



Revista IUS

ISSN: 1870-2147

Instituto de Ciencias Jurídicas de Puebla, Departamento de Investigaciones

Morán Espinosa, Alejandra
Responsabilidad penal de la Inteligencia Artificial (IA). *¿La próxima frontera?*
Revista IUS, vol. 15, núm. 48, 2021, Julio, pp. 289-323
Instituto de Ciencias Jurídicas de Puebla, Departamento de Investigaciones

DOI: <https://doi.org/10.35487/rius.v15i48.2021.706>

Disponible en: <https://www.redalyc.org/articulo.oa?id=293270311013>

- Cómo citar el artículo
- Número completo
- Más información del artículo
- Página de la revista en redalyc.org

Responsabilidad penal de la Inteligencia Artificial (IA). ¿La próxima frontera?*

Criminal Responsibility of Artificial Intelligence (AI). The next frontier?

Alejandra Morán Espinosa**

RESUMEN

La Inteligencia Artificial (IA) como la más reciente e impactante herramienta tecnológica, capaz de aprender y decidir, es probable que actualmente pueda cometer delitos -del tipo informático o ciberdelitos-, sumándose a los sujetos activos del delito y dejando de ser solo una herramienta más, cuya efectividad informática y decisiva, ocultaría el ataque, al atacante o a la herramienta (IA),*** lo que invita a analizar y ponderar los elementos fácticos actuales, para proponer su regulación especial a través de dos vertientes principales: 1. La creación de un tercer tipo de persona jurídica - "la persona artificial"-, y 2. La probable responsabilidad penal (IA) -frente a irresolvibles y variados casos cometidos por ésta-, y dada la ausencia de precedentes regulatorios nacionales, permite inducir claramente como la próxima, apremiante y urgente frontera jurídica a regular.

PALABRAS CLAVE

Inteligencia artificial (IA), robots, TIC, ciberdelitos, persona artificial.

ABSTRACT

Artificial Intelligence (AI) as the most recent and impressive technological tool, capable of learning and deciding, it is likely that currently it can commit crimes -of the computer type or cybercrimes-, joining the active subjects of crime and ceasing to be just a tool. Furthermore, whose computing and decisive effectiveness would hide the attack, from the attacker or the tool (AI)1, which invites us to analyze and weigh the current factual elements, to propose its special regulation through two main aspects: 1. The creation of a third type of legal person - "the artificial person" -, and 2. The probable criminal responsibility of the latter (IA) - in the face of unresolvable and varied cases committed by it -, and given the absence of regulatory precedents, allows us to clearly induce how the next, pressing and urgent legal border to regulate.

KEYWORDS

Artificial intelligence (AI), robots, information and communication technologies, cybercrime, artificial person.

*Artículo de Reflexión postulado el 19 de febrero de 2020 y aceptado el 1º de octubre de 2020

**Profesora investigadora en la Facultad de Estudios Superiores Acatlán de la Universidad Nacional Autónoma de México. (amoran@unam.mx) orcid.org/0000-0002-4315-0928

***Denoticias "Inteligencia artificial revienta el fraude del crimen en Silicon Valley", nota informativa en línea (febrero 9 de 2020), España [Consultada en febrero 10 del 2020], Disponible en: <https://www.denoticias.es/notas/inteligencia-artificial-revienta-el-fraude-del-crimen-en-silicon-valley.html>

“El día que la inteligencia artificial se desarrolle por completo podría significar el fin de la raza humana. Funcionará por sí sola y se rediseñará cada vez más rápido. Los seres humanos, limitados por la lenta evolución biológica, no podrán competir con ella y serán superados”. Stephen Hawking

Se dice que las fronteras están agotadas que han sido completamente abordadas por el hombre, no se espera descubrir nada más, ello es incorrecto algunos escenarios y fronteras aún no se agotan, como el espacio sideral¹ y otros se han creado recientemente, como el internet, con ello se renuevan las posibilidades de descubrir y explorar escenarios nuevos. Uno de ellos es precisamente el potencial y aplicaciones de la conocida como inteligencia artificial (IA), definición propuesta por Marvin Minsky (pionero) que dijo: “La inteligencia artificial es la ciencia de construir máquinas para que hagan cosas que, si las hicieran los humanos, requerirían inteligencia”,² o como dijo Rouse en 2017: “La inteligencia artificial es aquella inteligencia que se manifiesta a través de las maquinas, ... la ayuda idónea para cualquier ser humano, un agente racional, flexible y servicial...”³ Convirtiéndose así la IA en una herramienta producto de la evolución tecnológica cuyos primeros antecedentes⁴ se identifican a partir de los años 50 –entre ellos con Alan Turing⁵-. Encontrándola actualmente en todo tipo de escenarios, cuya razón de estudio es precisamente su potencial de desarrollo para emular de forma casi perfecta las actividades humanas -*incluso las criminales*-, incluyendo algunas tan especializadas que ni el ser humano puede realizar; como sucedió en 2019 con el minúsculo robot del Boston

