CONGRESO DE LA REPÚBLICA
ÁREA DE TRÁMITE DOCUMENTARIO
04 DIC. 2023
RECIBIDO
Firma: Hora: 3:05 pm

"LEY QUE INCORPORA COMO CIRCUNSTANCIA AGRAVANTE LA UTILIZACIÓN DE LA INTELIGENCIA ARTIFICIAL PARA LA COMISIÓN DE DELITOS"

La Congresista de la República, que suscribe **MARÍA DEL CARMEN ALVA PRIETO**, con la facultad establecida en el artículo 107° de la Constitución Política, en concordancia con el artículo 22° inciso c), 67°, 75° y 76° del Reglamento del Congreso de la República, presenta el siguiente:

PROYECTO DE LEY

EL CONGRESO DE LA REPÚBLICA;

Ha dado la siguiente Ley:

"LEY QUE INCORPORA COMO CIRCUNSTANCIA AGRAVANTE LA UTILIZACIÓN DE LA INTELIGENCIA ARTIFICIAL PARA LA COMISIÓN DE DELITOS"

Artículo 1. Incorporación del literal o) en el numeral 2 del artículo 46 y el literal 8) en el artículo 196-A del Código Penal aprobado en el Decreto Legislativo Nº 957.

Incorporase el literal o) en el numeral 2 del artículo 46 y el literal 8) en el artículo 196-A del Código Penal aprobado en el Decreto Legislativo Nº 957, los mismos que quedarán redactados de la siguiente manera:

"Artículo 46. Circunstancias de atenuación y agravación
(...)

2. *Constituyen circunstancias agravantes, siempre que no estén previstas específicamente para sancionar el delito y no sean elementos constitutivos del hecho punible, las siguientes:*

(...)
o) Cuando para la realización de la conducta punible se emplee la inteligencia artificial."

"**Artículo 196-A.- Estafa agravada**
La pena será privativa de libertad no menor de cuatro ni mayor de ocho años y con noventa a doscientos días-multa, cuando la estafa:

(...)

8. Se lleve a cabo mediante el empleo de la inteligencia artificial o tecnologías similares".

Artículo 2. Incorporación del numeral 5 en el artículo 11 de la Ley 30096 Ley de Delitos Informáticos

Incorpórese el numeral 5 en el artículo 11 en el artículo 11 de la Ley 30096 Ley de Delitos Informáticos, en los siguientes términos:

Artículo 11. Agravantes

El juez aumenta la pena privativa de libertad hasta en un tercio por encima del máximo legal fijado para cualquiera de los delitos previstos en la presente Ley cuando:

(...)
5. *El agente para cometer el delito emplea la inteligencia artificial o tecnologías similares".*

Artículo 2. Modificación del artículo 219, del Código Penal aprobado en el Decreto Legislativo Nº 957.

Modificase el artículo 219, del Código Penal, los mismos que quedarán redactados de la siguiente manera:

Artículo 219.- Plagio
Será reprimido con pena privativa de libertad no menor de cuatro ni mayor de ocho años y noventa a ciento ochenta días multa, el que, con respecto a una obra, la difunda como propia, en todo o en parte, copiándola o reproduciéndola textualmente, o tratando de disimular la copia mediante ciertas alteraciones, atribuyéndose o atribuyendo a otro, la autoría o titularidad ajena.

El plagio será reprimido con pena privativa de libertad no menor de seis ni mayor de diez cuando se programe o utilice la inteligencia artificial o tecnología análoga.

FIRMA DIGITAL
Firmado digitalmente por: ARRIOLA TUEROS JOSE ALBERTO FIR 25542661 hard
Motivo: En señal de conformidad
Fecha: 04/12/2023 14:23:20-0500

FIRMA DIGITAL
Firmado digitalmente por: ALVA PRIETO Maria Del Carmen FAU 20161749126 soft
Motivo: Soy el autor del documento
Fecha: 29/11/2023 17:27:09-0500

María del Carmen Alva Prieto
Congresista de la República del Perú

FIRMA DIGITAL
Firmado digitalmente por: MORI CELIS Juan Carlos FAU 20161749126 soft
Motivo: En señal de conformidad
Fecha: 01/12/2023 17:04:38-0500

FIRMA DIGITAL
Firmado digitalmente por: PAREDES FONSECA Karol Ivett FAU 20161749126 soft
Motivo: Doy V° B°
Fecha: 30/11/2023 10:46:57-0500

FIRMA DIGITAL
Firmado digitalmente por: MONTEZA FACHO Silvia Maria FAU 20161749126 soft
Motivo: En señal de conformidad
Fecha: 29/11/2023 17:51:38-0500

CONGRESO DE LA REPÚBLICA

Lima, **05** de **diciembre** de **2023**

Según la consulta realizada, de conformidad con el Artículo 77° del Reglamento del Congreso de la República: pase la Proposición N° **6573/2023 CR** para su estudio y dictamen, a la (s) Comisión (es) de

1. JUSTICIA Y DERECHOS HUMANOS.

GIOVANNI FORNO FLOREZ
Oficial Mayor
CONGRESO DE LA REPÚBLICA

EXPOSICIÓN DE MOTIVOS

I. FUNDAMENTACIÓN

La inteligencia artificial IA, viene presentando un crecimiento vertiginoso en los últimos años, gracias al aumento en la capacidad de procesamiento de datos y al desarrollo de algoritmos más complejos; lo que ha dado lugar a nuevas aplicaciones de la IA en áreas como la medicina, la robótica y la seguridad, entre otras.

