

CIBERSEGURIDAD Y DERECHO FRENTE A LOS DELITOS INFORMÁTICOS EN EL PERÚ: LÍMITES JURÍDICOS DE LA AGRAVACIÓN PENAL INCORPORADA POR LA LEY N.º 32314

*Cybersecurity and Law in relation to computer crimes in Peru:
legal limits of the criminal aggravating circumstance introduced
by Law No. 32314*

ERICK SEGUNDO SALAS FLORES* / CAYO LEON FERNANDEZ** /
JUSTO PEREZ SONCCO*** / MAYTTE HUAMANI CHAVEZ****

RESUMEN

La expansión de los servicios digitales ha incrementado la exposición de personas, empresas y entidades públicas a conductas que afectan sistemas, datos, patrimonio e identidad, mientras el uso de nuevas herramientas permite automatizar acciones, perfeccionar engaños y ampliar su alcance. En este contexto, la Ley N.º 32314 modificó en 2025 el Código Penal peruano y la Ley N.º 30096 para incorporar el empleo de inteligencia artificial y tecnologías similares o análogas dentro de distintas circunstancias de agravación. El artículo analiza los límites jurídicos de esta reforma y determina si la utilización de una tecnología de esta naturaleza basta para justificar un incremento de pena en los delitos informáticos. Se siguió una investigación jurídica dogmática, cualitativa y documental, mediante el examen sistemático de legislación peruana, instrumentos sobre ciberdelincuencia, doctrina penal y literatura reciente sobre criminalidad facilitada por inteligencia artificial. Los resultados muestran que el riesgo tecnológico que motivó la reforma es verificable, pero la redacción del numeral 5 del artículo 11 de la Ley N.º 30096 permite una aplicación excesivamente amplia si se entiende que cual-

* 0009-0003-1211-0960, erick.salasf@unmsm.edu.pe

** 0000-0003-1704-8214, cleonf@unmsm.edu.pe

*** 0009-0009-5116-4236, jperezso@unmsm.edu.pe

**** 0009-0007-2308-2749, mhuamanic_ac@unmsm.edu.pe

quier empleo de inteligencia artificial agrava automáticamente el delito. Se sostiene que la agravación debe aplicarse únicamente cuando exista utilización consciente de la tecnología, conexión funcional con la ejecución y un incremento material de la capacidad lesiva, el engaño, la automatización, la escala o la posibilidad de eludir controles. Se propone un criterio interpretativo de cinco componentes que preserve legalidad, culpabilidad, proporcionalidad y prohibición de doble valoración.

PALABRAS CLAVE: Ciberseguridad; delitos informáticos; derecho penal; agravantes; culpabilidad; legalidad; prueba digital; Perú.

ABSTRACT

The expansion of digital services has increased the exposure of individuals, businesses and public institutions to conduct affecting computer systems, data, property and identity, while new technological tools can automate actions, enhance deception and extend the reach of criminal activity. Within this context, Law No. 32314 amended the Peruvian Criminal Code and Law No. 30096 in 2025 by incorporating the use of artificial intelligence and similar or analogous technologies into several aggravating circumstances. This article examines the legal limits of that reform and determines whether the mere use of such technology is sufficient to justify increased punishment for computer crimes. A qualitative, documentary and dogmatic legal methodology was followed through a systematic examination of Peruvian legislation, cybercrime instruments, criminal law doctrine and recent literature on AI-enabled crime. The findings show that the technological risk underlying the reform is genuine, but the wording of Article 11(5) of Law No. 30096 may lead to an excessively broad application if every use of artificial intelligence is automatically treated as aggravating. The article argues that increased punishment should apply only when the technology is consciously used, functionally connected to the commission of the offence and materially increases harmful capacity, deception, automation, scale or the ability to evade controls. A five-component interpretative test is proposed to preserve legality, culpability, proportionality and the prohibition against double counting.

KEYWORDS: Cybersecurity; cybercrime; criminal law; aggravating circumstances; culpability; legality; digital evidence; Peru.

1. INTRODUCCIÓN

Las actividades económicas, laborales, educativas y administrativas dependen cada vez más de sistemas digitales que concentran información, permiten acreditar identidades y ejecutan operaciones capaces de producir efectos jurídicos inmediatos. Esta transformación ha ampliado las posibilidades de interacción y prestación de servicios, aunque también ha creado escenarios donde una conducta ejecutada desde un dispositivo puede afectar simultáneamente el patrimonio de una persona, la integridad de una base de datos o la continuidad de una organización. Wall (2024) explica que la ciberdelincuencia contemporánea se caracteriza precisamente por la capacidad de aprovechar redes, servicios y datos interconectados para ejecutar actividades que pueden superar los límites territoriales y alcanzar un número elevado de víctimas.

En el Perú, este proceso puede observarse junto con un aumento sostenido de las denuncias relacionadas con ciberdelincuencia, el Ministerio Público (2026) informó que estas pasaron de aproximadamente 19010 en 2021 a 44703 durante 2025, crecimiento que representa un aumento de alrededor del 134% en cinco años. El crecimiento de estas denuncias refleja la mayor presencia que han adquirido los delitos cometidos mediante tecnologías digitales en el Perú y, al mismo tiempo, plantea mayores exigencias para su prevención, investigación y sanción dentro del sistema penal.

La respuesta jurídica frente a este fenómeno se construyó inicialmente alrededor de la Ley N.º 30096, publicada en 2013, cuyo objeto consiste en prevenir y sancionar conductas ilícitas que afectan datos y sistemas informáticos, junto con otros bienes jurídicos comprometidos mediante tecnologías de la información o comunicación. Esta norma incorporó delitos como el acceso ilícito, los atentados contra datos y sistemas, la interceptación, el fraude informático y la suplantación de identidad, mientras las reformas posteriores ampliaron o ajustaron algunas de sus disposiciones para responder a nuevas modalidades de ciberdelincuencia (Congreso de la República del Perú, 2013).

El desarrollo tecnológico también ha ampliado las posibilidades de uso de herramientas que pueden emplearse tanto con fines legítimos como delictivos, entre ellas la inteligencia artificial, capaz de generar textos, imágenes, voces y videos, procesar grandes volúmenes de información y automa-

tizar tareas que antes requerían mayores conocimientos técnicos. Panattoni (2025) señala que estas capacidades pueden ser aprovechadas para producir contenidos dañinos, llegar a un mayor número de personas y elaborar mensajes o materiales dirigidos a influir con mayor precisión sobre determinadas víctimas.

En el contexto de la ciberseguridad, estas posibilidades pueden utilizarse para cometer fraudes, realizar suplantaciones, perfeccionar técnicas de ingeniería social o apoyar distintas acciones vinculadas con ataques informáticos. El National Cyber Security Centre (2025) advierte que la inteligencia artificial puede aumentar la rapidez y la escala de algunas actividades maliciosas y facilitar su ejecución a personas con menores conocimientos técnicos, aunque los ataques de mayor complejidad continúan dependiendo, en buena medida, de la intervención y las decisiones de personas con experiencia especializada.

Teniendo en cuenta lo señalado, el legislador peruano respondió a este escenario mediante la Ley N.º 32314, publicada el 29 de abril de 2025, que modificó diferentes disposiciones del Código Penal y añadió el numeral 5 al artículo 11 de la Ley N.º 30096. De acuerdo con esta nueva disposición, el juez puede elevar la pena privativa de libertad hasta en un tercio por encima del máximo legal cuando el agente comete alguno de los delitos regulados por la Ley de Delitos Informáticos empleando inteligencia artificial o tecnologías similares o análogas (Congreso de la República del Perú, 2025).

La misma ley introdujo modificaciones que exceden el ámbito estricto de los delitos informáticos, debido a que incorporó referencias a estas tecnologías dentro del artículo 46 del Código Penal y reformó figuras vinculadas con pornografía infantil, difamación y estafa agravada. En esta última, por ejemplo, se incorporó un supuesto referido a la manipulación de voz, imagen, audio o movimiento corporal de terceros mediante inteligencia artificial o tecnologías análogas cuando de esa conducta deriva un perjuicio económico para la víctima. La reforma refleja una preocupación legítima frente a contenidos sintéticos capaces de hacer más convincente un engaño, aunque también genera interrogantes respecto de la forma en que debe delimitarse la intervención penal.

