

Criminalidad en tiempos de ChatGPT: Análisis del uso de la Inteligencia Artificial como agravante penal en el Perú

Giacomo Sanguineti*

Resumen.- El autor analiza la Ley 32314, la cual incorporó el uso de inteligencia artificial y tecnologías análogas como agravante penal y modalidad específica en ciertos delitos. Este artículo analiza su legitimidad bajo los criterios de subsidiariedad y necesidad de pena, y examina las capacidades institucionales requeridas para una aplicación efectiva, así como los beneficios y riesgos de dicha ley.

Palabras clave.- Inteligencia Artificial – Agravantes Penales – Delitos Informáticos – Deepfakes – Evidencia Digital – Política Criminal – Perú.

Abstract.- The author analyzes Law 32314, which incorporated the use of artificial intelligence and similar technologies as a criminal aggravating factor and specific modality in certain crimes. This article analyzes its legitimacy under the criteria of subsidiarity and necessity of punishment, and examines the institutional capacities required for effective implementation, as well as the benefits and risks of such a law.

Keywords.- Artificial Intelligence – Criminal Aggravating Factors – Cybercrime – Deepfakes – Digital Evidence – Criminal Policy – Peru.

* Estudiante de Derecho en la Universidad del Pacífico. Integrante del equipo técnico del despacho de asesores de la Tercera Vicepresidencia del Congreso de la República del Perú. Asociado de la Revista de Derecho Forseti. Miembro del Comité de Calidad de la Facultad de Derecho de la Universidad del Pacífico. Presidente del Centro de Estudiantes de la Universidad del Pacífico (CEUP). Asistente de docencia del curso de Derecho Penal General de la Universidad del Pacífico.

I. Introducción

A este punto resulta innegable la expansión que ha tenido la inteligencia artificial (IA) en un sinfín de áreas que inciden en el día a día de las personas¹. La impresionante capacidad de esta tecnología para replicar funciones humanas con una velocidad fuera de nuestras posibilidades, que van desde la realización de tareas cotidianas hasta procesos mucho más complejos, han forzado a que el Derecho se encuentre en la obligación de responder con la mayor rapidez y eficacia que le sea posible ante los desafíos éticos y las nuevas modalidades delictivas que ha traído consigo.

En ese contexto, el Perú ha dado un interesante pero significativo paso con la reciente aprobación de la Ley 32314² mediante la cual

¹ Respecto a lo que se entiende por IA, resulta complicado elaborar una definición unánime, ya que esta puede ser entendida de diversas maneras, dependiendo del enfoque que se adopte. No obstante, la Organización para la Cooperación y el Desarrollo Económico ha conceptualizado el término de Sistema de Inteligencia Artificial en: (OECD). *Hola, mundo: La Inteligencia Artificial y su uso en el sector público*. Documentos de trabajo de la OECD sobre Gobernanza Pública, Núm. 36. 2019, pp. 204-206. <https://oecd-opsi.org/wp-content/uploads/2020/11/OPSI-AI-Primer-Spanish.pdf> de la siguiente manera:

Un sistema basado en máquinas que puede, para un conjunto determinado de objetivos definidos por el ser humano, hacer predicciones, recomendaciones o tomar decisiones que influyen en entornos reales o virtuales. Los sistemas de IA están diseñados para funcionar con diversos niveles de autonomía. Además, las IA son “máquinas que realizan funciones cognitivas similares a las de los seres humanos”.

Asimismo, para tener una mayor comprensión sobre cómo la IA incide en los distintos ámbitos de las vidas de las personas, se recomienda consultar Comisión Europea. *Propuesta del Reglamento del Parlamento Europeo y del Consejo por el que se establecen normas armonizadas en materia de Inteligencia Artificial (Ley de Inteligencia Artificial) y se modifican determinados actos legislativos de la Unión*. 2021, p.1. https://eur-lex.europa.eu/resource.html?uri=cellar:e0649735-a372-11eb-9585-01aa75ed71a1.0008.02/DOC_1&format=PDF

² En el Perú los avances sobre propuestas normativas vinculadas a la inteligencia artificial son relativamente recientes, razón por la cual se ha empezado a desarrollar relacionada directamente con la Guía sobre la Inteligencia Artificial. Es con base a dichos avances que resulta novedosa la aprobación de la Ley 31813, Ley que promueve el uso de la inteligencia artificial en favor del desarrollo económico y social del país, cuyo artículo 3 establece que la inteligencia artificial debe entenderse como “Tecnología emergente de propósito general que tiene el potencial de mejorar

se introduce la utilización de la IA como circunstancia agravante en diversas conductas punibles, tanto en el Código Penal como en la Ley de Delitos Informáticos (aprobada mediante la Ley 30096)³. Esta decisión aprobada por el Congreso de la República refleja una respuesta directa a la creciente utilización maliciosa de la tecnología como las falsificaciones profundas (las denominadas “*deepfakes*”⁴), la manipulación multimedia y otras modalidades emergentes de delitos potenciados por IA.

