *dongles*, son **diseñados específicamente para eludir las restricciones tecnológicas impuestas por los fabricantes** (como firmware bloqueado o mecanismos anti-copia).

La tienda **publicita abiertamente** que los dispositivos sirven para "liberar tu consola" y **obtiene beneficios económicos** de estas ventas.

Aplicación del artículo 220-B:

- Se trata de **dispositivos comercializados** específicamente para **eludir medidas tecnológicas**.
- Los sistemas protegidos son obras **protegidas por derechos de propiedad intelectual** (videojuegos, firmware).
- La conducta se realiza **con fines de comercialización**.



Artículo 220-C. Servicios destinados a la elusión de medidas tecnológicas

El que, con fines de comercialización u otro tipo de ventaja económica, brinde u **ofrezca servicios** al público **destinados principalmente a eludir una medida tecnológica efectiva** que utilicen los productores de fonogramas, artistas intérpretes o ejecutantes, así como los autores de cualquier obra protegida por derechos de propiedad intelectual, será reprimido con pena privativa de libertad no menor de dos ni mayor de cuatro y de sesenta a ciento veinte días – multa.

Castiga la prestación de **servicios que faciliten la elusión de medidas tecnológicas.** Se amplía la sanción a plataformas o personas que, aunque no vendan productos físicos, colaboren en la vulneración tecnológica.

Un **sitio web** especializado en **"hackeo de cuentas de servicios de streaming"** ofrece un servicio a sus usuarios para **eludir las medidas de protección de plataformas de música y video en línea**. Este sitio web brinda un servicio de suscripción mensual donde los usuarios pueden pagar una tarifa para **obtener acceso ilimitado a contenido premium sin pagar por suscripciones**. Utiliza **técnicas para sortear restricciones tecnológicas** (como el cifrado o el uso de contraseñas múltiples) que las plataformas imponen para proteger su contenido.

Aplicación del artículo 220-C:

- El sitio web **ofrece un servicio** que permite eludir **medidas tecnológicas efectivas** (como el cifrado o las restricciones de acceso a contenido pago).
- La **finalidad económica** es evidente, ya que los usuarios pagan una **suscripción mensual**.
- El servicio está destinado **principalmente a eludir medidas tecnológicas** utilizadas para proteger los derechos de autor y propiedad intelectual.

II. Ley 30096, Ley de delitos informáticos

Modificatoria	Comentario
Se incorpora el numeral 5 al artículo 11 El juez aumenta la pena privativa de libertad hasta en un tercio por encima del máximo legal fijado para cualquiera de los delitos previstos en la presente Ley cuando: [...] 5. El agente comete el delito **empleando la inteligencia artificial o tecnologías similares o análogas**.	Esta modificación **introduce como agravante el uso de inteligencia artificial (IA)** en la comisión de delitos informáticos. Esto implica que, si el agente utiliza IA (por ejemplo, para vulnerar sistemas, falsificar identidades, automatizar ataques, generar contenido engañoso, etc.), el juez puede imponer una **pena hasta un tercio superior al máximo legal del delito base**. Se reconoce así el mayor daño potencial y sofisticación que representa el uso de IA como herramienta delictiva. **Ejemplo:** Un **hacker** utiliza **inteligencia artificial** para llevar a cabo un **ataque automatizado** a una red corporativa. Utilizando algoritmos de IA, logra **eludir los sistemas de seguridad** y acceder a bases de datos sensibles, donde sustrae información personal de los usuarios, como contraseñas y datos bancarios. Además, emplea IA para **falsificar identidades** y **generar correos electrónicos falsos** (phishing) con el objetivo de **robar dinero de cuentas bancarias**. La IA se usa en todas las fases del ataque, desde la **identificación de vulnerabilidades** hasta la **automatización de la explotación** de esas brechas de seguridad. El uso de IA le permite **escalar el ataque** y realizarlo con **mayor rapidez y eficacia** que si lo hubiera hecho manualmente. **Aplicación del artículo 11, numeral 5:** • El **agente utiliza inteligencia artificial** como herramienta para **cometer el delito**. • **El uso de IA aumenta la sofisticación y el daño potencial** del ataque, ya que automatiza las acciones y permite evadir las medidas de seguridad de manera más eficaz que los métodos tradicionales.

NUESTRO EQUIPO

AUGUSTO LOLI
SOCIO
augusto.loli@rebaza-alcazar.com

HÉCTOR GADEA
SOCIO
hector.gadea@rebaza-alcazar.com

SERGIO MATTOS
SOCIO
sergio.mattos@rebaza-alcazar.com

CARLOS AVALOS
COUNSEL
carlos.avalos@rebaza-alcazar.com

CAMILO CLAVIJO
ASOCIADO SENIOR
camilo.clavijo@rebaza-alcazar.com

PAMELA MORALES
ASOCIADA SENIOR
pamela.morales@rebaza-alcazar.com

LIMA
Av. Víctor Andrés Belaúnde
147, Vía Principal 133, Piso 3
Edificio Real Dos, San Isidro
Teléfono (511) 442-5100

SANTIAGO DE CHILE
Av. Apoquindo 3650, Piso 12
Las Condes
Teléfono (562) 2244-68432

MADRID
Calle Velázquez 34, Piso 7
Salamanca, 28001, Madrid
Teléfono (34) 910623682

NUESTRO EQUIPO

ALEXANDER GONZALES
ASOCIADO SENIOR
alexander.gonzales@rebaza-alcazar.com

FRANCISCO VALDEZ
ASOCIADO SENIOR
francisco.valdez@rebaza-alcazar.com

FLAVIO PUCHURI
ASOCIADO SENIOR
flavio.puchuri@rebaza-alcazar.com

RAUL ARTICA
ASOCIADO
raul.artica@rebaza-alcazar.com

BIANCA ÁLVAREZ
ASOCIADA
bianca.alvarez@rebaza-alcazar.com

LIMA
Av. Víctor Andrés Belaúnde
147, Vía Principal 133, Piso 3
Edificio Real Dos, San Isidro
Teléfono (511) 442-5100

SANTIAGO DE CHILE
Av. Apoquindo 3650, Piso 12
Las Condes
Teléfono (562) 2244-68432

MADRID
Calle Velázquez 34, Piso 7
Salamanca, 28001, Madrid
Teléfono (34) 910623682