Aunque la inteligencia artificial puede aumentar la capacidad para cometer determinados delitos, su sola utilización no debería justificar automá-

ticamente una pena más grave, porque primero debe evaluarse qué función cumplió realmente dentro del hecho y si produjo una mayor afectación del bien jurídico protegido. Mir Puig (2016) recuerda que la responsabilidad penal continúa sujeta a la conducta personalmente atribuible, la culpabilidad y los límites derivados del principio de legalidad, de modo que la incorporación de un nuevo medio tecnológico no elimina las exigencias construidas para contener el ejercicio del poder punitivo. Esta consideración adquiere una importancia particular cuando la ley no exige expresamente que el empleo de inteligencia artificial haya producido una mayor capacidad lesiva o haya facilitado de manera relevante la comisión del delito.

La literatura peruana comenzó a estudiar esta reforma poco después de su entrada en vigor. Sanguineti Ravettino (2025) analiza la legitimidad de considerar el uso de inteligencia artificial como agravante penal desde criterios relacionados con subsidiariedad, necesidad de pena y capacidad institucional para aplicar la nueva regulación. Sobre esta base, el artículo examina los criterios que deberían orientar la aplicación del numeral 5 del artículo 11 de la Ley N.º 30096, especialmente para evitar que cualquier uso de inteligencia artificial sea considerado automáticamente como fundamento de una agravación penal.

El objetivo del estudio es determinar bajo qué condiciones jurídicas puede aplicarse la agravación incorporada por la Ley N.º 32314 a los delitos informáticos sin afectar los principios de legalidad, culpabilidad y proporcionalidad ni valorar dos veces el mismo elemento tecnológico. A partir de dicho objetivo se analiza el alcance de la reforma y proponer criterios que permitan diferenciar el empleo de inteligencia artificial que incrementa realmente el desvalor de la conducta de aquellos usos secundarios o circunstancias que no justifican una pena mayor.

La posición que se defiende es que la sola utilización de inteligencia artificial no debería ser suficiente para aumentar la pena, teniendo en cuenta que la agravación adquiere fundamento cuando la fiscalía puede demostrar que el agente conocía el empleo de la tecnología, la utilizó deliberadamente dentro de la ejecución y obtuvo mediante ella una ventaja funcional que incrementó de manera material la capacidad lesiva, la escala, el engaño, la automatización o la posibilidad de eludir controles.

2. METODOLOGÍA

La investigación se desarrolló bajo un enfoque cualitativo y utilizó el método jurídico dogmático para examinar el contenido, alcance y relación sistemática de las disposiciones modificadas por la Ley N.º 32314. El objeto de estudio estuvo constituido por las normas que regulan la agravación penal vinculada con el empleo de inteligencia artificial en el ordenamiento peruano, con especial atención al numeral 5 del artículo 11 de la Ley N.º 30096 y a su relación con el artículo 46 del Código Penal.

El análisis normativo comprendió la Ley N.º 30096 y las modificaciones directamente relacionadas con la materia, la Ley N.º 32314, el Código Penal y la Ley N.º 31814, junto con el Decreto Supremo N.º 115-2025-PCM que aprobó su reglamento. También se consideró el Convenio sobre la Ciberdelincuencia del Consejo de Europa como marco internacional relevante para comprender la protección penal de datos y sistemas y la necesidad de mantener garantías cuando se investigan conductas ejecutadas mediante tecnologías digitales.

Para analizar la norma se revisó primero lo que señala de manera expresa, luego su relación con las demás disposiciones penales y, finalmente, la finalidad que persigue la reforma, evitando ampliar la agravante a situaciones que la ley no ha previsto. La revisión comenzó por el contenido expreso de la norma y continuó con su relación con las demás agravantes previstas en el Código Penal y en la Ley N.º 30096. También se tuvo en cuenta la finalidad de la reforma, pero sin apartarse de los límites que el propio derecho penal establece para evitar que una agravante termine aplicándose a supuestos que la ley no contempla.

La revisión doctrinal incorporó literatura especializada sobre ciberdelincuencia, inteligencia artificial, responsabilidad penal y evidencia digital, a partir de publicaciones recientes que permiten conocer cómo está evolucionando el problema. Se incluyeron los trabajos de Panattoni (2025), Sanguineti Ravettino (2025), Casals Fernández (2025), Sandoval et al. (2024), Muhly et al. (2025) y Meneses Ochoa (2026), además de obras generales de derecho penal y ciberdelincuencia utilizadas para sostener las categorías de legalidad, culpabilidad, autoría y atribución.

En la revisión documental no se utilizó población ni muestra debido a que el estudio no busca medir comportamientos de personas o instituciones, toda vez que las unidades de análisis fueron disposiciones normativas, documentos técnicos y publicaciones académicas vinculadas con el objeto de investigación, cuya lectura permitió identificar problemas de indeterminación normativa, concurrencia de agravantes, atribución subjetiva y acreditación probatoria.

3. CIBERSEGURIDAD Y TRANSFORMACIÓN DE LA CRIMINALIDAD INFORMÁTICA EN EL PERÚ

La ciberseguridad no puede limitarse a la instalación de programas de protección o reaccionar después de un ataque, sino que comprende decisiones destinadas al gobierno de los riesgos, la identificación de activos, la protección de sistemas, la detección de incidentes, así como responder y recuperar servicios. Pascoe et al. (2024), al desarrollar el Cybersecurity Framework 2.0 del NIST, incorporan estas funciones dentro de una estructura que relaciona las medidas técnicas con decisiones de gobierno y responsabilidades organizativas, es importante destacar que dicha perspectiva es importante en el derecho porque muestra que la reducción del riesgo digital no depende exclusivamente del aumento de sanciones.

Los sistemas y los datos adquieren relevancia jurídica porque de ellos dependen bienes como el patrimonio, la privacidad, la identidad, las comunicaciones y la continuidad de muchos servicios, de modo que una afectación tecnológica puede producir consecuencias que van más allá del propio sistema comprometido. Una intrusión informática puede afectar la confidencialidad de una base de datos, una modificación puede alterar su integridad y una interferencia puede impedir su disponibilidad, pero la respuesta no es igual frente a cada situación. En ese sentido, el derecho penal interviene cuando la conducta reúne los elementos previstos por la ley y puede atribuirse a una persona, mientras la gestión de ciberseguridad debe actuar incluso cuando todavía se desconoce si el incidente tuvo origen delictivo.

Esta diferencia evita que se equipare un ciberdelito con un incidente de seguridad, es decir, un sistema puede quedar indisponible debido a una falla técnica, un error de configuración o un ataque deliberado, por lo que la organización necesita contener los efectos antes de establecer su origen. Clough (2015) explica que el derecho aplicado a la ciberdelincuencia debe

delimitar cuidadosamente la conducta, la autorización, los resultados y la participación individual, precisamente porque un resultado tecnológico no revela automáticamente quién lo produjo ni con qué finalidad actuó.

La inteligencia artificial introduce nuevas capacidades dentro de este escenario sin modificar esa regla de atribución, en ese contexto, el National Cyber Security Centre (2025) advierte que los actores maliciosos ya emplean herramientas de esta naturaleza para apoyar el reconocimiento de víctimas, la ingeniería social, la investigación de vulnerabilidades y el procesamiento de información obtenida ilícitamente. También considera probable que la automatización aumente la escala de determinadas operaciones, aunque señala que los ataques avanzados todavía necesitarán participación de personas especializadas.

Esta última precisión tiene consecuencias jurídicas porque impide trasladar la responsabilidad desde la persona hacia la herramienta, por lo que Panattoni (2025) sostiene que la delegación parcial de actividades a sistemas generativos obliga al derecho penal a preservar la culpabilidad y determinar qué sujeto adoptó las decisiones relevantes. El hecho de que un contenido haya sido producido automáticamente no elimina la necesidad de conocer quién formuló las instrucciones, seleccionó a la víctima, decidió utilizar el resultado y ejecutó posteriormente la conducta que produjo el daño.

Los contenidos sintéticos pueden hacer más creíble un engaño, sobre todo cuando imitan la voz, la imagen o la forma de comunicarse de una persona y logran que la víctima confíe en que está interactuando con alguien conocido. Sandoval et al. (2024), después de revisar la literatura sobre deepfakes y justicia penal, identificaron relaciones frecuentes con fraude, pornografía y manipulación de información, junto con dificultades para comprobar autenticidad y atribuir determinadas conductas. Estas herramientas pueden producir audios o imágenes suficientemente convincentes para alterar la confianza de una víctima, aunque no todo contenido sintético posee necesariamente esa capacidad ni todo uso de inteligencia artificial se traduce en un daño mayor.

Muhly et al. (2025) muestran cómo las falsificaciones de voz e imagen pueden ser utilizadas para aparentar comunicaciones legítimas dentro de organizaciones y obtener información o transferencias patrimoniales. Su propuesta no se encuentra concentrada de forma exclusiva en la sanción,

pues combina medidas técnicas, organizativas y educativas para reducir la posibilidad de que el engaño llegue a producir el resultado, lo que coincide con la concepción de ciberseguridad donde el derecho penal representa una herramienta de respuesta y no sustituye a la prevención.