A partir de esta respuesta del Estado peruano, se ha podido evidenciar que, si bien el boom del uso de la IA se ha producido tan solo hace algunos años, rápidamente este se ha convertido en un mecanismo instrumentalizado por personas malintencionadas para causar daño a terceros y vulnerar bienes jurídicos que el Código Penal busca a toda costa proteger. En ese sentido, la relevancia de esta regulación radica no solo en un reconocimiento formal del potencial impacto que puede tener la IA sobre la gravedad de determinados delitos, sino que también representa un mensaje simbólico respecto de la intencionalidad del Estado para adaptar el marco jurídico a uno que sea capaz de dar respuesta a los desafíos tecnológicos actuales.

Sin embargo, cualquier tipo de adaptación normativa no va a estar libre de complejidades y puntos críticos. En particular, en este tipo de propuestas siempre se van a presentar cuestionamientos respecto de cuál va a ser el tipo de concepto que se va a adoptar de inteligencia artificial, qué se va a entender por “tecnologías análogas”, los mecanismos probatorios que

el bienestar de las personas, contribuir a una actividad económica global sostenible positiva, aumentar la innovación y la productividad, y ayudar a responder a los desafíos globales clave”.

³ Específicamente, el nombre completo de la referida norma -la cual fue publicada en el Diario Oficial El Peruano con fecha 29 de abril de 2025- es Ley 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.

⁴ Como tal, las *deepfakes* son entendidas como un tipo de manipulación digital de contenido, el cual tiene como elemento esencial el utilizar la IA para crear videos, audios o imágenes que simulan de manera extremadamente realista a personas diciendo o haciendo cosas que en realidad jamás ocurrieron. Debe tenerse en cuenta que estas resultan particularmente peligrosas en el contexto actual, ya que pueden ser utilizadas como herramienta para engañar, difamar, extorsionar o cometer fraudes, entre otros delitos, los cuales no son sencillos de detectar.

son necesarios para demostrar su rol en el marco de la comisión de un delito o, en general, si es que es necesaria como tal una regulación de la IA en un escenario en donde esta tecnología recién está empezando a consolidarse en un país como el nuestro.

Ante esta problemática, el presente artículo pretende delinear algunos conceptos esenciales para poder entender los aspectos que abarca la Ley 32314 (en adelante, la ley de IA como agravante), para posteriormente identificar sus implicancias jurídicas y los desafíos que representa, para finalmente brindar algunas ideas sobre posibles soluciones a dichos retos.

II. Criminalidad potenciada por la IA: Análisis de la Ley 32314

i. Antecedente legislativo

La ley bajo análisis tuvo su origen en el Proyecto de Ley 8746/2024-CR, el cual fue presentado a iniciativa del congresista Isaac Mita Alanoca. La fórmula utilizada en el proyecto de ley proponía modificar el Código Penal para (i) incorporar el uso de inteligencia artificial como circunstancia agravante genérica en el artículo 46.2.e y (ii) agravar el delito de estafa mediante la introducción del numeral 7 en el artículo 196-A cuando se empleen voz, imagen, audio o movimiento corporal de terceros con IA⁵.

Respecto a la Exposición de Motivos, esta sustenta la necesidad de intervención penal en la medida que las herramientas digitales se han convertido en un medio para facilitar actividades ilícitas y aprovecharse de las víctimas. Asimismo, la Exposición de Motivos sostiene que ello iría en línea con la expansión del marco normativo en diferentes aspectos vinculados a la IA, tales como las leyes de delitos informáticos⁶ y de ciberseguridad⁷. Además, si bien existe la Ley de Promoción del Uso de

⁵ Si bien la fórmula inicial del Proyecto de Ley hablaba sobre el agravante genérico para diversos delitos, el enfoque sobre tipos específico se encontraba en su totalidad enfocado en la estafa agravada mediante inteligencia artificial, no advirtiéndose la presencia de agravantes en otros tipos penales como el plagio, pornografía infantil, infracción de derechos de autor, etc.

⁶ Ley 30096, Ley de delitos informáticos.

⁷ Ley 31212, Ley de Ciberseguridad. La referida norma también cuenta con su reglamento, aprobado por Decreto Supremo 012-2020-IN.

la IA, aprobado por la Ley 31814, esta es una norma genérica que no contiene ninguna disposición sancionatoria.

En cuanto al contexto que se brinda en torno a la norma, la Exposición de Motivos sitúa la propuesta en un escenario de rápida expansión de la IA: la adopción global de estas tecnologías creció 250% entre 2017 y 2022, y se resalta que el país busca integrar la IA en servicios públicos como educación y seguridad ciudadana. Asimismo, resulta interesante la referencia de que el Perú se ubicaría entre los cinco primeros países de Latinoamérica que más han adoptado este tipo de tecnologías, lo cual justificaría la oportunidad y urgencia para la intervención penal.

En un plano similar, se afirma que la regulación de IA debe tener un impacto transversal en el ordenamiento jurídico, –que implica la creación y actualización de leyes– a fin de asegurar un uso ético y seguro de esta.