Varios países han implementado o están en proceso de implementar leyes y regulaciones relacionadas con la inteligencia artificial, las mismas que varían en alcance y detalle, pero generalmente se centran en cuestiones como la ética, la privacidad, la seguridad y la responsabilidad de la Inteligencia Artificial. Entre los ejemplos que podemos citar son:

a) La Unión Europea (UE) ha propuesto regulaciones que buscan abordar cuestiones como la transparencia y la responsabilidad de los sistemas de inteligencia artificial, especialmente aquellos utilizados en sectores críticos como la salud y el transporte.

b) Estados Unidos, ha propuesto y discutido diversas iniciativas a nivel estatal y federal para abordar cuestiones de inteligencia artificial, incluida la privacidad de los datos y la responsabilidad de los algoritmos.

c) En China se ha establecido directrices y regulaciones sobre el uso de la inteligencia artificial en diversas industrias, y está trabajando en marcos legales más amplios para abordar la seguridad y la ética de la inteligencia artificial.

d) Canadá tiene un papel de liderazgo en esta importante área tecnológica y ha publicado directrices éticas sobre inteligencia artificial y está trabajando en regulaciones más amplias para la inteligencia artificial, con un enfoque en la transparencia y la responsabilidad.

"Asimismo, en 2021, Armenia, Bahréin, Cuba, Islandia, Marruecos, Nueva Zelanda y Omán se encontraban en proceso de desarrollo de una estrategia nacional de IA, mientras que en 2022 se sumaron Azerbaiyán, Bélgica, Benín, Israel, Jordania, Nigeria y Uzbekistán." (HAI Stanford University, citado por Christine Weidenslaufer y Raimundo Roberts pág.8, 2023)".[1]

.

"Según un informe de la OCDE de 2021, los países se encuentran en diferentes etapas de desarrollo e implementación de las estrategias y políticas nacionales de IA (Galindo et al, citado por Christine Weidenslaufer y Raimundo Roberts

---

[1] HAI Stanford University (2023:23), citado por Christine Weidenslaufer y Raimundo Roberts (Junio 2023) Regulación de la IA en la experiencia comparada Unión Europea y Estados Unidos, disponible en https://www.bcn.cl/obtienearchivo?id=repositorio/10221/34367/2/BCN_regulacion_global_IA_2023_CW_RRrr_2.pdf

pág.8, 2023)"[2]. *"Asimismo, éstas tienen diversos y a veces coincidentes enfoques y énfasis. Por ejemplo, mientras las estrategias nacionales de Alemania y de la Comisión Europea se enfocan en el establecimiento de centros de investigación y desarrollo, en Finlandia y Canadá el enfoque está en la aplicación de la IA en el sector público. En Dinamarca se destaca la importancia de la tecnología lingüística de alta calidad para respaldar el desarrollo y la implementación de la IA en danés, en Japón se promueve el desarrollo de infraestructura digital para la IA (A modo de ejemplo, ese país tiene una de las super computadoras más potentes del mundo, llamada Fugaku, diseñada para desarrollar simulaciones que combinan IA y Big Data), en Alemania y Colombia se diseñan y establecen entornos controlados para la experimentación con IA (sandboxes), y en Reino Unido se propone asesoramiento personalizado para apoyar el crecimiento de las empresas, entre otros aspectos relevantes. ((Galindo et al, citado por Christine Weidenslaufer y Raimundo Roberts pág.8, 2023)"* [3].

La regulación de la inteligencia artificial sigue siendo un campo en evolución, y es probable que veamos el desarrollo de nuevas normas en los próximos años a medida que la tecnología continúe avanzando y sobre todo teniendo en cuenta que la situación legal de la inteligencia artificial puede variar considerablemente de un país a otro.

Con el objeto de regular la Inteligencia Artificial, con fecha 25 de mayo del presente año el Pleno del Congreso aprobó la primera votación y la exoneración de la segunda votación de la Ley Nº 31814[4] "*Ley que promueve el uso de la inteligencia artificial en favor del desarrollo económico y social del país*".

Esta norma entre otros aspectos, declara de interés nacional el fomento del desarrollo y uso de la inteligencia artificial para la mejora de los servicios públicos, de la educación y los aprendizajes, la salud, la justicia, la seguridad ciudadana, la seguridad digital, la economía, la inclusión, los programas sociales, la seguridad y la defensa nacional, así como para toda otra actividad económica y social a nivel nacional.