En ese contexto, la política criminal debe considerar esa diferencia en la medida que una reforma que agrava la pena puede tener fundamento cuando una tecnología aumenta de forma apreciable el peligro o el daño, pero no reemplaza la necesidad de fortalecer la autenticación, la conservación de evidencia, la investigación especializada y la cooperación con proveedores. El crecimiento de las denuncias de ciberdelincuencia en el Perú muestra que el problema posee una dimensión que difícilmente puede abordarse mediante una sola modificación punitiva, especialmente cuando las actividades digitales se distribuyen entre plataformas, cuentas y servicios ubicados en diferentes jurisdicciones.

Desde esta perspectiva, el vínculo entre ciberseguridad y derecho penal debe construirse sobre una idea sencilla, cuanto mayor sea la capacidad tecnológica disponible para ejecutar una conducta, más importante resulta identificar qué función cumplió realmente esa capacidad dentro del hecho y qué decisiones humanas permitieron utilizarla. El incremento del riesgo puede justificar una reacción jurídica diferenciada, pero esa conclusión necesita demostrarse en el caso concreto y no presumirse por la sola aparición de una herramienta etiquetada como inteligencia artificial.

4. EVOLUCIÓN DEL MARCO PENAL PERUANO Y ALCANCE DE LA LEY N.º 32314

La Ley N.º 30096 consolidó en el Perú un régimen especial para conductas que afectan datos y sistemas informáticos y para determinados delitos vinculados con el uso de tecnologías de la información. Su artículo 1 establece una finalidad preventiva y sancionadora frente a conductas ilícitas que comprometen sistemas, datos y otros bienes jurídicos de relevancia penal, lo que permitió diferenciar figuras específicamente informáticas de delitos tradicionales que pueden utilizar canales digitales (Congreso de la República del Perú, 2013).

La regulación peruana fue modificándose conforme aparecieron nuevas necesidades de adecuación y cooperación internacional, en ese sentido,

la Ley N.º 30171 introdujo cambios orientados a aproximar la legislación nacional al Convenio de Budapest, mientras otras reformas atendieron fenómenos relacionados con la violencia digital, la protección de menores y el uso ilícito de datos. Estos cambios muestran que las formas de cometer delitos mediante tecnologías digitales van variando con el tiempo, por lo que la legislación penal también necesita responder cuando aparecen nuevas maneras de afectar datos, sistemas u otros bienes protegidos.

La Ley N.º 32314, publicada el 29 de abril de 2025, incorporó de manera expresa el uso de inteligencia artificial en distintas disposiciones del Código Penal peruano, modificando el artículo 46 sobre circunstancias de agravación y otras figuras relacionadas con pornografía infantil, difamación, estafa agravada y determinados delitos vinculados con derechos de autor. Con estos cambios, el legislador buscó responder a formas de comisión que pueden apoyarse en herramientas capaces de generar, modificar o manipular contenidos digitales y que plantean nuevos problemas para la aplicación del derecho penal (Congreso de la República del Perú, 2025).

Entre las modificaciones introducidas en el artículo 46 aparecen dos referencias al uso de inteligencia artificial que pueden generar dificultades al momento de determinar qué agravante corresponde aplicar, ya que el literal e) del numeral 2 comprende su uso indebido o el de tecnologías similares o análogas, mientras que el nuevo literal ñ) considera también como agravante que estas tecnologías sean utilizadas para realizar la conducta punible. La cercanía entre ambas disposiciones hace necesario diferenciar su alcance para evitar que un mismo uso tecnológico termine siendo valorado más de una vez al momento de determinar la pena.

La reforma alcanzó directamente a la Ley N.º 30096 mediante la incorporación del numeral 5 al artículo 11, que permite elevar la pena hasta en un tercio por encima del máximo previsto cuando alguno de los delitos informáticos regulados en esta ley se comete empleando inteligencia artificial o tecnologías similares o análogas. Sin embargo, la disposición no señala si ese aumento exige demostrar que la tecnología tuvo una incidencia concreta en la gravedad del hecho, como podría ocurrir cuando permite ampliar el número de víctimas, hacer más convincente un engaño, acelerar la ejecución de la conducta o dificultar su detección.

Las principales modificaciones introducidas por la Ley N.º 32314 pueden ordenarse de la siguiente forma para observar de forma clara cómo se incorporó el uso de inteligencia artificial dentro del sistema de agravantes.

Tabla 1.

Modificaciones introducidas por la Ley N.º 32314

Disposición	Tratamiento del uso tecnológico	Consecuencia jurídica
Artículo 46.2.e del Código Penal	Uso indebido de inteligencia artificial o tecnologías similares o análogas	Circunstancia agravante general
Artículo 46.2.ñ del Código Penal	Uso de inteligencia artificial o tecnologías similares o análogas para realizar la conducta	Circunstancia agravante general
Artículo 196-A.7 del Código Penal	Manipulación de voz, imagen, audio o movimiento corporal mediante IA o tecnología análoga	Forma específica de estafa agravada
Artículo 11.5 de la Ley N.º 30096	Empleo de inteligencia artificial o tecnologías similares o análogas en un delito informático	Aumento de hasta un tercio por encima del máximo legal

Nota. Elaboración propia a partir de la Ley N.º 32314.

La incorporación de la inteligencia artificial dentro del régimen de agravantes parece responder a que ciertas herramientas pueden ampliar las posibilidades con las que se ejecuta un delito, especialmente cuando permiten contactar a muchas víctimas al mismo tiempo, imitar una voz con mayor credibilidad, generar mensajes personalizados de manera automática o superar algunos controles de seguridad. Sin embargo, esa mayor capacidad no se presenta de la misma forma en todos los casos, de modo que su sola utilización no debería llevar necesariamente a considerar que el hecho tiene una gravedad mayor.

Esta diferencia puede observarse cuando una persona utiliza una herramienta generativa únicamente para mejorar la redacción de un mensaje que después empleará en un fraude, mientras otra recurre a la misma tecnología para clonar la voz de un directivo, enviar comunicaciones personalizadas a varios trabajadores y hacer creíble una orden falsa de transferencia. Aunque en ambos casos interviene inteligencia artificial, la forma en que esta influye en la ejecución del delito es distinta y también debería serlo su valoración al momento de determinar la pena.

Una regulación algo más precisa puede encontrarse en el artículo 196-A.7 del Código Penal, donde la estafa agravada vincula el uso de estas tecnologías con la manipulación de la voz, la imagen, el audio o el movimiento corporal de terceros y con la producción de un perjuicio económico. De esta manera, la tecnología no aparece simplemente como un medio utilizado durante el delito, sino relacionada con la forma en que se realiza el engaño y con el resultado que afecta a la víctima, delimitación que no se observa con la misma claridad en el numeral 5 del artículo 11 de la Ley N.º 30096.

Para comprender qué puede considerarse inteligencia artificial dentro del ordenamiento peruano también resulta útil revisar la Ley N.º 31814, que la reconoce como una tecnología emergente de propósito general y se refiere a sistemas capaces de generar predicciones, recomendaciones o decisiones con distintos niveles de autonomía (Congreso de la República del Perú, 2023). Estas definiciones ayudan a precisar el concepto desde el ámbito regulatorio, aunque no deberían utilizarse para incluir dentro de una agravante penal conductas que la propia norma sancionadora no permite identificar con suficiente claridad.

El marco fue desarrollado posteriormente mediante el Decreto Supremo N.º 115-2025-PCM, que aprobó en septiembre de 2025 el Reglamento de la Ley N.º 31814 y precisó varios conceptos relacionados con los sistemas de inteligencia artificial. Su contenido puede servir como referencia para comprender las características de estas tecnologías, pero no para ampliar los supuestos que generan una consecuencia penal más grave, ya que una interpretación de esa naturaleza podría terminar incorporando situaciones que no estaban claramente comprendidas en la norma al momento de cometerse el hecho.

Al analizar la Ley N.º 32314 dentro del sistema penal peruano, la aparición de una herramienta tecnológica durante alguna etapa del delito no debería convertirse automáticamente en motivo para aumentar la pena. Casals Fernández (2025) señala que la autonomía, la opacidad y cierto grado de imprevisibilidad de algunos sistemas plantean nuevos problemas para determinar la responsabilidad, aunque estas características no eliminan las exigencias de culpabilidad y proporcionalidad. Las formas de cometer un delito pueden cambiar con la tecnología, pero la responsabilidad continúa dependiendo de lo que hizo la persona, de lo que conocía y de la importancia que tuvo esa herramienta en el hecho investigado.