Sin dudas, el referido Proyecto de Ley 8746/2024-CR fue la base esencial para poder llevar a cabo la aprobación de la norma bajo referencia, por lo que se procederá a describir brevemente el texto final de la norma, a fin de poder continuar con el análisis respectivo.

ii. Modificaciones introducidas mediante la aprobación de la Ley 32314

La Ley de IA como agravante introduce dos artículos clave y una Disposición Complementaria Final, con un objetivo claro: insertar el uso de la IA y tecnologías similares o análogas como criterio de agravación tanto en el Código Penal, como en la Ley 30096. En términos prácticos, ello habilitaría, cuando corresponda, el incremento de la pena hasta un tercio por encima del máximo legal fijado para cualquiera de los delitos comprendidos en el mismo.

De forma específica, lo esencial de la reforma está en las circunstancias de atenuación y agravación (art. 46): se reformula el literal e) y se incorpora el literal ñ) para convertir el empleo de IA o tecnologías análogas en una agravante genérica, útil cuando el tipo base no prevé expresamente el empleo de dicho componente tecnológico. Así, este cambio actuaría como una “puerta de entrada” transversal a distintos tipos penales para capturar escenarios en los que la tecnología aumenta sustancialmente la lesividad, la escala del daño o la expectativa de impunidad.

Tomando como base la lógica de este criterio general -aunque bajo una lógica distinta- la ley ajusta tipos específicos donde la IA ya viene teniendo impactos prácticos. En delitos contra la libertad sexual, el art. 129-M (pornografía infantil) incluye contenidos generados por IA – como *deepfakes* u otras técnicas de síntesis – para cerrar la brecha entre producción “tradicional” y generación artificial de material. En delitos contra el honor, el art. 132 (difamación) eleva el reproche cuando la falsedad o denigración se difunde mediante contenidos creados por IA, atendiendo al alcance y persistencia que la manipulación automatizada de contenidos puede dar a la lesión reputacional de las personas afectadas. En delitos patrimoniales, el numeral 7 del art. 196-A agrava la estafa cuando el agente manipula voz, imagen o movimiento corporal mediante IA para causar el perjuicio económico, con el foco puesto en clonación de voz y suplantación audiovisual como medios de captación de confianza. Finalmente, en delitos contra los derechos intelectuales, se modifican los artículos 217, 218, 219 y 220 y se incorporan los arts. 220-A, 220-B y 220-C, para sancionar la elusión de medidas tecnológicas y la fabricación o provisión de herramientas o servicios destinados a esa elusión cuando tal conducta sea facilitada por IA, reforzando la tutela frente a automatizaciones que erosionan controles de acceso o integridad de obras.

Por otro lado, la Ley 30096 de Delitos Informáticos es coherente también con este diseño, dado que faculta al juez a aumentar la pena hasta un tercio por encima del máximo legal cuando el agente comete el delito informático empleado herramientas de inteligencia artificial o tecnologías análogas, buscando lograr una armonización entre el tratamiento que se está buscando implementar en el Código Penal y el sistema de delitos informáticos.

Estándares de subsidiariedad y necesidad de la pena: ¿Se encuentra justificada la Ley 32314?

Ahora bien, resulta menester tener en consideración que el solo hecho de que el Perú se presente como un escenario propenso al uso masivo de la inteligencia artificial no justifica, por sí mismo, la necesidad de que el derecho penal deba intervenir sancionando conductas. Al final, en más de una oportunidad se han incluido tipos al Código Penal cuya elaboración no ha pasado por la mejor técnica legislativa, lo que al final termina resultando ineficiente y dejando con una protección nula a los bienes jurídicos que se pretendía cuidar en primer lugar.

La intervención penal del Estado en el marco del crecimiento de la IA en el país debe ser resultado de una reflexión consciente sobre sus costos, beneficios y riesgos. En ese sentido, una modificación del Código Penal debe examinar cuidadosamente la expansión del *ius puniendi* del Estado. Para ello, es importante evaluar la pertinencia de la presente ley desde los criterios de subsidiariedad y necesidad de la pena⁸.

Al respecto, la subsidiariedad exige recordar que el Derecho penal es *ultima ratio*, esto es, su intervención debe constreñirse únicamente a los escenarios en los que otros instrumentos -normas extrapenales, políticas públicas, técnicas jurídicas o normas y agravantes ya existentes- resultan insuficientes para contener un incremento real de lesividad o de impunidad. La necesidad de la pena impone, además, que cualquier agravación demuestre idoneidad, ausencia de alternativas menos gravosas y se demuestre que se cumple un criterio de proporcionalidad en sentido estricto.