Entre las principales disposiciones que contiene la norma antes mencionada podemos resaltar que:

---

[2] Galindo et al (2021:16). citado por Christine Weidenslaufer y Raimundo Roberts (Junio 2023) Regulación de la IA en la experiencia comparada Unión Europea y Estados Unidos, disponible en https://www.bcn.cl/obtienearchivo?id=repositorio/10221/34367/2/BCN_regulacion_global_IA_2023_CW_RRrr_2.pdf

[3] Galindo et al (2021:16 y ss.) citado por Christine Weidenslaufer y Raimundo Roberts (Junio 2023) Regulación de la IA en la experiencia comparada Unión Europea y Estados Unidos, disponible en https://www.bcn.cl/obtienearchivo?id=repositorio/10221/34367/2/BCN_regulacion_global_IA_2023_CW_RRrr_2.pdf

[4] Ley Nº 31814, disponible en https://www.gob.pe/institucion/congreso-de-la-republica/normas-legales/4565760-31814

- Tiene como objetivo incentivar el uso de la inteligencia artificial en el marco del proceso nacional de transformación digital, buscando el desarrollo a nivel económico y social del país, priorizando a la persona y promoviendo un uso sostenible, ético y responsable.

- Para el uso y desarrollo de la inteligencia artificial, se han establecido 6 principios: Estándares de seguridad basados en riesgos, enfoque de pluralidad de participantes, gobernanza de internet, sociedad digital, desarrollo ético para una inteligencia artificial responsable y privacidad de la inteligencia artificial.

- Se definen los conceptos de: Inteligencia Artificial, Sistema basado en inteligencia artificial, Tecnologías emergentes y Algoritmo.

- El Sistema Nacional de Transformación Digital es la autoridad técnico-normativa responsable de dirigir, evaluar y supervisar el uso y la promoción del desarrollo de la inteligencia artificial y las tecnologías emergentes.

- La Secretaría de Gobierno y Transformación Digital de la Presidencia del Consejo de ministros es el ente rector del Sistema Nacional de Transformación Digital.

- La Autoridad Nacional deberá promover e impulsar el desarrollo de la inteligencia artificial, formación de profesionales con competencias para aprovechar la inteligencia artificial en el país, crear y fortalecer la estructura digital como habilitadora para el desarrollo de la inteligencia artificial, entre otras acciones. Asimismo, deberá remitir un informe anual al Congreso de la República sobre los avances en la implementación de la Política Nacional de Transformación Digital y la Estrategia Nacional de inteligencia artificial.

Es preciso resaltar que la Ley esta Ley 31814 Ley que promueve el uso de la inteligencia artificial en favor del desarrollo económico y social del país, contiene pautas generales y traza el camino para nuevos dispositivos legales que regulen el uso y aprovechamiento de la inteligencia artificial. Si bien la mencionada Ley entró en vigencia el 6 de julio del presente año esta debe ser reglamentada por el Poder Ejecutivo en el plazo de 90 días hábiles, el cual aún no ha vencido.

Otro aspecto, a resaltar es que el Poder Ejecutivo ha propuesto la Estrategia Nacional de Inteligencia Artificial para el periodo 2021-2026[5], con la finalidad de situar al país como líder en investigación, desarrollo, aplicación y promoción de Inteligencia Artificial a nivel educativo, científico, estatal y ciudadano.

Es importante tener en cuenta que la inteligencia artificial no es solo una tecnología, sino una herramienta que debemos aprovechar y moldear con

[5] Estrategia Nacional de Inteligencia Artificial para el periodo 2021-2026, disponible en https://cdn.www.gob.pe/uploads/document/file/1899077/Estrategia%20Nacional%20de%20Inteligencia%20Artificial.pdf?v=1630689418

sabiduría y visión; no obstante, es necesario controlar sus excesos y aprobar reglas para su uso en la vida cotidiana.

Por ello es necesario preguntarnos si la inteligencia artificial puede emplearse para actos delictivos y sobre todo si en la actualidad se encuentra normada la responsabilidad penal en el uso de esta. Que sucedería si alguien desarrolla un sistema de inteligencia artificial diseñado para asesinar, o si la IA se emplea para realizar lavado de activos o se desarrolla programas para suplantar voces e identidades por medio de Inteligencia artificial y se emplea para estafar.

"*Por ejemplo, en Arizona, Estados Unidos, la Inteligencia Artificial (IA) llegó a límites inesperados, hasta el punto en que fue utilizada para cometer delitos como fraudes. Eso fue lo que le ocurrió a una mujer llamada Jennifer De Stefano, quien afirmó que estafadores utilizaron esa tecnología para clonar de forma exacta la voz de su hija adolescente y simular un secuestro, para posteriormente exigir un rescate de una alta cifra de dinero. Diario Chileno La Tercera)*"[6].

"*Para expertos en esta área como Subbarao Kambhampati, académico de informática en la Universidad Estatal de Arizona y que también ha estudiado de cerca las aristas de la IA, la clonación de voz está avanzando a niveles cada vez más perfeccionados. A diferencia de como ocurría en el pasado, ahora solo basta una muestra mínima para conseguir clonar una voz, advirtió Kambhampati. (Diario Chileno La Tercera)*" [7].

Conforme al hecho citado anteriormente, se suplantó la identidad y simularon un secuestro, utilizando voces dirigidas por Inteligencia artificial, lo que demuestra el mal uso de la IA, lo que constituye un riesgo latente.

"A continuación citaremos lo que refiere el estudio, publicado en Crime Science y financiado por el Centro Dawes para el Crimen Futuro de la UCL elaborado por científicos del University College de Londres (UCL) (disponible como informe de políticas):

El referido estudio, identificó 20 formas en que la IA podría usarse para facilitar el crimen en los próximos 15 años. Estos se clasificaron en orden de preocupación: en función del daño que podrían causar, el potencial de obtener ganancias o beneficios delictivos, lo fácil que sería ejecutarlos y lo difícil que sería detenerlos.