5. LA AGRAVACIÓN POR EMPLEO DE INTELIGENCIA ARTIFICIAL EN LOS DELITOS INFORMÁTICOS

El numeral 5 del artículo 11 de la Ley N.º 30096 permite aumentar la pena cuando el delito informático se comete empleando inteligencia artificial o tecnologías similares o análogas, aunque la norma no precisa si ese uso debe haber influido de manera concreta en la gravedad del hecho. Si se atendiera únicamente a su redacción, podría entenderse que basta acreditar la presencia de alguna de estas herramientas durante la comisión del delito, incluso cuando su intervención haya sido mínima o no haya producido una diferencia apreciable en la ejecución.

Para que una circunstancia agravante justifique una pena mayor debe existir alguna razón que permita considerar más grave la conducta realizada, pues el medio utilizado no siempre modifica por sí mismo la afectación producida. Mir Puig (2016) relaciona la proporcionalidad de la pena con la gravedad del hecho y con la culpabilidad del autor, de manera que dos conductas que generan un riesgo semejante y afectan de forma equivalente el mismo bien jurídico no deberían recibir un tratamiento diferente únicamente porque una de ellas utilizó una tecnología más reciente.

La situación es distinta cuando la inteligencia artificial interviene de una manera que hace más fácil o más efectiva la comisión del delito, como podría ocurrir con la generación de una voz falsa capaz de convencer a la víctima o con el envío automatizado de mensajes dirigidos a numerosas personas. El National Cyber Security Centre (2025) advierte que estas herramientas pueden aumentar la rapidez, la frecuencia y la escala de determinadas actividades maliciosas, lo que permite entender por qué su utilización podría tener relevancia al momento de valorar la gravedad del hecho.

Panattoni (2025) explica que los sistemas generativos pueden facilitar la elaboración y difusión de contenidos utilizados con fines ilícitos, pero mantiene la necesidad de identificar la conducta y la responsabilidad de las personas que intervienen. Esta idea resulta especialmente útil para interpretar la reforma peruana, porque permite considerar una mayor gravedad cuando la herramienta tuvo una participación importante en la comisión del delito, sin asumir que cualquier uso de inteligencia artificial produce necesariamente el mismo efecto.

En los fraudes realizados mediante deepfakes puede observarse con mayor facilidad cuándo la tecnología influye realmente en el engaño, especialmente si se utiliza para imitar la voz o la imagen de una persona conocida por la víctima. Muhly et al. (2025) describen situaciones en las que estas falsificaciones permiten aparentar comunicaciones de directivos o personas autorizadas para solicitar información o transferencias, casos en los que la tecnología mejora la credibilidad del engaño y puede dificultar que la víctima advierta la falsedad.

No ocurre lo mismo cuando la herramienta cumple una función secundaria que prácticamente no cambia la manera en que se ejecuta el delito, como podría suceder si se utiliza únicamente para corregir la ortografía de un mensaje, traducir un texto previamente elaborado o resumir información pública. Aunque técnicamente exista un uso de inteligencia artificial, sería difícil sostener que esa intervención hizo más grave la conducta o produjo una ventaja que justifique elevar la pena.

La importancia de la herramienta tampoco debería medirse por su nivel de complejidad tecnológica, porque un sistema sencillo puede tener una intervención decisiva en determinados hechos y una plataforma mucho más avanzada puede limitarse a cumplir una tarea secundaria. Para efectos penales interesa principalmente conocer qué hizo la tecnología dentro de la conducta investigada y cuánto influyó en la forma en que se produjo el delito.

Esta precisión cobra mayor importancia porque muchas aplicaciones de uso cotidiano ya incorporan funciones de inteligencia artificial sin que el usuario necesariamente conozca cada una de ellas. Los servicios de correo, editores de texto, buscadores y plataformas empresariales pueden utilizar procesos automatizados como parte de su funcionamiento habitual, por lo que no sería razonable aplicar una agravante simplemente porque una de estas funciones estuvo presente durante la actividad desarrollada por el agente.

Cuando el artículo 11.5 señala que el delito debe cometerse “empleando” inteligencia artificial, esa expresión puede entenderse como un uso consciente relacionado con la ejecución del hecho y no como la simple presencia de esta tecnología dentro del servicio utilizado. Debería acreditarse, por tanto, que el autor recurrió a una determinada función y que esta tuvo alguna participación reconocible en la conducta que se le atribuye.

Esa participación puede manifestarse de distintas maneras y no necesariamente mediante una pérdida económica mayor, pues en los delitos contra datos o sistemas podría permitir ejecutar acciones de forma más rápida, alcanzar un número superior de recursos digitales o dificultar determinados controles, mientras que en una suplantación podría hacer más convincente la identidad falsa. Lo relevante sería comprobar que la tecnología tuvo alguna incidencia concreta en la mayor gravedad del hecho y no limitarse a demostrar que fue utilizada.

Sanguineti Ravettino (2025) señala que la reforma plantea dudas relacionadas con la necesidad de la pena y con las capacidades que requieren las instituciones para aplicar estas nuevas disposiciones. A ello puede añadirse que demostrar el uso de inteligencia artificial constituye solo una parte del análisis, porque también corresponde explicar qué importancia tuvo esa utilización dentro del delito y por qué debería producir una consecuencia penal más grave.

La aplicación del numeral 5 del artículo 11 debe permitir responder a conductas en las que la tecnología realmente aumenta las posibilidades de causar daño, pero sin llegar al punto de considerar más grave cualquier delito simplemente porque intervino una herramienta de inteligencia artificial. De esta manera, la respuesta penal puede adaptarse a nuevas formas de criminalidad digital manteniendo la pena vinculada con lo que ocurrió en el caso y con la conducta que puede atribuirse al autor.

6. LEGALIDAD Y TAXATIVIDAD FRENTE A LAS TECNOLOGÍAS SIMILARES O ANÁLOGAS

El principio de legalidad obliga a que tanto la conducta sancionada como las consecuencias que pueden imponerse se encuentren previstas con suficiente claridad antes de la comisión del hecho, lo que impide ampliar una norma penal desfavorable a situaciones que no fueron contempladas por el legislador. La Constitución Política del Perú recoge esta garantía al establecer que nadie puede ser procesado ni condenado por una conducta que no estuviera previamente calificada por la ley de manera expresa e inequívoca, criterio que también orienta la interpretación de las disposiciones del Código Penal.

En la Ley N.º 32314, el problema de precisión no se encuentra solamente en determinar qué debe entenderse por inteligencia artificial, sino también en la inclusión de las expresiones tecnológicas “similares o análogas”, que amplían considerablemente el alcance de la agravante. Es comprensible que el legislador haya intentado evitar que la norma quede desactualizada frente a la aparición de nuevas herramientas, pero en materia penal esa apertura necesita manejarse con especial cuidado para no terminar incluyendo conductas que la ley no permite identificar con claridad.

La rapidez con la que aparecen nuevas herramientas digitales hace difícil que una norma mencione cada tecnología que podría utilizarse en la comisión de un delito, aunque esta realidad no elimina la necesidad de establecer límites suficientemente claros cuando está en juego un aumento de pena. Pagallo (2025) explica que una regulación que no dependa de tecnologías o productos específicos puede conservar mejor su vigencia con el paso del tiempo, pero también advierte que las categorías demasiado amplias generan dificultades para establecer qué sistemas quedan realmente comprendidos dentro de ellas.

Por esa razón, la referencia a tecnologías “similares o análogas” debería interpretarse atendiendo a características que permitan relacionarlas realmente con los sistemas de inteligencia artificial y no únicamente al hecho de que una herramienta automatice procesos o trabaje con grandes cantidades de información. Un programa tradicional que ejecuta instrucciones previamente definidas no tendría que ser considerado una tecnología análoga solo porque realiza una tarea con rapidez, pues una interpretación tan amplia haría difícil establecer dónde comienza y dónde termina la agravante.

Para precisar mejor estos conceptos puede recurrirse a la Ley N.º 31814 y a su Reglamento, que describen los sistemas de inteligencia artificial tomando en cuenta su capacidad para generar contenidos, predicciones, recomendaciones o decisiones con determinados niveles de autonomía. Estas referencias pueden ayudar a comprender técnicamente la tecnología utilizada en un caso concreto, pero no deberían servir para incorporar dentro de una agravante penal situaciones que no podían desprenderse razonablemente de la norma vigente cuando se cometió el hecho.