A fin de aterrizar dichos criterios en esta materia, el examen debe responder, al menos, a tres preguntas encadenadas: (i) si la IA cumple un rol de contribución sustancial en la comisión, la escala u ocultamiento del delito; (ii) si su empleo eleva *ex ante* el riesgo de lesión del bien jurídico o la expectativa de impunidad más allá de lo ya previsto por la ley vigente; y (iii) si introduce una dificultad probatoria añadida (detección, atribución o trazabilidad) que justifique un mayor reproche. Cuando estas condiciones se cumplen de forma copulativa, la agravación

⁸ Respecto a este concepto, Villavicencio es bastante categórico cuando señala que la doctrina coincide en que la subsidiariedad es una nota distintiva de la respuesta penal. Esto significa que el Derecho penal solo debe activarse cuando los demás instrumentos del ordenamiento y los controles sociales no penales resultan insuficientes; precisamente por la severidad de sus sanciones, los ataques menos graves a los bienes jurídicos deberían de canalizarse, en principio, por vías extrapenales.

La subsidiariedad se complementa con el principio de fragmentariedad, y ambas se ordenan bajo el principio de intervención mínima. Según Villavicencio, esta directriz de política criminal tiene un triple alcance: el Derecho penal debe (i) seleccionar únicamente los ataques de especial gravedad contra el bien jurídico; (ii) tipificar solo una parte de las conductas que en otras ramas ya se consideran antijurídicas; y (iii) excluir del castigo las acciones meramente inmorales.

Para mayor referencia, ver VILLAVICENCIO, F. (2006). *Derecho Penal. Parte general*. Lima: Grijley.

de conductas ya no es simbólico, sino un ajuste funcional a un *modus operandi* que intensifica el desvalor de la conducta.

Aplicado al artículo 46 como cláusula general, el test se supera siempre que el término “tecnología análoga o similar” no opere como un “cajón de sastre”, sino como una “llave” que permita incluir medios que efectivamente potencian la comisión o dificultan su persecución. La idoneidad es clara si el uso de IA hace posible un ataque a escala o un ocultamiento que el agente no habría logrado con medios ordinarios.

En ese sentido, la necesidad se verifica cuando no existen agravantes previas que puedan abarcar ese plus de riesgo o de impunidad, mientras que la proporcionalidad exige un umbral de aplicación explícito en la motivación judicial, lo cual también resulta necesario por criterios del derecho al debido proceso⁹.

Respecto del conjunto de modificaciones específicas (libertad sexual, honor, patrimonio y derechos intelectuales), el mismo patrón analítico permite una valoración diferenciada sin entrar aún al detalle caso por caso.

En estos bloques, la idoneidad se fortalece porque el legislador identifica fenómenos concretos -tales como síntesis audiovisual artificial, clonación de voz, elusión automatizada de controles- cuyos efectos típicos son la ampliación del daño y la dificultad de realizar trazabilidad sobre la autoría. De ahí que la necesidad se justifica en la medida en que el tipo base o sus agravantes tradicionales no reflejan adecuadamente ese plus de peligrosidad ni la expectativa de impunidad que trae la automatización; y la proporcionalidad se satisface si la agravación se reserva a supuestos donde la IA no es un mero accesorio, sino un factor determinante para la consumación del delito.

Resulta evidente que pueden caber objeciones sobre un eventual solapamiento con agravantes ya previstos; aun así, al tratarse de técnicas

⁹ Un posible cuestionamiento sobre este apartado sería la vaguedad de término en sí. Una situación similar ocurre a las críticas que -salvando las distancias entre el derecho penal y administrativo- tuvo desde sus inicios la cláusula general en la Ley de Represión de la Competencia Desleal. Sin embargo, acotada por el umbral descrito y apoyada en indicios técnicos verificables, lo cual requiere de inversión y desarrollo de capacidades técnicas, la cláusula cumple la función de cierre que persigue.

de generación o manipulación sintética de difícil detección, el ajuste normativo se sostiene siempre que se exija al juez la demostración el nexo causal tecnológico en la motivación.

En cuanto a la regla de aumento en la Ley 30096, su justificación deriva de lo anterior: los ciberdelitos cometen, por definición, su ataque en un entorno donde la IA puede multiplicar velocidad, alcance y opacidad.

De todas maneras, resulta importante advertir que este debería haberse derivado de forma explícita en la misma Exposición de Motivos y no tener que presumirla, por lo que fue una oportunidad perdida. Sin perjuicio de ello, como se ha demostrado en el presente apartado, existe efectivamente una metodología que permite justificar la razón de ser de la Ley de IA como agravante en función de los criterios de subsidiariedad y necesidad de la pena.

En todo caso, la superación de este test no un tema meramente dogmático, sino también operativo: exige capacidades institucionales suficientes en las autoridades pertinentes como la Fiscalía y la Policía Nacional del Perú para constatar el nexo tecnológico y su rol en la comisión del delito. Como mínimos, deberá garantizarse la integridad y preservación de evidencia digital (por ejemplo, con procesos adecuados de *hashing* y cadena de custodia), pericia especializada en análisis audiovisual y de voz, así como protocolos para la recepción de las pruebas. Sin estos estándares, la aplicación de la agravante corre el riesgo de generar inseguridad jurídica.