Los investigadores recopilaron los 20 crímenes permitidos por la IA a partir de artículos académicos, noticias e informes de actualidad, ficción y cultura popular.

(...)

---

[6] La tercera Diario Chileno, disponible en https://www.latercera.com/tendencias/noticia/mama-ayudame-inteligencia-artificial-imita-voz-de-adolescente-para-fingir-secuestro-y-exigir-rescate/XTQEUXTJZJH5BJJXHRJX7QID4E/

[7] Idem

Los delitos de mediana preocupación incluían la venta de artículos y servicios fraudulentamente etiquetados como "IA", como controles de seguridad y publicidad dirigida. Estos serían fáciles de lograr, con ganancias potencialmente grandes.

Los delitos de menor preocupación incluían los robots ladrones (pequeños robots utilizados para entrar en propiedades a través de puntos de acceso como buzones o gateras) que se consideraban fáciles de derrotar; por ejemplo, mediante jaulas tipo buzón, y el acecho asistido por IA, que, aunque extremadamente dañino para las personas, no podría operar a escala.

A diferencia de muchos delitos tradicionales, los delitos en el ámbito digital pueden compartirse, repetirse e incluso venderse fácilmente, lo que permite comercializar técnicas delictivas y proporcionar el delito como un servicio. Esto significa que los delincuentes pueden subcontratar los aspectos más desafiantes de sus delitos basados en IA". [8]

Como se puede apreciar de lo antes señalado, la IA a abierto las puertas a la comisión de nuevas figuras delictivas que requieren necesariamente ser reguladas su uso y sobre todo el mal uso que los individuos podrían realizar de la misma.

A continuación, se enumeran los 20 delitos más peligrosos que se pueden dar consecuencia del uso de la inteligencia artificial en los próximos años, los cuales han sido señalado en el estudio antes mencionado y han sido colocados de menor a mayor gravedad; cabe señalar, que esta información se ha considerado oportuno recogerse a efecto de sustentar la necesidad de las incorporaciones no solo en el Código Penal, sino también en la Ley de Delitos Informáticos.

"Falsificación de contenido
Evento en el que se presentan partes de la décima sinfonía inconclusa de Ludwig van Beethoven que buscan completarse utilizando inteligencia artificial antes del 250 aniversario del nacimiento de Beethoven en Bonn, Alemania, el 13 de diciembre de 2019.

La amenaza menos preocupante que generará la IA en los próximos años será la creación de contenido falso en ámbitos como el arte o la música que pueda ser posteriormente vendido bajo falsas pretensiones en cuanto a su autoría. Este delito ocupa el puesto más bajo de la lista en cuanto a los daños que puede ocasionar, así como por sus probabilidades de éxito.

Como detalla el informe, si bien la inteligencia artificial ha mostrado capacidades para emular el estilo visual de creadores como grandes pintores, esta podría verse ampliamente limitada a la hora de abordar la creación de un objeto físico real. Por otro lado, las casas de subastas, galerías y especialistas llevan siglos luchando contra las falsificaciones,

---

[8] Noticias de la UCL, disponible en: https://www.ucl.ac.uk/news/2020/aug/deepfakes-ranked-most-serious-ai-crime-threat

por lo que es un campo en el que cabe esperar que cuenten con prácticas defensivas adecuadas.

Acoso ayudado por inteligencia artificial
Por tal debe entenderse el uso de sistemas de aprendizaje capaces de monitorizar la actividad y la ubicación de un individuo a través de las redes sociales o los datos disponibles en sus dispositivos móviles.

Asimismo, el estudio también engloba aquí la provisión por parte de tecnológicas de aplicaciones capaces de hacer cumplir las normas sociales en sociedades represivas.

Si bien estos delitos pueden ser realmente dañinos, el informe considera que al tratarse de acciones sobre individuos no supondrían un alcance significativo a gran escala.

Reseñas falsas creadas por IA
Esta capacidad de generar de manera automática reseñas falsas podría utilizarse en espacios muy basados en la opinión de los usuarios, como Amazon o TripAdvisor, para ofrecer falsas impresiones sobre un producto con la intención de promoverlo o alejarlo del interés de los clientes.

Una práctica deshonesta que hoy en día ya es realizada por actores humanos.

Tecnología para eludir la detección de la inteligencia artificial
Un policía español investigando un caso de pornografía infantil en 2006.

A medida que los asuntos policiales y de seguridad vayan dependiendo más de la inteligencia artificial y la automatización de los datos en los procesos de investigación, cabe esperar que aumenten los ataques en los que se busque eludir esta tecnología frustrando posibles descubrimientos o incluso que permitan el borrado de pruebas.

Bots ladrones
El desarrollo de la tecnología puede permitir la creación de pequeños robots autónomos capaces de introducirse en casas y otras instalaciones por espacios como buzones para recuperar llaves o abrir puertas y permitir que ladrones humanos entren para llevar a cabo un robo.

El estudio lo cataloga como un delito de baja amenaza ya que se trataría de robos a muy pequeña escala y que podrían detenerse fácilmente a través de dispositivos que impidan la entrada del robot por el buzón.