Esta cautela se explica también porque la Ley N.º 31814 y la Ley N.º 32314 cumplen funciones diferentes dentro del ordenamiento peruano, ya

que la primera regula el uso y desarrollo de la inteligencia artificial en diferentes ámbitos económicos y sociales, mientras la segunda introduce consecuencias que pueden aumentar la pena de una persona. Una definición flexible puede ser útil para regular una tecnología que cambia rápidamente, pero requiere mayores límites cuando de ella depende una consecuencia penal más severa.

Al momento de aplicar la agravante, por tanto, debería identificarse con claridad qué herramienta fue utilizada, cuáles son las características que permiten considerarla inteligencia artificial o una tecnología realmente semejante y qué función cumplió durante la comisión del delito. No sería suficiente afirmar de manera general que se utilizó una “tecnología análoga”, porque una expresión de ese tipo podría terminar comprendiendo programas y sistemas muy distintos sin explicar por qué se encuentran dentro del supuesto previsto por la ley.

Otro problema aparece al revisar el artículo 46 del Código Penal, donde la reforma incluyó dentro del literal e) el “uso indebido” de inteligencia artificial o tecnologías similares o análogas y, al mismo tiempo, incorporó en el literal ñ) su utilización para realizar una conducta punible. La cercanía entre ambas disposiciones dificulta establecer en qué situaciones corresponde aplicar una u otra, especialmente cuando el mismo uso tecnológico podría quedar comprendido en las dos.

Cuando ambas agravantes se apoyan exactamente en la misma utilización de inteligencia artificial, aplicar las dos podría significar que un solo aspecto de la conducta sea considerado más de una vez para aumentar la pena. Si la herramienta fue utilizada para cometer el delito y ese mismo comportamiento es presentado también como un uso indebido, tendría que explicarse qué elemento diferente existe entre ambas circunstancias antes de atribuirles consecuencias separadas.

Los cambios que producen los deepfakes, el fraude automatizado y otras formas de utilización delictiva de nuevas tecnologías justifican que el derecho penal revise la manera en que responde frente a estas conductas, pero esa actualización no debería debilitar las garantías que limitan la imposición de una pena. Casals Fernández (2025) sostiene que los nuevos escenarios tecnológicos obligan a revisar categorías tradicionales de responsabilidad, manteniendo la culpabilidad y la proporcionalidad como límites de esa adaptación.

Desde esta perspectiva, una regulación capaz de responder a tecnologías futuras puede ser necesaria, siempre que permita conocer con suficiente claridad qué comportamiento justifica una consecuencia penal más grave.

7. LESIVIDAD, CULPABILIDAD Y PROPORCIONALIDAD EN LA AGRAVACIÓN

Cuando se analiza la agravación penal por el uso de inteligencia artificial, la lesividad y la culpabilidad siguen siendo necesarias para determinar si corresponde una respuesta más severa, ya que no basta con identificar la presencia de una herramienta tecnológica. La primera obliga a observar cómo fue afectado el bien jurídico, mientras la segunda exige establecer qué conocía la persona, qué decisiones tomó y hasta qué punto dirigió la conducta realizada con apoyo del sistema.

El artículo 11.5 de la Ley N.º 30096 señala que la agravación procede cuando el agente comete el delito “empleando” inteligencia artificial, expresión que permite relacionar el aumento de pena con una utilización consciente y no con la simple presencia de estas funciones dentro de una plataforma. Para aplicar la agravante tendría que comprobarse que la persona conocía la capacidad que estaba utilizando y que decidió incorporarla a la ejecución del hecho.

Este aspecto adquiere mayor importancia en servicios digitales que incorporan procesos automatizados sin que el usuario intervenga directamente en cada una de sus funciones, pues una plataforma puede modificar contenidos, organizar información o seleccionar destinatarios como parte de su funcionamiento habitual. Si cualquiera de estas operaciones bastara para aumentar la pena, el resultado dependería más de las características del servicio utilizado que de la conducta que realmente puede atribuirse al agente.

Tammenlehto y Kallio (2025) señalan que la participación de sistemas de inteligencia artificial no elimina la necesidad de comprobar los elementos subjetivos requeridos por el derecho penal, aun cuando parte de la actividad haya sido realizada de manera automatizada. Aunque su estudio se desarrolla en el ámbito de la propiedad intelectual, su planteamiento permite advertir que la existencia de un resultado ilícito generado con apoyo tecnológico no explica, por sí misma, qué conocía o pretendía la persona que utilizó la herramienta.

También debe considerarse que algunos sistemas pueden generar respuestas diferentes de aquellas que el usuario esperaba inicialmente, por lo que atribuir responsabilidad exige revisar las instrucciones proporcionadas, el resultado recibido y las decisiones posteriores tomadas por la persona. De esa manera puede distinguirse entre una consecuencia inesperada del funcionamiento del sistema y un uso deliberado de sus capacidades para facilitar la comisión del delito.

La proporcionalidad adquiere especial importancia cuando se decide aumentar la pena, porque la intervención de la inteligencia artificial puede tener efectos muy distintos según el caso. Si permite dirigirse a numerosas víctimas, hacer más convincente una suplantación o ejecutar con mayor rapidez acciones contra varios sistemas, existen razones para considerar una mayor gravedad, mientras que un uso meramente auxiliar que no modifica de forma apreciable el riesgo o el daño difícilmente justificaría la misma consecuencia.

La diferencia puede observarse si una persona utiliza una herramienta generativa únicamente para corregir la redacción de un mensaje fraudulento y se compara ese supuesto con otro en el que se emplean grabaciones públicas para clonar la voz de un directivo, enviar comunicaciones personalizadas a numerosos trabajadores y solicitar transferencias aparentando una identidad verdadera. En ambos casos existe inteligencia artificial, pero su importancia dentro de la ejecución y su capacidad para aumentar el engaño son claramente diferentes.

Aunque el legislador no incorporó expresamente esta diferencia dentro del numeral 5 del artículo 11, la agravante puede interpretarse de acuerdo con los principios que limitan la imposición de una pena más severa, de manera que el incremento no dependa únicamente del tipo de herramienta utilizada. Exigir que exista una relación entre la tecnología y una mayor gravedad del hecho permite mantener la aplicación de la norma dentro de los márgenes de lesividad, culpabilidad y proporcionalidad.

El conocimiento técnico del autor tampoco debería convertirse en una razón independiente para aumentar la pena, porque saber utilizar herramientas avanzadas o poseer experiencia en programación no significa necesariamente que exista una mayor culpabilidad. Lo que interesa para el análisis penal es cómo fueron utilizados esos conocimientos dentro del hecho, qué

finalidad tuvieron y si realmente facilitaron o hicieron más grave la conducta atribuida.

Panattoni (2025) sostiene que el uso de inteligencia artificial obliga a mantener la responsabilidad vinculada con las decisiones de las personas incluso cuando algunas tareas han sido delegadas a un sistema. Este enfoque resulta pertinente para interpretar la reforma peruana, porque permite reconocer que ciertas herramientas pueden aumentar las posibilidades de cometer un delito sin dejar de exigir que la responsabilidad y la eventual agravación se construyan a partir de lo que hizo y decidió concretamente el agente.

8. CONCURRENCIA DE AGRAVANTES Y PROHIBICIÓN DE DOBLE VALORACIÓN

La Ley N.º 32314 incorporó varias referencias al uso de inteligencia artificial que pueden llegar a coincidir dentro de un mismo hecho, especialmente cuando una conducta encaja al mismo tiempo en una agravante general del artículo 46 del Código Penal, en la agravante especial del artículo 11 de la Ley N.º 30096 o en una modalidad delictiva que ya contempla expresamente el empleo de esta tecnología. Esta situación obliga a revisar con cuidado qué disposición corresponde aplicar para evitar que un mismo elemento sea utilizado más de una vez al momento de determinar la pena.

El propio artículo 46 del Código Penal establece que sus circunstancias agravantes se aplican siempre que no hayan sido previstas de manera específica para sancionar el delito ni formen parte de sus elementos, lo que ofrece una pauta útil para resolver estos casos. Cuando una característica ya ha sido tomada en cuenta dentro de una figura especial, no tendría sentido volver a utilizarla como agravante general, pues se estaría aumentando la pena sobre la base del mismo aspecto de la conducta.

En los delitos comprendidos en la Ley N.º 30096, esta regla es importante en la medida que el numeral 5 del artículo 11 regula de manera específica el empleo de inteligencia artificial o tecnologías similares o análogas. Si ese mismo uso se considerara posteriormente bajo el literal ñ) del artículo 46 del Código Penal, la tecnología utilizada estaría influyendo dos veces sobre la pena sin que exista un elemento distinto que justifique una nueva agravación.