El criterio central es claro: agravar únicamente cuando la IA aporte una contribución sustancial, un aumento del riesgo y/o daño y añada una dificultad probatoria sustantiva, lo que deberá reflejarse adecuadamente en la motivación de las sentencias en las que deban ser analizados la comisión de estos tipos penales.

iv. Análisis de las implicancias jurídicas y desafíos

Si hay algo que no se puede negar a partir de la incorporación de la Ley de IA como agravante es que es representa un antes y un después en el abordaje regulatorio que va a tener la inteligencia artificial en el Perú. Por un lado, existen posturas más proteccionistas que ven con sospecha a la violenta evolución de la inteligencia artificial, tanto por sus impactos en el entorno laboral relacionado al potencial reemplazo de puestos de trabajo en diversas áreas cuyas labores podrían ser automatizadas (o, en

todo caso, volverlas mucho más productivas con el uso de la IA), como el mal uso que se le ha dado a esta herramienta en múltiples ámbitos, tales como los vinculados al plagio académico o la violación de derechos de propiedad intelectual, entre otros.

Por otro lado, una posición diferente se ve representada por el sector privado y los negocios emergentes –y hasta, en varias oportunidades, el sector público– quienes ven a la inteligencia artificial como un fenómeno revolucionario que vino para quedarse y al que debemos adaptarnos; y mientras antes nos adaptemos, mejor. Esta tendencia más receptiva y liberal hacia la IA ve con buenos ojos el enorme potencial que tiene para mejorar el desarrollo de la colectividad, sobre todo teniendo en cuenta el crecimiento exponencial de la economía digital en los últimos años. De hecho, por la misma redacción de la Ley 31813 y su Proyecto de Reglamento, pareciera ser este el enfoque por el que el legislador ha optado.

Ahora bien, aunque ambas posiciones naturalmente suelen verse enfrentadas, no quiere decir que no puedan –e incluso deban– complementarse en determinados contextos. Es decir, las posiciones previamente descritas no son en ninguna circunstancia excluyentes, por lo que considero que debemos tener una posición en general de apertura hacia la IA, pero a la vez debemos ser capaces de reconocer sus riesgos y de actuar respecto de ellos de forma preventiva, a fin de que las virtudes de la IA puedan convivir con los objetivos de desarrollo del Estado peruano.

Teniendo ello bajo consideración, el hecho de que se haya incluido a la IA como un agravante en el Código Penal y en la Ley de Delitos Informáticos representa una modernización sin precedentes en nuestra legislación penal. A nivel simbólico, la tipificación de la IA en este escenario genera una narrativa por parte del legislador de que no serán tolerables las conductas de todo aquel que procure instrumentalizar esta herramienta para facilitar la comisión de un delito o para ampliar su alcance, razón por la cual la respuesta punitiva del Estado será mayor, buscando reforzar la función preventiva de la norma penal.

De esta manera, podemos apreciar la primera virtud de norma, que es el efecto disuasivo que busca alcanzar. Si lo analizamos desde la perspectiva del transgresor de la norma penal, el empleo de la IA, que en otras circunstancias lo habría ayudado a poder generar *deepfakes*

para extorsionar a otras personas o plagiar una obra, deja de ser un mecanismo rentable.

Ello principalmente se debería a dos motivos: (i) La sanción penal es mayor, por lo que el análisis costo-beneficio del delincuente para ejecutar la conducta sancionable debe necesariamente incluir este factor en la evaluación; y (ii) es posible que aumente la probabilidad de detección si es que el Estado garantiza el empleo de recursos públicos a las instituciones competentes para hacer viable la identificación de estos delitos. En otras palabras, se pretende alterar la balanza de incentivos del infractor, con el objetivo que la IA ya no sea percibida únicamente como un factor que garantiza el anonimato o que puede implicar alguna sanción administrativa (o, en el mejor de los casos, un ostracismo mediático), sino como un factor que hace que la comisión del delito pierda atractivo.

Un segundo tema que merece atención es el hecho de que la reforma combina una agravante genérica, que es la contenida en el artículo 46 del Código Penal, con ajustes específicos en tipos penales concretos relativos a conductas que en la práctica son los que más han sufrido por el incremento en el uso de la IA.

Esta decisión, a menos a mi entender, no es caprichosa o deliberada, sino que es parte de una estrategia de técnica en diseño legislativo que opta por evitar constantes modificaciones normativas cada vez que una nueva herramienta tecnológica que pueda ser catalogada como “análoga” a la IA incida en algún delito. De esta forma, mientras que por un lado se tiene a ciertos delitos que ya contienen el agravante de la IA incorporado en el texto del tipo, en el resto de los casos solo basta verificar que la conducta se encuentre “potenciada por IA” para agravarla.

De todas formas, respecto al artículo 46 en concreto, la aplicabilidad de esta cláusula recae también en la capacidad del Poder Judicial para exigir una motivación reforzada cuando se invoque el uso de IA como agravante. En línea con lo desarrollado previamente, corresponde al juzgador explicitar por qué la tecnología tuvo una contribución sustancial en la comisión, escala u ocultamiento del delito y por qué ese plus no está ya captado por agravantes ordinarias. Tal conclusión debe apoyarse en pericias técnicamente fiables, con metodología identificable, control de errores y adecuada trazabilidad y cadena de custodia.