Explotación de sesgos
Descubrir los sesgos aprendidos de algoritmos influyentes o muy utilizados podría llevar a aprovechar esto en beneficio de intereses concretos.

La investigación indica como ejemplos las clasificaciones de Google donde poder poner en desventaja a los competidores o las recomendaciones de YouTube encaminadas a impactar en los espectadores más idóneos. Algo que de manera no legal ya se pone en práctica a través de técnicas por ejemplo de SEO, pero que el desarrollo de la IA podría potenciar en extremo.

Alteraciones del mercado bursátil

En el puesto más bajo dentro de las amenazas de grado medio se encuentra la manipulación de los mercados financieros o bursátiles con el objetivo de dañar a competidores, divisas o hacer colapsar sistemas económicos en su totalidad.

Aunque los daños de este delito podrían ser realmente elevados, su rentabilidad es sin embargo considerada baja debido a la extrema dificultad que puede conllevar simular con precisión el comportamiento del mercado.

Engaño del reconocimiento facial

Un poster que simula la tecnología de reconocimiento facial durante una exhibición en China en 2018.

Los sistemas de reconocimiento facial a través de la IA son cada vez más utilizados. Desde hace tiempo son incluidos como medida de seguridad para el desbloqueo de dispositivos móviles e incluso comienzan a servir a la policía en los procesos de rastreo de sospechosos en espacios públicos.

Lo cual hace que estos sistemas puedan posicionarse en el futuro como objetivo atractivo para muchos delincuentes.

Delitos en actividades online

El auge de las actividades online en distintos aspectos de la vida actual, desde las finanzas a las relaciones sociales, presenta un nuevo objetivo en cuanto a los ataques hacia las personas: denegar este acceso en línea a ciertos servicios esenciales.

Lo cual podría utilizarse, según el informe, para dañar a ciertos usuarios o causar el caos.

Ataques con drones autónomos

Según el informe cabe esperar que los drones autónomos controlados por IA permitirán una mayor complejidad y coordinación de ataques y delitos perpetrados por este tipo de dispositivos, que además dificultan la detención del atacante.

Los drones pueden ser altamente peligrosos si se equipan con armamento y actúan en masa de "enjambres autoorganizados", remarca el estudio.

Ciberataques basados en aprendizaje

La IA en el futuro puede permitir que los ciberataques masificados sean cada vez más complejos y sofisticados sirviéndose del aprendizaje por refuerzo para poder analizar las debilidades de numerosos sistemas en paralelo antes de lanzar varios ataques de manera simultánea.

Manipulación de datos

Otro de los delitos de amenaza media detectados por el estudio es la manipulación deliberada de los datos utilizados para entrenar a una inteligencia artificial, con el objetivo de introducir de manera deliberada sesgos específicos.

En este aspecto, cuanto más utilizada y fiable sea la fuente de los datos más daño podrá causar posteriormente. Entre estos el estudio contempla desde sesgos orientados a dañar a un competidor hasta aquellos pensados para alterar un discurso político.

Venta de tecnología falsa bajo la apariencia de IA

Este delito se refiere a la venta de servicios o tecnologías fraudulentas que realmente no son capaces de cumplir los objetivos para los que han sido diseñados, todo ello enmascarado bajo la apariencia de IA.

El éxito de este fraude está directamente vinculado con las empresas u organismos gubernamentales a los que se dirigen estos estafadores, ya que es esencial que estas crean en las capacidades declaradas a dicha inteligencia artificial. Por lo que debería ser potencialmente fácil impedirlos.

Acceso fraudulento a robots militares

Cabe esperar que cualquier acceso por parte de organizaciones criminales a hardware militar represente una seria amenaza, especialmente si se trata de robots autónomos destinados a utilizarse como despliegue defensivo o en campos de batalla.

Por ello el informe cataloga este acceso criminal a robots armados militares como la mayor amenaza de grado medio.

Chantaje a gran escala

En el puesto más bajo de las amenazas de nivel más alto se encuentran los chantajes a gran escala.

Como identifica el informe, la IA puede permitir llevar a cabo extorsiones a mayo nivel, recopilando informaciones de redes sociales o grandes conjuntos de datos personales de historiales de navegador, contenidos del disco duro o del propio móvil. También favorece la identificación de vulnerabilidades para una gran cantidad de objetivos e incluso elaborar mensajes personalizados de chantaje para cada una de las víctimas.

El estudio calificó esta amenaza de elevada en cuanto a las ganancias obtenidas, así como en la dificultad de detenerlo.

Interrupción de los sistemas controlados por IA

A medida que aumente el uso de la IA por parte de empresas, gobiernos y hogares, no solo estos sistemas se harán más esenciales, sino que cabe esperar un aumento del número de ataques que se dirigirán a ellos.

Desde el informe se señala a los sistemas vinculados con la seguridad y las transacciones financieras como los objetivos clave de estos delitos.

"En general, cuanto más complejo es un sistema de control, más difícil puede ser defenderlo por completo" asegura el estudio, subrayando la complejidad que supone poder frenar este tipo de fraudes.