Una dificultad parecida aparece entre los literales e) y ñ) del propio artículo 46, ya que el primero incluye el uso indebido de inteligencia artificial y el segundo considera su utilización para realizar la conducta punible. Cuando ambos supuestos se apoyan exactamente en la misma acción, tendría que existir alguna diferencia concreta entre ellos antes de aplicar consecuencias separadas, porque utilizar dos denominaciones legales para describir un solo comportamiento no convierte ese hecho en dos circunstancias agravantes distintas.

En la estafa agravada prevista en el artículo 196-A.7 la situación resulta más clara, debido a que la propia figura relaciona la inteligencia artificial con la manipulación de voz, imagen, audio o movimiento corporal de terceros y exige que de esa conducta se produzca un perjuicio económico. Si esa manipulación es precisamente la razón por la cual la estafa recibe una calificación más grave, volver a emplearla como agravante general del artículo 46 significaría valorar nuevamente el mismo elemento tecnológico.

Teniendo en cuenta lo señalado, dicha apreciación debe mantenerse cuando otras figuras modificadas por la Ley N.º 32314 ya incluyen contenidos sintéticos o herramientas de inteligencia artificial dentro de la forma en que se describe el delito, porque en esos casos la tecnología ya ha sido considerada por el legislador al definir la conducta sancionada. Para justificar un aumento adicional tendría que existir otra circunstancia distinta que incremente realmente la gravedad del hecho y no una nueva referencia al mismo uso tecnológico.

Meneses Ochoa (2026), al estudiar el tratamiento penal de las imágenes sexuales sintéticas en el ordenamiento peruano, señala que la expansión de los deepfakes obliga a revisar cómo las figuras vigentes responden a nuevas formas de afectación y qué aspectos todavía presentan vacíos. Su análisis permite advertir que la inteligencia artificial debe examinarse dentro de cada delito concreto, atendiendo a la conducta realizada y al bien afectado, sin convertir su sola utilización en una explicación suficiente para agravar cualquier comportamiento.

Antes de aplicar el numeral 5 del artículo 11 de la Ley N.º 30096, el juez tendría que verificar si el uso de inteligencia artificial ya fue considerado dentro del delito aplicable, de una modalidad agravada específica o de otra circunstancia empleada para aumentar la pena. Cuando se trate exactamente

del mismo aspecto y no exista una razón adicional que permita diferenciarlo, volver a utilizarlo produciría una nueva consecuencia sobre un elemento que ya fue valorado.

Evitar esta repetición no impide sancionar con una mayor severidad los hechos que realmente presentan una gravedad superior, sino que exige explicar qué circunstancia concreta justifica cada incremento de pena. De esta manera, pueden distinguirse los casos en los que concurren varios elementos diferentes de aquellos en los que una misma utilización tecnológica aparece mencionada en más de una disposición, manteniendo la respuesta penal vinculada con lo que efectivamente ocurrió y no con la cantidad de normas que pueden describir el mismo hecho.

9. PROBLEMAS PROBATORIOS PARA ACREDITAR EL EMPLEO DE INTELIGENCIA ARTIFICIAL

Para aplicar la agravante que se vincula con el uso de inteligencia artificial no basta con solo demostrar que se cometió un delito informático, ya que también debe acreditarse que esta tecnología intervino en su ejecución y que dicho uso puede atribuirse a la persona investigada, de tal forma que dicha tarea puede resultar compleja cuando se utilizan servicios externos, cuando el contenido generado es modificado posteriormente o cuando la plataforma no conserva durante mucho tiempo los registros necesarios para reconstruir lo ocurrido.

La evidencia que permitiría demostrar ese uso puede encontrarse repartida entre dispositivos, cuentas, aplicaciones, archivos, proveedores y servicios alojados en la nube, por lo que su adecuada conservación resulta necesaria para conocer de dónde provino la información y qué cambios pudo experimentar. Guttman et al. (2022) explican que la preservación debe mantener los datos necesarios para verificar su origen, integridad y tratamiento, mientras que la ISO/IEC 27037 establece pautas para identificar, recopilar, adquirir y preservar información que podría adquirir valor probatorio.

Cuando aparece un audio, una imagen o un video con características que hacen pensar que pudo ser generado mediante inteligencia artificial, esa apariencia constituye apenas un punto de partida para la investigación y no una prueba suficiente de quién lo produjo. Será necesario revisar, según la información disponible, la herramienta utilizada, los archivos relacionados,

los metadatos y los registros de las cuentas involucradas, siempre mediante los procedimientos que correspondan.

Los deepfakes hacen más difícil esta tarea porque no solo permiten crear contenidos falsos con una apariencia cada vez más convincente, sino que también pueden generar dudas sobre materiales que sí son auténticos. Sandoval et al. (2024) advierten esta dificultad al estudiar sus efectos dentro del sistema de justicia penal, donde puede producirse tanto el riesgo de aceptar como verdadero un contenido manipulado como el de cuestionar un material legítimo únicamente porque técnicamente pudo haber sido alterado.

Incluso cuando una pericia determine que un archivo presenta características compatibles con un contenido generado mediante inteligencia artificial, todavía quedan varios aspectos por esclarecer antes de atribuir responsabilidad. Será necesario conocer quién produjo el material, qué cuenta o servicio se utilizó, quién tenía control sobre ellos, qué instrucciones fueron ingresadas y de qué manera el resultado terminó siendo utilizado dentro del delito investigado.

Si en la elaboración y utilización del contenido participaron varias personas, la atribución exige diferenciar qué hizo cada una y qué conocimiento tenía respecto de la finalidad perseguida, porque quien genera un archivo no necesariamente es la misma persona que lo modifica o lo emplea posteriormente para cometer el delito. Las reglas de autoría y participación continúan siendo aplicables y obligan a individualizar el aporte de cada interviniente antes de establecer una responsabilidad penal.

La presencia del archivo en un teléfono, una computadora o una cuenta tampoco permite concluir automáticamente que su titular actuó con dolo, pues todavía debe revisarse el contexto en el que fue creado, las comunicaciones vinculadas, las instrucciones utilizadas y las acciones realizadas posteriormente. Mir Puig (2016) recuerda que la culpabilidad exige una atribución personal de la conducta, de manera que la relación con un dispositivo o con una cuenta constituye un elemento de análisis, pero no sustituye la prueba sobre el conocimiento y la actuación del sujeto.

Cuando parte de la información necesaria se encuentra bajo el control de un proveedor tecnológico, su obtención debe respetar la privacidad y las garantías propias del proceso penal, por lo que una investigación no puede

extenderse sin límites sobre todas las conversaciones, archivos o actividades de una cuenta. Los requerimientos deben guardar relación con los hechos investigados y circunscribirse a la información necesaria para determinar si la tecnología fue utilizada y cuál fue su participación dentro de la conducta.

Las dificultades para obtener o interpretar esta evidencia no justifican disminuir las exigencias probatorias cuando de su resultado depende un aumento de pena, ya que corresponde a la acusación demostrar que la inteligencia artificial fue efectivamente utilizada en los términos previstos por la agravante. Si persisten dudas sobre el origen del contenido, la herramienta empleada o la intervención del investigado, esas cuestiones deben resolverse mediante la prueba disponible y no mediante una presunción construida a partir de la apariencia tecnológica del material.

Al momento de valorar la agravante, el juez tendría que examinar de manera relacionada si la inteligencia artificial fue realmente utilizada, si el agente conocía y dirigía ese uso, qué relación tuvo con la ejecución del delito y si esa misma circunstancia ya fue considerada dentro del tipo penal o de otra agravante. De esta forma, la pericia técnica aporta elementos para comprender lo ocurrido, pero la decisión sobre la responsabilidad y el aumento de pena sigue correspondiendo al análisis jurídico del caso.

10. DISCUSIÓN Y PROPUESTA DE UN CRITERIO INTERPRETATIVO

La revisión realizada permite advertir que la Ley N.º 32314 responde a cambios que ya pueden observarse en la forma en que se cometen algunos delitos digitales, especialmente por el uso de herramientas capaces de hacer más creíbles ciertos engaños, automatizar tareas y ampliar el número de personas alcanzadas por una misma conducta. Estas posibilidades explican por qué el legislador decidió incorporar la inteligencia artificial dentro del régimen de agravantes, aunque su presencia en un hecho no significa necesariamente que el delito haya sido más grave.

El problema se encuentra en la forma en que fue redactado el numeral 5 del artículo 11 de la Ley N.º 30096, porque permite aumentar la pena cuando se emplea inteligencia artificial sin precisar cuánto debe haber influido esa tecnología en la ejecución del delito. Bajo una lectura demasiado amplia, podría terminar recibiendo el mismo tratamiento quien utilizó una

herramienta de manera secundaria y quien la aprovechó para aumentar el engaño, automatizar la conducta o alcanzar a un número mayor de víctimas.