Un tercer acierto de la norma radica en que es plenamente consciente de los riesgos que la inteligencia artificial implica para determinadas conductas sociales. De un lado tenemos el reconocimiento explícito de fenómenos contemporáneos como lo son los *deepfakes*, por lo que su evaluación en el marco de una investigación penal tendrá cierto nivel de certeza.

De otro lado, las conductas cuyas modificaciones no se ven afectadas por el artículo 46 han sido objeto de constantes y acalorados debates en la actualidad. Por ejemplo, escándalos relativos a la posesión o distribución de pornografía infantil¹⁰, así como las interminables discusiones del rol de la IA en la elaboración de documentos de autoría propia que pueden terminar en plagio¹¹, son situaciones que se dan en el día a día y frente a los cuales la población buscaba una respuesta.

¹⁰ Durante los últimos años, constantemente ha habido escándalos de estudiantes universitarios que han sido capturados por posesión y presunta difusión de pornografía infantil, tal como el caso de un estudiante arequipeño en 2023. LINARES, K. (2023). Universitario de 22 años fue detenido por posesión de pornografía infantil. Diario el Pueblo. <https://diarioelpueblo.com.pe/2023/07/20/universitario-de-22-anos-fue-detenido-por-posesion-de-pornografia-infantil/>.

Aún más sorpresivo, recién el pasado 21 de mayo un estudiante fue detenido en Trujillo por la posesión de videos sexuales en donde aparecerían menores de 13 años, lo cual ha generado gran debate en redes sociales. RAMOS, P. (2025). PJ dicta prisión preventiva para joven universitario tras hallársele 100 mil archivos de pornografía infantil en Trujillo. RPP. <https://rpp.pe/peru/la-libertad/trujillo-dictan-prision-preventiva-para-joven-universitario-tras-hallarsele-100-mil-archivos-de-pornografia-infantil-noticia-1636064>.

Si bien en ninguno de estos casos parte de la discusión se ha encontrado en la utilización de la IA como herramienta que facilite el delito, la norma busca anticiparse ante estos escenarios, a fin proteger los bienes tutelados de libertad e indemnidad sexual de los menores en contextos tan delicados como este.

¹¹ El año pasado, el congresista del Bloque Magisterial, Paul Gutiérrez, fue acusado de copiar y pegar contenido generado por IA en, al menos, la elaboración de dos propuestas legislativas presentadas como si fueran de su autoría. PINEDO, J. (2024). Acusan a congresista Paul Gutiérrez de copiar y pegar respuestas de la inteligencia artificial en sus proyectos de ley. RPP. <https://rpp.pe/politica/congreso/acusan-a-congresista-paul-gutierrez-de-copiar-y-pegar-respuestas-de-la-inteligencia-artificial-en-sus-proyectos-de-ley-noticia-1556672>.

Probablemente el caso más paradigmático, atendiendo al contexto de los últimos meses, es el de la extorsión¹², las amenazas y las estafas¹³, ante las cuales nuestro país lamentablemente se ha visto sumido en una ola de violencia que no parece que vaya a cesar de forma significativa en el corto plazo. En ese sentido, la atención de estas situaciones era necesaria vista la realidad peruana que nos rodea. De esta forma, se espera que esta normativa pueda alcanzar a los referidos actos delictivos en las circunstancias en las que se use IA, a fin de disminuir su reincidencia.

Aunque ello va a depender mucho de la voluntad de los funcionarios públicos, un efecto positivo de este impulso podría estar vinculado con la presión que esta ley ejerce sobre las instituciones públicas encargadas de la persecución penal. Bajo esa línea de argumentación, el convertir a la IA como agravante de un delito “obliga” a la Policía Nacional del Perú, al Ministerio Público y al poder Judicial a reforzar sus conocimientos y capacidades técnicas.

Así, se requiere de peritos especializados, capacitación constante y protocolos de cadena de custodia para el material digital que sean más robustos. A ello se suma la necesidad de contar con una infraestructura tecnológica suficiente (laboratorios forenses, softwares de preservación

¹² Nuestro país durante los últimos meses se ha visto inmerso en una gigantesca ola de violencia. RAMÍREZ, S. Paro nacional para el 14 de mayo: ¿Qué gremios paralizarán y qué servicios no estarán disponibles? El Comercio. <https://elcomercio.pe/lima/paro-nacional-para-el-14-de-mayo-que-gremios-paralizaran-y-que-servicios-no-estaran-disponibles-noticia/>. Redacción EC. (2025). Transportistas de Lima convocan a paro el 10 de abril por creciente ola de extorsiones y violencia. El Comercio. <https://elcomercio.pe/lima/transportistas-de-lima-convocan-a-paro-el-10-de-abril-por-creciente-ola-de-extorsiones-y-violencia-inseguridad-ciudadana-estado-de-emergencia-ultimas-noticia/>.