Phishing adaptado

Los ataques de phishing buscan recabar información confidencial de un usuario o instalar un malware a través de mensajes falos de fuentes de confianza, como por ejemplo un banco. De esta forma se pueden conseguir por ejemplo contraseñas.

Hasta ahora estos ataques se hacen enviando mensajes genéricos a un gran número de potenciales víctimas, lo que suele conllevar tasas de éxito bajas.

Pero la IA ofrece el potencial de poder mejorar el éxito de estos ataques al poder generar mensajes que parezcan más reales, por ejemplo, incorporando información privada obtenida de redes sociales o utilizar el learning para entender qué mensajes funcionan mejor ante los usuarios en este tipo de fraudes.

Vehículos sin conductor utilizados como armas

Las organizaciones criminales y terroristas se han servido en numerosas ocasiones de vehículos para ser usados como armas (bien al cargarlos de explosivos o siendo dirigidos contra un objetivo, como es el caso de algunos de los últimos atentados recientes sufridos en Europa).

Estas capacidades terroristas podrían verse amplificadas, como señala el estudio, por el desarrollo de los coches con conducción autónoma al reducir la necesidad de conductores. No solo eso. Esta tecnología permitiría a su vez realizar múltiples ataques al coordinar varios vehículos al mismo tiempo.

Ante esto es de esperar que a medida que se avanza en la conducción autónoma estos coches incorporen sistemas de seguridad destinados a imposibilitar este tipo de usos. Asimismo, derrotarlos podría ser posible con las mismas medidas que se utilizan con los vehículos actuales, como barreras físicas o restricciones de tráfico.

Deepfakes

Los deepfakes son vídeos falsos generados con inteligencia artificial que permiten cambiar el rostro de una persona para que parezca que hace o dice algo que no ha hecho o dicho. Algo que más allá de la broma puntual que pueda ocasionar, supone un riesgo preocupante para las democracias, que viene a sumarse a la generación de las fake news.

La suplantación de identidad por vídeo y audio podrían utilizarse para acceso de información y contraseñas para acceso a fondos económicos o en el caso de figuras públicas para manipular su apoyo a estas.

Todos los expertos inmersos en el estudio consideraron los deepfakes como el tipo de delito más preocupante de esta tecnología, obteniendo puntuaciones elevadas en las cuatro categorías de análisis". [9]

Otro aspecto relevante es el crecimiento de otras formas delictivas, las cuales se han generado a consecuencia de la virtualidad la cual fue impulsada por la pandemia, así se han ido perfeccionando nuevas prácticas criminales, el Reporte de Información estadística y recomendaciones para la prevención elaborado por el Ministerio de Justicia, en Agosto de 2022, señala que: (...) "*Lima encabeza la lista de los departamentos que registran la mayor cantidad de denuncias por ciberdelitos (delitos informáticos) durante los años 2019, 2020 y 2021. Llama especialmente la atención este crecimiento sostenido de las denuncias por ciberdelitos durante los tres años en mención, y de forma especial, el crecimiento experimentado hacia el último año (2021), en el que aumentaron las denuncias en todos los territorios, pero especialmente en el departamento de Lima con un total de 7 mil 324 casos señalados ante las autoridades policiales. Así también, es importante volver a destacar el crecimiento de las denuncias a nivel nacional desde el 2020 hacia el 2021, en el que pasamos de 25% a 65% más denuncias por este tipo de ilícitos".* [10]

---

[9] Bussiness Inside, disponible en: https://www.businessinsider.es/delitos-peligrosos-creara-inteligencia-artificial-695577

[10] Reporte de información estadística y recomendaciones para la prevención elaborado por el Ministerio de Justicia, en Agosto de 2022, págs. 10 y 11, disponible en: https://cdn.www.gob.pe/uploads/document/file/3562747/Reporte%20de%20Ciberdelincuencia.pdf.pdf

CUADRO 01 » Número de denuncias por delitos informáticos registrados en la PNP según departamento, 2019-2021

Lima	4,139	4,527	7,324
Arequipa	496	645	877
La Libertad	483	602	835
Callao	341	510	774
Lambayeque	306	466	719
Piura	223	325	576
Tacna	83	126	426
Ancash	193	285	405
Huánuco	80	232	358
Junín	58	162	338
Cusco	178	225	308
Ica	115	142	236
San Martín	31	73	189
Ucayali	47	85	187
Moquegua	56	83	184
Loreto	78	92	167
Puno	19	49	163
Ayacucho	36	42	142
Cajamarca	26	57	120
Amazonas	45	49	101
Apurímac	21	46	66
Pasco	9	34	62
Huancavelica	20	15	51
Tumbes	16	18	34
Madre de Dios	9	7	29
Total	7,108	8,897	14,671
Variación porcentual		25%	65%

Fuente: PNP, SIDPOL, información preliminar
Elaboración: Observatorio Nacional de Política Criminal INDAGA