Sanguineti Ravettino (2025) examina esta reforma desde la necesidad y legitimidad de una respuesta penal más severa, mientras que Casals Fernández (2025) aborda los problemas que estos sistemas plantean para determinar la conducta, la culpabilidad y la responsabilidad. A partir de estos aportes, el análisis desarrollado en este artículo busca precisar qué aspectos deberían revisarse antes de aplicar la agravante del artículo 11.5, evitando que el aumento de pena dependa únicamente de comprobar que se utilizó una herramienta de inteligencia artificial.

Para realizar esa evaluación se proponen cinco aspectos que deberían revisarse de manera relacionada, comenzando por la identificación de la tecnología utilizada y continuando con el conocimiento del agente, la función que cumplió dentro del delito, la influencia que tuvo en su gravedad y la comprobación de que ese mismo elemento no haya sido utilizado previamente para aplicar otra agravante.

Tabla 2.
Componentes

Componente	Pregunta que debe responderse	Función jurídica
Identificación tecnológica	¿Qué sistema o tecnología fue utilizada y por qué puede considerarse inteligencia artificial o funcionalmente equivalente?	Evitar conceptos tecnológicos indeterminados
Conocimiento del agente	¿La persona conocía y decidió utilizar esa capacidad dentro de su conducta?	Preservar culpabilidad y responsabilidad personal
Conexión funcional	¿La tecnología participó efectivamente en la ejecución del delito?	Excluir usos accesorios o circunstanciales
Incremento material	¿El empleo aumentó de manera relevante el engaño, la escala, la automatización, la capacidad lesiva o la evasión de controles?	Justificar proporcionalmente el aumento de pena
Control de duplicidad	¿El mismo uso tecnológico ya forma parte del tipo o de otra agravante aplicada?	Evitar doble valoración

Teniendo en cuenta lo señalado en la tabla 2, para comenzar, la acusación tendría que identificar con claridad qué herramienta fue utilizada y

por qué sus características permiten considerarla inteligencia artificial o una tecnología semejante dentro del sentido previsto por la ley, evitando expresiones generales como “programa avanzado” o “tecnología análoga” que no explican qué sistema intervino realmente. Esta precisión adquiere mayor importancia si se considera que la aplicación de la agravante puede elevar la pena hasta en un tercio por encima del máximo establecido para el delito.

También debe acreditarse que el agente conocía la función que estaba utilizando y que decidió incorporarla a la comisión del hecho, pues no sería suficiente que una plataforma haya activado automáticamente alguna herramienta de inteligencia artificial durante su funcionamiento. No se requiere que la persona conozca cómo fue diseñado técnicamente el sistema, pero sí que sepa qué función está utilizando y que exista una decisión consciente de aprovecharla dentro de la conducta investigada.

Junto con ello, corresponde determinar qué papel cumplió la inteligencia artificial durante la ejecución, porque no tiene el mismo significado utilizarla de manera secundaria que recurrir a ella para crear una identidad falsa, imitar una voz, automatizar mensajes dirigidos a numerosas víctimas o procesar información obtenida ilícitamente. La relación con el delito debe ser concreta y demostrable, sin extender la agravante a cualquier uso tecnológico realizado por la persona antes o después de los hechos.

La importancia de esa intervención puede apreciarse a partir de los efectos que produjo en la forma de cometer el delito, como ocurre cuando permite llegar a un número mayor de víctimas, hacer más creíble un engaño, repetir operaciones de manera automatizada, dificultar la detección o aumentar la capacidad para afectar datos y sistemas. Estos supuestos no forman una lista cerrada, pero muestran que el aumento de pena debería responder a una diferencia real entre el delito cometido con esta tecnología y aquel que podría haberse realizado sin ella.

Antes de determinar la pena también tendría que revisarse si ese mismo uso de inteligencia artificial ya fue considerado dentro del propio delito o mediante otra agravante, porque una misma circunstancia no debería utilizarse nuevamente para aumentar la sanción. Cuando la figura penal ya contempla la manipulación mediante inteligencia artificial o existe una agravante especial sustentada en exactamente el mismo hecho, volver a aplicar el

artículo 11.5 o el artículo 46 generaría una valoración repetida de la misma conducta.

Estos criterios pueden aplicarse con la legislación vigente porque parten de la propia expresión “empleando” contenida en el artículo 11.5 y de los principios que orientan la responsabilidad penal, sin necesidad de ampliar el contenido de la norma hacia situaciones no previstas. Su utilidad radica en exigir que el aumento de pena pueda explicarse a partir de lo ocurrido en el caso concreto y no únicamente porque se haya identificado alguna herramienta de inteligencia artificial durante la investigación.

Una modificación posterior del numeral 5 podría ofrecer mayor claridad si relacionara expresamente el uso consciente de inteligencia artificial con una mayor capacidad para cometer el delito, engañar a la víctima, alcanzar a más personas, automatizar acciones o superar controles de seguridad. Una redacción de este tipo permitiría que el fundamento del aumento aparezca directamente en la ley y reduciría las diferencias de interpretación que podrían surgir cuando los jueces comiencen a aplicar esta agravante.

Desde esta perspectiva, podría plantearse que la norma señale que el aumento procede cuando el agente emplea deliberadamente un sistema basado en inteligencia artificial o una tecnología equivalente y dicho uso influye de manera relevante en la gravedad del delito, al facilitar el engaño, ampliar su alcance, automatizar su ejecución, aumentar el daño o permitir superar controles relacionados con la conducta realizada. Con ello no se busca excluir nuevas formas de criminalidad, sino hacer que la mayor pena dependa de la importancia que realmente tuvo la tecnología dentro del hecho.

La discusión tampoco debería concentrarse únicamente en aumentar las penas, porque la prevención de los delitos informáticos depende igualmente de la capacidad para detectar incidentes, proteger sistemas, verificar identidades, conservar evidencia y responder oportunamente cuando se presenta una afectación. Pascoe et al. (2024) integran gobierno, protección, detección, respuesta y recuperación dentro de la gestión de la ciberseguridad, mientras que Muhly et al. (2025) muestran que frente a fraudes apoyados en deepfakes siguen siendo necesarias medidas organizativas y mecanismos de verificación que reduzcan las posibilidades de engaño.

El crecimiento de las denuncias por ciberdelincuencia en el Perú exige, por la misma razón, algo más que incorporar nuevas agravantes, ya que fiscales, peritos y jueces necesitan contar con mejores condiciones para obtener, conservar e interpretar evidencia que muchas veces se encuentra distribuida entre dispositivos, cuentas y proveedores. La Ley N.º 32314 puede contribuir a sancionar conductas que presentan una gravedad mayor, pero su aplicación dependerá de que el uso de la tecnología pueda demostrarse adecuadamente y de que se respeten las garantías propias del proceso penal.

La ciberseguridad y el derecho penal cumplen funciones diferentes que se relacionan cuando ocurre un delito informático, pues mientras la primera busca reducir riesgos, proteger sistemas y mantener la continuidad de los servicios, el segundo determina si existe una conducta penalmente relevante y quién debe responder por ella. Mantener esa diferencia permite enfrentar nuevas formas de criminalidad sin convertir el uso de una determinada tecnología en una presunción de mayor responsabilidad.

11. CONCLUSIONES

La Ley N.º 32314 surge en un contexto en el que algunas herramientas de inteligencia artificial ya permiten ejecutar determinadas conductas con mayor rapidez, llegar a más personas y producir contenidos capaces de hacer más creíbles ciertos engaños. La generación sintética de voz e imagen, la automatización y el procesamiento de grandes cantidades de información muestran que la tecnología puede modificar la manera en que se cometen algunos delitos, lo que explica la decisión del legislador de incorporarla dentro del régimen de agravantes.

Sin embargo, el numeral 5 del artículo 11 de la Ley N.º 30096 permite aumentar la pena cuando se emplea inteligencia artificial o tecnologías similares o análogas sin precisar cuánto debe haber influido ese uso en la comisión del delito. Esta amplitud puede llevar a tratar de la misma manera a quien utilizó una herramienta de forma secundaria y a quien recurrió a ella para hacer más convincente el engaño, automatizar la conducta o ampliar considerablemente su alcance.

La referencia a tecnologías “similares o análogas” también requiere una aplicación cuidadosa para no incluir dentro de la agravante cualquier programa que presente algún grado de automatización. Aunque la Ley N.º 31814

y el Decreto Supremo N.º 115-2025-PCM pueden ayudar a comprender las características de los sistemas de inteligencia artificial, sus definiciones deben utilizarse como apoyo para interpretar la tecnología y no como una vía para ampliar los supuestos que pueden generar una pena más grave.