Si bien el uso de la IA no se da en todos los contextos, la preocupación por esta herramienta sumado al miedo por las extorsiones tradicionales provoca que el miedo colectivo aumente.

Sin perjuicio de ello, el plagio mediante IA es un tema que se ha venido discutiendo en la academia y en la prensa desde hace algún tiempo.

¹³ El fraude digital ha ido cogiendo bastante fuerza en el país, situación que podría empeorar debido a la mayor especialización de los ciberdelinquentes que usan herramientas de inteligencia artificial. MELO, Y. (2025). Fraude digital en Perú: el 90% de limeños teme ser víctima mientras las estafas se vuelven más sofisticadas. Infobae. <https://www.infobae.com/peru/2025/03/24/fraude-digital-en-peru-el-90-de-limenos-teme-ser-victima-mientras-las-estafas-se-vuelven-mas-sofisticadas/>

de evidencia, servidores seguros, etc) y de criterios uniformes de actuación que eviten diferencias arbitrarias entre fiscalías o distritos judiciales. Cuando no se invierte en este tipo de capacidades, la prueba digital termina cuestionada en cualquier instancia del proceso judicial, con el riesgo de absoluciones por fallas técnicas más que por falta de culpabilidad.

Evidentemente, ello implica una importante inversión de los recursos públicos para que dichas competencias puedan ser efectivamente ejercidas, por lo que, volviendo a la idea previa, ello será bastante contingente al compromiso que exista por parte de las instituciones.

Ahora bien, a modo de primera crítica, resulta relevante señalar que la expresión “tecnologías análogas o similares” representan cierto nivel de riesgo para el principio de legalidad y taxatividad. Sin perjuicio de que sus alcances se hayan esbozado en las secciones precedentes de este artículo, no puede negarse que una expresión tan amplia puede colisionar con la predictibilidad en la aplicación de la norma y, ergo, en la seguridad jurídica que debe primar en el derecho penal.

Así, el no contar con una definición clara para estas herramientas, aumenta el riesgo de discrecionalidad con la que los jueces pueden aplicar la norma, vulnerando potencialmente no solo el derecho de defensa, sino aumentando también el riesgo de pronunciamientos contradictorios. Además, teniendo en consideración que la Única Disposición Complementaria Final prevé la emisión de normativa adicional necesaria en el plazo de sesenta días calendarios desde la entrada en vigor de la norma, quedan dudas razonables sobre cómo se van a abordar este otro tipo de tecnologías (sobre todo, teniendo en cuenta que nuestro desarrollo sobre investigación en IA aún es muy incipiente y solemos extraer las definiciones que ya han sido acogidas en otras legislaciones), por lo que uno se podría preguntar, ¿estamos ante una remisión normativa? ¿Se trata de una ley penal en blanco? ¿Respecto de qué otro tipo de tecnologías me podrían sancionar? Dada esta situación, resulta imperante tener una respuesta adecuada.

Otra discusión importante radica en tema probatorio. Primero, los operadores de justicia deben tener cuidado con la interpretación de la norma y ser bastante precisos al momento de determinar que el uso de la inteligencia artificial cumplió un papel trascendental en la comisión de la conducta infractora. El mero uso de una tecnología no necesariamente

aumenta de forma significativa la lesividad de un hecho, pero el riesgo se encuentra en concluir inmediatamente que corresponde la aplicación del agravante. En ese sentido, resulta necesario definir los lineamientos y estándares que serán aplicables para estos casos.

Sobre este mismo punto, debe tenerse en cuenta que la intervención de algoritmos, redes neuronales y *deepfakes* usualmente requieren de pericias avanzadas, acceso a herramientas de análisis forenses especializadas o conservación de evidencias efímeras¹⁴. En la medida que no se cuentan con dichos recursos, o estos son muy limitados, es menester realizar una distribución eficiente del dinero público para invertir en herramientas avanzadas que permiten un verdadero incremento en la probabilidad de detección de estos delitos.

Finalmente, se debe cuidado con el efecto inhibitorio que pueda generar la Ley de IA como agravante sobre la innovación. Si bien resulta positivo que se genere un mensaje de modo que el sector privado tenga cuidado en el desarrollo de software potenciado con IA, ello puede implicar una serie de costos. En principio resulta positivo que la reforma induzca a proveedores y desarrolladores a reforzar autenticación, trazabilidad y políticas de uso responsable de la inteligencia artificial, así como a ser mucho más cuidadosos con la cadena de custodia de información.