Otro aspecto que recoge el reporte antes señalado es el referente a las modalidades durante el periodo 2019 – 2021, así se tiene que "de acuerdo con los registros de denuncias de la Policía Nacional, los delitos en torno a la comisión de fraude informático son los que más afectan a los ciudadanos y ciudadanas, los que han reunido un total de 6 mil 946 denuncias en el año 2020, llegando hasta 10 mil 924 para el siguiente año. En un segundo lugar, con un crecimiento que no pasa desapercibido, la modalidad de suplantación de identidad pasó de 935 denuncias en el 2020, hasta un total de 2 mil 666 denuncias para el 2021. (…) asimismo de 3 de cada 4 ciberdelitos en el Perú están relacionados a la comisión de fraudes informáticos para el año 2021 los delitos informáticos de acceso ilícito concentran gran parte de estos (386 de un total de 581). Seguidamente, están los atentados contra la integridad de datos informáticos (82) y finalmente los ataques a la integridad de sistemas informáticos (20). (…) sobre los casos de delitos cometidos contra los datos y sistemas informáticos, encontramos que estos también muestran un importante crecimiento, entre el 2019 y el 2020, presentando un aumento de hasta en 37%; mientras que del 2020 al 2021, incrementaron en 33%.(…) los delitos cometidos mediante el uso de estas tecnologías y/o espacios virtuales, afectando la intimidad y el secreto de las comunicaciones, existe un notable y sostenido aumento, pasando de 47 delitos en el año 2017 hasta 479 en el año 2021; siendo que entre el 2020 y el 2021, el aumento fue de hasta un 38.8%; aspecto que

llama especialmente la atención, teniendo en cuenta que en el año 2020 se registró un aumento del 200% de los casos en comparación con el año 2019"[11]

Como se puede apreciar el tema de la cibercriminalidad es un tema que va en aumento, lo cual va acompañado con el uso delicado que se viene dando a la IA, dado que como lo señala el profesor Shane Johnson, director del Centro Dawes para Crímenes Futuros de la UCL, que financió el estudio, dijo: "Vivimos en un mundo en constante cambio que crea nuevas oportunidades, buenas y malas. Como tal, es imperativo que anticipemos las futuras amenazas delictivas para que los formuladores de políticas y otras partes interesadas con competencia para actuar puedan hacerlo antes de que se produzcan nuevas "cosechas de delitos"[12].

De acuerdo a lo señalado existe una serie de futuras amenazas criminales asociadas con tecnologías nuevas y emergentes, por ello es que, consideramos necesario complementar el avance que en nuestro país se viene dando en cuanto a la regulación de la inteligencia artificial, teniendo en cuenta que si bien la IA no tiene naturaleza humana dado que es una herramienta sobre la que no podría recaer responsabilidad penal; sin embargo, debería recaer en la persona que está tras esta, por utilizarla dolosamente para cometer un delito; motivo por el cual se ha planteado la presente propuesta legislativa, que busca abrir la discusión en la materia, para adaptar nuestro marco normativo a estos retos específicos.

En este sentido, esta iniciativa legislativa busca incorpora la inteligencia artificial como circunstancia agravante en el Código Penal, para lo cual se propone la incorporación del literal o) en el numeral 2 del artículo 46 y el literal 8) en el artículo 196-A del Código Penal aprobado en el Decreto Legislativo Nº 957.

Así en el numeral 2 del Artículo 46 del Código Penal se incorpora el literal o) por él que constituye circunstancia agravante, siempre que no estén previstas específicamente para sancionar el delito y no sean elementos constitutivos del hecho punible, cuando para la realización de la conducta punible se emplee la inteligencia artificial.

El Código Penal peruano establece diversas circunstancias agravantes que pueden aumentar las penas impuestas a los infractores de la ley. Las circunstancias agravantes se utilizan para aumentar la pena en función de la gravedad de la conducta delictiva y la culpabilidad del infractor. Cada caso se evalúa de manera individual para determinar si estas circunstancias son aplicables. Con la presente propuesta, se incluye una agravante más, teniendo en cuenta el mal manejo que se puede dar de la inteligencia artificial.

---

[11] Reporte de información estadística y recomendaciones para la prevención elaborado por el Ministerio de Justicia, en Agosto de 2022, págs. 10 y 11, disponible en: https://cdn.www.gob.pe/uploads/document/file/3562747/Reporte%20de%20Ciberdelincuencia.pdf.pdf

[12] https://noticiasdelaciencia.com/art/39043/los-deepfakes-son-considerados-la-amenaza-mas-peligrosa-de-la-inteligencia-artificial

Otra de las propuestas es incorporar el numeral 8 en el artículo 196-A. del código Penal es una causal más que se debe contemplar para el caso de la estafa agravada, así se propone que la pena será privativa de libertad no menor de cuatro ni mayor de ocho años y con noventa a doscientos días-multa, cuando la estafa: 8. Se lleve a cabo mediante el empleo de la inteligencia artificial o tecnologías similares.

La estafa agravada mediante inteligencia artificial es una forma específica de delito que involucra el uso de sistemas de inteligencia artificial para perpetrar una estafa o fraude. Este tipo de delito se considera agravado debido a la sofisticación y el alcance que la inteligencia artificial puede proporcionar a los estafadores. Algunos elementos que pueden considerarse en casos de estafa agravada mediante inteligencia artificial pueden incluir como se ha señalado anteriormente en el uso de algoritmos y sistemas de IA puede permitir que los estafadores creen engaños más sofisticados y convincentes, lo que aumenta la gravedad del delito, en el uso de IA para acceder o utilizar información privada de manera indebida puede ser considerado agravante, en la automatización a través de la IA puede permitir que se dirijan a un gran número de víctimas simultáneamente.