Para atribuir esta agravante tampoco sería suficiente comprobar que durante los hechos estuvo presente alguna función de inteligencia artificial, pues debe establecerse que el agente conocía esa capacidad y decidió utilizarla como parte de la conducta. Una función activada automáticamente por una plataforma o desconocida por el usuario no tiene el mismo significado que el empleo consciente de una herramienta destinada a facilitar la ejecución del delito, diferencia que debe mantenerse para que la responsabilidad continúe vinculada con las decisiones de la persona.

El aumento de pena encuentra una mejor justificación cuando puede demostrarse que la inteligencia artificial hizo realmente más grave la conducta, por ejemplo, al permitir engañar con mayor facilidad, alcanzar a numerosas víctimas, automatizar acciones, afectar una cantidad superior de datos o superar determinados controles. Cuando la herramienta solo tuvo una intervención secundaria que no modificó de manera apreciable el riesgo, el daño o la forma de ejecución, resulta mucho más difícil sostener que su sola presencia merece una respuesta penal más severa.

Otro aspecto que debe cuidarse al aplicar la reforma es la coincidencia entre las distintas disposiciones que incorporaron el uso de inteligencia artificial, pues esta aparece en los literales e) y ñ) del artículo 46 del Código Penal, en el numeral 5 del artículo 11 de la Ley N.º 30096 y en algunas figuras agravadas específicas. Cuando todas estas referencias recaen sobre el mismo uso tecnológico, no correspondería emplearlas sucesivamente para aumentar la pena si no existe una circunstancia diferente que justifique cada valoración.

Demostrar que un audio, una imagen o un texto fue generado mediante inteligencia artificial tampoco permite atribuir inmediatamente su creación o utilización a una persona determinada, porque todavía debe establecerse quién controlaba la cuenta, qué herramienta se empleó, qué instrucciones fueron proporcionadas y cómo llegó ese contenido a formar parte del delito. La autenticidad, la integridad y la trazabilidad de la evidencia digital ad-

quieren así especial importancia, pero deben valorarse junto con los demás elementos que permitan reconstruir la actuación del investigado.

A partir de estos problemas, antes de aplicar el artículo 11.5 resulta conveniente revisar cinco aspectos relacionados entre sí, referidos a la identificación de la tecnología utilizada, el conocimiento que tenía el agente, la función que cumplió la herramienta dentro del delito, la influencia que tuvo en su gravedad y la posible existencia de una valoración previa del mismo elemento. Estos criterios permiten aplicar la agravante cuando realmente exista una diferencia respecto del delito base y mantener el aumento de pena dentro de los límites de legalidad, culpabilidad y proporcionalidad.

La respuesta frente a los delitos informáticos en el Perú tampoco debería descansar únicamente en el incremento de las penas, porque una protección efectiva requiere prevenir incidentes, fortalecer la seguridad de los sistemas, conservar adecuadamente la evidencia y mejorar las capacidades de investigación. La Ley N.º 32314 puede contribuir a sancionar con mayor severidad aquellos hechos en los que la tecnología haya tenido una participación relevante, pero su aplicación no debería convertir cualquier uso de inteligencia artificial en motivo suficiente para aumentar la pena sin demostrar primero cómo influyó realmente en la gravedad del delito.

REFERENCIAS

- Casals Fernández, Á. (2025). La inteligencia artificial: su uso ilícito y el impacto en el Derecho Penal. *Revista Peruana de Ciencias Penales*, (39), 40–68. DOI 10.56176/rpcp.39.2025.150.
- Clough, J. (2015). *Principles of cybercrime* (2.ª ed.). Cambridge University Press. DOI 10.1017/CBO9781139540803.
- Congreso Constituyente Democrático. (1993). *Constitución Política del Perú*.
- Congreso de la República del Perú. (2013). *Ley N.º 30096, Ley de Delitos Informáticos*. Diario Oficial *El Peruano*.
- Congreso de la República del Perú. (2014). *Ley N.º 30171, Ley que modifica la Ley N.º 30096, Ley de Delitos Informáticos*. Diario Oficial *El Peruano*.

- Congreso de la República del Perú. (2023). *Ley N.º 31814, Ley que promueve el uso de la inteligencia artificial en favor del desarrollo económico y social del país*. Diario Oficial *El Peruano*.
- Congreso de la República del Perú. (2025). *Ley N.º 32314, Ley que modifica el Código Penal, Decreto Legislativo 635, y la Ley 30096, Ley de Delitos Informáticos, para incluir el uso de la inteligencia artificial en la comisión de delitos*. Diario Oficial *El Peruano*.
- Consejo de Europa. (2001). *Convention on Cybercrime*. European Treaty Series No. 185.
- Defensoría del Pueblo. (2023). *La ciberdelincuencia en el Perú: Estrategias y retos del Estado*. Defensoría del Pueblo.
- Guttman, B., White, D. R., & Walraven, T. (2022). *Digital evidence preservation: Considerations for evidence handlers* (NIST IR 8387). National Institute of Standards and Technology. DOI 10.6028/NIST.IR.8387.
- International Organization for Standardization. (2012). *ISO/IEC 27037:2012. Information technology –Security techniques– Guidelines for identification, collection, acquisition and preservation of digital evidence*. ISO.
- International Organization for Standardization. (2015). *ISO/IEC 27042:2015. Information technology –Security techniques– Guidelines for the analysis and interpretation of digital evidence*. ISO.
- Meneses Ochoa, J. P. (2026). Uso indebido de la inteligencia artificial en la difusión de imágenes sexuales: análisis del artículo 154-B del Código Penal peruano frente a los deepfakes y los deepnudes. *Revista Oficial del Poder Judicial*, 18(25), 71–112. DOI 10.35292/ropj.v18i25.1263.
- Ministerio Público Fiscalía de la Nación. (2026, 2 de marzo). *Celebran quinto aniversario de Fiscalías en Ciberdelincuencia con desarrollo de conferencia internacional*. Ministerio Público.
- Mir Puig, S. (2016). *Derecho penal: Parte general* (10.ª ed.). Reppertor.
- Muhly, F., Chizzonic, E., & Leo, P. (2025). AI-deepfake scams and the importance of a holistic communication security strategy. *International Cybersecurity Law Review*, 6, 53–61. DOI 10.1365/s43439-025-00143-7.

- National Cyber Security Centre. (2025). *Impact of AI on cyber threat from now to 2027*. NCSC.
- Panattoni, B. (2025). Generative AI and criminal law. *Cambridge Forum on AI: Law and Governance*, 1, e9. DOI 10.1017/cfl.2024.9.
- Pagallo, U. (2025). LLMs meet the AI Act: Who's the sorcerer's apprentice? *Cambridge Forum on AI: Law and Governance*, 1, e1. DOI 10.1017/cfl.2024.6.
- Pascoe, C., Quinn, S., & Scarfone, K. (2024). *The NIST Cybersecurity Framework (CSF) 2.0* (NIST CSWP 29). National Institute of Standards and Technology. DOI 10.6028/NIST.CSWP.29.
- Poder Ejecutivo del Perú. (1991). *Decreto Legislativo N.º 635, Código Penal*. Diario Oficial *El Peruano*.
- Presidencia del Consejo de Ministros. (2025). *Decreto Supremo N.º 115-2025-PCM, Decreto Supremo que aprueba el Reglamento de la Ley N.º 31814, Ley que promueve el uso de la inteligencia artificial en favor del desarrollo económico y social del país*. Diario Oficial *El Peruano*.
- Sandoval, M.-P., de Almeida Vau, M., Solaas, J., & Rodrigues, L. (2024). Threat of deepfakes to the criminal justice system: A systematic review. *Crime Science*, 13, 41. DOI 10.1186/s40163-024-00239-1.
- Sanguineti Ravettino, G. (2025). Criminalidad en tiempos de Chat-GPT: Análisis del uso de la Inteligencia Artificial como agravante penal en el Perú. *Forseti. Revista de Derecho*, 14(22), 395–411. DOI 10.21678/forseti.v14i22.2843.
- Tammenlehto, L., & Kallio, H. (2025). Artificial intelligence, criminal infringement and intent – Is the protection really equal for all works? *IIC - International Review of Intellectual Property and Competition Law*, 56, 939–969. DOI 10.1007/s40319-025-01592-7.
- Wall, D. S. (2024). *Cybercrime: The transformation of crime in the information age* (2.^a ed.). Polity.
- Yar, M., & Steinmetz, K. F. (2019). *Cybercrime and society* (3.^a ed.). SAGE.