No obstante, una regulación excesivamente laxa también genera costos y puede desalentar decisiones empresariales relevantes. Si el marco no es lo suficientemente claro, aumentan los costos de cumplimiento privado preventivos (seguros, auditorías, contratos más restrictivos) y los riesgos ex post (litigios o sanciones reputacionales) por la dificultad de demostrar la diligencia. En ese entorno, empresas prudentes podrían retrasar lanzamientos, limitar funcionalidades sensibles o imponer

14 Piénsese, por ejemplo, en la necesidad de (i) software de análisis de patrones de comprensión o incongruencias de fotogramas para comparar videos sospechosos con bases de datos de rostros o voz originales en el caso de los *deepfakes*; (ii) herramientas de espectrograma o programas de análisis forense de audio clonado; (iii) inspección de redes neuronales en dispositivos incautados para rastrear si es que fueron entrenadas para generar contenido ilícito; (iv) órdenes de preservación rápida con el fin de congelar logs, metadatos y snapshots de las máquinas donde se generaron los archivos; y (v) herramientas de análisis de tráfico de red para tener trazabilidad sobre los flujos de datos que permita rastrear la distribución de *deepfakes*, entre otros.

barreras de acceso a usuarios de mayor riesgo, lo que igualmente impacta en la velocidad de innovación.

En cambio, un marco sólido y predecible —como el que se viene consolidando en materia de ciberdelincuencia— puede operar como señal de certidumbre, dado que alinea expectativas, facilita la debida diligencia con clientes y proveedores y reduce la probabilidad de controversias por zonas grises. El punto no es “más” o “menos” regulación, sino mejor aplicación de la misma: criterios claros de cuándo la IA aporta una contribución sustancial que justifica la agravación, estándares probatorios mínimos y una motivación reforzada que evite sancionar el mero uso tecnológico neutro.

En cualquier caso, se debe tener cuidado con la aplicación de la ley, ya que nuestro ordenamiento aún se encuentra construyendo sus primeros cimientos en regulación de inteligencia artificial, por lo que, si bien la iniciativa se saluda y tiene una serie de puntos a destacar, la cautela siempre será la estrategia más adecuada.

III. Conclusiones

Definitivamente la aprobación de la Ley 32314 marca un punto de inflexión en la política criminal ante la expansión de la inteligencia artificial. La norma moderniza el Código Penal y la Ley 30096 al reconocer que la IA amplifica la velocidad, el alcance y la magnitud de una serie de conductas ilícitas. Debido a ello, la ley presenta un mensaje disuasorio claro; no obstante, la reforma evidencia tensiones inevitables entre la necesidad de proteger bienes jurídicos y el deber de salvaguardar los principios de legalidad, proporcionalidad y seguridad jurídica.

Como se ha explicado a lo largo de la presente investigación, este nuevo régimen presenta algunos riesgos que deben examinarse. Entre ellos, el uso de conceptos como “tecnologías análogas o similares” puede generar cierto grado de incertidumbre normativa; la carga probatoria para demostrar que una conducta ilícita ha sido facilitada o conseguida mediante IA exige de una infraestructura forense difícil de aplicar en nuestro país hoy mismo; y la amenaza de sanciones sin criterios claros podría desalentar algunos proyectos de innovación si es que no existe una armonización con los intereses legítimos del sector privado.

En ese sentido, más allá de los beneficios de la norma que han sido resaltados en el presente trabajo, a fin de mitigar los riesgos se recomienda,

de forma general: (i) Emitir criterios técnicos que delimiten de forma más precisa las circunstancias en las que se configura el agravante o, en todo caso, que la normativa futura que se va a emitir sea lo suficientemente clara en este apartado; (ii) Procurar dotar a los jueces, fiscales y peritos de los recursos necesarios y la capacitación adecuada en temas de inteligencia artificial y cómo combatir su uso para fines ilícitos; y (iii) No descuidar el *soft law*, ya que acompañar este proceso con guías de buenas prácticas o *sandboxes* regulatorios pueden permitir a las empresas desarrollar programas de IA responsable y ética sin el riesgo de que sean penalizados por ello.

En síntesis, la promulgación de esta ley constituye un gesto relevante del legislador frente a los complejos desafíos que plantea el entorno digital contemporáneo. Sin embargo, en el ámbito penal, la aprobación de una norma no puede leerse simplemente como una respuesta coyuntural; debe entenderse como el ejercicio, siempre delicado, del ius puniendi del Estado. Y ese poder, por su misma naturaleza, exige sobriedad, contención y una responsabilidad institucional a la altura de su alcance.

Una política criminal efectiva no se define por la severidad de sus penas ni por la celeridad de su tramitación legislativa, sino por su capacidad de resistir al tiempo, a la presión política y a los vaivenes de la opinión pública. El verdadero equilibrio se alcanza cuando se logra proteger eficazmente a la sociedad sin erosionar los pilares del Estado de Derecho, la seguridad jurídica ni el dinamismo propio de la innovación tecnológica.

Se dice —con razón— que el derecho y la justicia suelen llegar tarde. Y aunque ello sea cierto, más grave aún es que se anticipen sin reflexión, pues pueden terminar lesionando los derechos que buscaban tutelar. En ese sentido, legislar con rigor técnico, con deliberación informada y con conciencia de las consecuencias jurídicas y sociales de cada decisión no es una opción: es una exigencia inherente al mandato constitucional del legislador.