Por ello es importante que el Código Penal se adapte a medida que la tecnología evoluciona para abordar casos de estafa agravada mediante inteligencia artificial y garantizar que los estafadores sean responsables de sus acciones.

Por lo tanto, es fundamental que la legislación se adapte para abordar las nuevas formas de delitos relacionados con la tecnología y la inteligencia artificial, y que se asegure que los infractores sean responsables de sus acciones, por lo que se propone esta iniciativa legislativa para combatir este tipo de fraude tecnológico.

Asimismo, se propone incorporar el numeral 5 en el Artículo 11 de la Ley 30096 Ley de Delitos Informáticos, a efecto de establecer un agravante para el caso de los delitos informáticos, si estos se realizan empleando la inteligencia artificial o tecnologías similares.

Y por último la propuesta es la modificación del artículo 219, del Código Penal, a efecto de establecer como un agravante para la figura delictiva en el Plagio cuando se programe o utilice la inteligencia artificial o tecnología análoga.

El plagio a través de la inteligencia artificial es una preocupación creciente en el ámbito académico y editorial. La inteligencia artificial puede utilizarse para generar contenido de manera automática, lo que puede incluir la copia no autorizada de material existente, por lo que resulta necesario regular este aspecto también.

II. EFECTO DE LA VIGENCIA DE LA NORMA SOBRE LA LEGISLACIÓN NACIONAL

La presente propuesta legislativa propone incorporar el literal o) en el numeral 2 del artículo 46 y el literal 8) en el artículo 196-A del Código Penal aprobado en el Decreto Legislativo Nº 957. Así como la incorporación del numeral 5 en el artículo 11 de la Ley 30096 Ley de Delitos Informáticos y por último la modificación del artículo 219, del Código Penal aprobado en el Decreto Legislativo Nº 957.

Esta iniciativa busca incorporar la inteligencia artificial como circunstancia agravante en el Código Penal peruano e incluirlo en los delitos de y plagio como un agravante.

III. ANÁLISIS COSTO – BENEFICIO

La propuesta legislativa tiene como finalidad incorporar la inteligencia artificial como un agravante en la comisión de los delitos. En cuanto a los beneficios de la presente iniciativa, a continuación, se detallan los impactos que se generarían con la promoción e implementación de dicho proyecto de Ley.

- Se busca promover el uso adecuado de la inteligencia artificial

- Se busca prioriza, la seguridad de los datos a ser utilizados por personas naturales, jurídicas e instituciones u organismos públicos y privados por medio de la tecnología, cuando se trate de utilización y procesamiento de cálculos o bases de datos en operaciones de ámbito público o público privado.

- Establecer medios disuasivos respecto al mal uso de la inteligencia artificial, cuando esta se destina a la comisión de delitos de diversa índole, que afectan los derechos de las personas.

- Se busca impulsar la seguridad, la confianza, la conectividad digital, así como el aprovechamiento de las tecnologías emergentes en favor del bienestar social y económico de la ciudadanía.

- Se busca impulsar la construcción de certezas regulatorias sobre estos sistemas, que permita su desarrollo, respetando los derechos fundamentales de acuerdo con la Constitución y las leyes.

- Se busca combatir el uso inapropiado de la IA que puede perjudicar a grupos vulnerables.

- Se busca proteger los derechos de las personas, en razón a que el mal manejo de la IA puede infringir estos y justificar la consideración de un delito.

En resumen, el mal manejo de la inteligencia artificial puede tener consecuencias negativas significativas, y la consideración de tales acciones como delitos puede

ayudar a mantener la responsabilidad y la integridad en el desarrollo y uso de la IA, por lo que es importante que se regule este aspecto.

IV. VINCULACIÓN CON EL ACUERDO NACIONAL Y LA AGENDA LEGISLATIVA

La iniciativa legislativa se enmarca en varias políticas del Acuerdo Nacional y de la Agenda legislativa para el período anual de sesiones 2023-2024 de manera especial con:

La 35va política de Estado expresada en el Acuerdo Nacional y en la Agenda Legislativa, denominada "Sociedad de la información y sociedad del conocimiento", referida a impulsar una sociedad de la información hacia una sociedad del conocimiento orientada al desarrollo humano integral y sostenible, en base al ejercicio pleno de las libertades y derechos de las personas.

Así también, con 12va política de Estado, referida a la promoción al acceso universal al conocimiento a través de las Tecnologías de la Información y Comunicación (TIC).

Asimismo, se vincula con la 9na política de Estado, denominada Política de Seguridad Nacional.

La norma se relaciona igualmente con la décimo octava política de Estado expresada en el Acuerdo Nacional y en la Agenda Legislativa, denominada: "Búsqueda de la competitividad, productividad y formalización de la actividad económica", en lo referido al punto (i) fomentará la investigación, creación, adaptación y transferencia tecnológica y científica.

La propuesta encuentra vinculación igualmente con la vigésima política de Estado expresada en el Acuerdo Nacional y en la Agenda Legislativa, denominada: "Desarrollo de la ciencia y la tecnología", en donde se señala fortalecer la capacidad de/ país para generar y utilizar conocimientos científicos y tecnológicos.