¹ Y no estoy segura de que ahí no se cometan delitos o ciberdelitos, véase: DW “NASA investiga primer posible delito cometido en el espacio”, nota informativa en línea, (agosto 25 del 2019), [Consultada en diciembre 28 del 2019]. Disponible en: <https://www.dw.com/es/nasa-investiga-primer-possible-delito-cometido-en-el-espacio/a-501566162maca=es-Facebook-sharing>

² Minsky, Marvin definición de “Inteligencia artificial”, en Escolano Ruiz, Francisco, Cazorla Quevedo, Miguel A. y otros “Inteligencia Artificial: Modelos técnicas y áreas de aplicación”, edición digital (2003), Ed. Thomson [Consultado en noviembre 9 del 2019], Disponible en: https://books.google.com.mx/books?hl=es&lr=&tid=_spC6S7UfZg-C&oi=fnd&tpg=PP1&dq=tipos+de+inteligencia+artificial&tots=sPmnKDNuBU&sig=URMtRML1QfTLD4Pt9AqylzPJCE#v=onepage&q=tipos%20de%20inteligencia%20artificial&f=false

³ Rouse Margaret. “Inteligencia artificial o AI”, (en línea), TechTarget, (abril 2017), [Consultado en enero 3 del 2020], Disponible en: <https://searchdatacenter.techtarget.com/es/definicion/Inteligencia-artificial-o-AI>,

⁴ Sin embargo, en la mitología griega se sabe que “Talos”, era un mítico autómata gigante con inteligencia artificial, lo que demuestra que la idea de una inteligencia superior creada por el hombre no es tan reciente como parece.

⁵ Sus trabajos en IA son muy reconocidos, con importantes aportes, al ser matemático, lógico, científico de la computación, criptógrafo y filósofo, considerado como uno de los padres de la computación, además de precursor de la informática actual y los conceptos de algoritmo y computación.

Children's Hospital que navegó dentro de un cerdo y reparó una falla cardiaca.⁶ Tal circunstancia es donde nace el problema de estudio dado que la imitación de un ser humano es la pretensión de emular a un ser imperfecto naturalmente, donde hacerlo con una máquina que teóricamente es perfecta y que *¡realizará perfectamente las funciones de un ser imperfecto!* se convierte en toda una locura⁷ y considerando que en esa emulación de todo tipo de conductas, existe una muy alta probabilidad de que se encuentran incluidas conductas lesivas, indeseadas o delictivas, entonces es necesario regularla jurídicamente y esa es la meta de análisis, aportar razones de hecho y de derecho para ponderar la propuesta de su regulación jurídica en México.

En los aspectos metodológicos, este estudio es una investigación teórico-descriptiva de fuentes cualitativas, basada en un método correlacional, que permite inducir la posibilidad jurídica de normar el reconocimiento de la responsabilidad penal de una Inteligencia Artificial (IA) en México. Investigación de tipo explorativo, descriptivo y explicativo, donde se seleccionaron los referentes teóricos y mediáticos confiables y de mayor actualidad disponibles para acceso público y abierto; sintetizando los conocimientos fragmentados y sumando la propia experiencia profesional de los últimos 15 años allegada a dicho campo. Seleccioné a la IA como objeto de estudio jurídico -evitando su conceptualización tradicional de herramienta tecnológica para la comisión de un delito o como el objetivo de éste-, para lo cual consideré los siguientes objetivos de estudio: 1) Definir el tema de estudio para contribuir a la generación de investigación científica y al análisis de nuevos conocimientos jurídicos relacionados con los delitos informáticos, 2) Explicar el aprendizaje autónomo de la IA -*maching learning-* potencial, usos y casos, para contribuir al estudio de sus precedentes; 3) Proponer el reconocimiento de la IA -*del tipo maching learning-* como una tercera persona jurídica denominada "persona artificial", para facilitar la determinación de su responsabilidad penal ante la comisión de delitos que realice y 4) Establecer la tendencia actual en la comisión de delitos cometidos por IA, para identificar nuevas líneas de investigación jurídica y contribuir a la cultura de la legalidad y de la seguridad de la información, ante:

⁶ Olivares Joaquín. "Mi cirujano, el Dr. Robot". The Conversation, Academic rigor, journalistic flair. Artículo digital, enero 29 del 2020. [Consultada en: 31 de enero del 2010], Disponible en: <https://theconversation.com/mi-cirujano-el-dr-robot-130812>

⁷ N. de A. Un breve acercamiento a los principales pasos de desarrollo de la IA en: Mora Castro José Luis. "La evolución de la Inteligencia Artificial", 2016. Revista digital Mundo Contact, [Consultada en noviembre 7 del 2019], Disponible en: <https://mundocontact.com/la-evolucion-de-la-inteligencia-artificial/>

a) Nuevos escenarios jurídicos, b) Existencia de innumerables conductas atípicas y c) Inexistente responsabilidad penal del atacante artificial.

Se ha centrado el planteamiento del problema al considerar que la posibilidad de aprendizaje autónomo y toma de decisiones probablemente facilitarían que una IA decida y aplique sus capacidades y potencial, a la comisión de conductas delictivas, que ante un escenario informático en el que la IA ha evolucionado, se encontrarían dirigidas probablemente a cometer particularmente conductas delictivas relacionadas con los delitos informáticos, realizándolas a la perfección, incluso mejor que el ser humano. La hipótesis quedó determinada de la siguiente forma: “La inteligencia artificial (IA) del tipo *machine learning*, es condición necesaria para emular las capacidades mentales y actividades humanas⁸ diversas, incluyendo la comisión de delitos; por tanto, constituye el único tipo de tecnología que requerirá una regulación jurídica especial que determine su responsabilidad penal.”

Dentro de los resultados obtenidos se encuentran hallazgos muy interesantes, comenzando por el elemento fundamental, a qué nos referimos cuando hablamos de “Inteligencia”. Ésta debe considerarse como la capacidad de un sujeto que en la vida cotidiana dirige su comportamiento usando la información captada, aprendida, elaborada o producida por él mismo.⁹ En el contexto de estudio, comprende diversos elementos entre los que se encuentran: adquisición, representación y almacenamiento del conocimiento; generación y aprendizaje del comportamiento; desarrollo y uso de motivaciones y emociones; definición de prioridades; adquisición, representación y almacenamiento del conocimiento; generación y aprendizaje de comportamiento; transformación de señales sensoriales en símbolos -su manipulación para razonar el pasado y planificar el futuro-; así como fenómenos de ilusión, creencias, esperanzas, temores, sueños, cariño y amor. Con lo anterior se reconoce fácilmente su importancia e impacto en la toma de decisiones y por supuesto, emularla suena realmente emocionante y aventurado, considerando que ya sucede hace varios años en un nivel importante a través de la IA, se visualiza peligroso si se piensa en los aspectos negativos de esa misma “inteligencia” humana.

En ese orden de ideas y conscientes de la incuestionable existencia de la IA, se identificaron diversas clasificaciones:

- La IA es fuerte o débil.

⁸ -P.e.: razonamiento, comprensión, imaginación, reconocimiento, creatividad, emociones y toma de decisiones, entre otras.

⁹ Marina José Antonio. "La inteligencia fracasada", Edición impresa, Ed. Anagrama, (2016), ISBN: 978-84-339-7805-9. 176 p.p.

- Se integra por cuatro tipos fundamentales: reactiva, limitada, de teorías mentales y de autoconciencia.
- Existen otros, como los cuatro señalados por Daniel Martínez, que indica son formas particulares de expresión, que de no cumplir con alguno de los criterios, no puede considerarse como IA; entre estos se encuentran:
 - a) *IA Asistida*: colabora en las tareas para realizarlas con rapidez.
 - b) *IA Automatizada*: realiza tareas cotidianas y excepcionales de forma automática, generalmente de apoyo administrativo en el sector empresarial (administración).
 - c) *IA Aumentada*: facilita la toma de decisiones, aprendiendo de la interacción realizada y los resultados obtenidos (sugerencias no solicitadas de navegadores y redes sociales p.e.)
 - d) *IA Autónoma*: su capacidad es la toma de decisiones sin intervención humana (p.e. los vehículos autónomos).

En los tipos de IA existen diversas técnicas -*no todas relacionadas con el tema de fondo el presente estudio*-, entre ellas destacan las siguientes: Aprendizaje automático (-machine learning- analíticas de texto y NLP, siglas en inglés de procesamiento de lenguaje natural, utiliza las analíticas de texto para descifrar la estructura de enunciados, su significado, entonación y hasta la comprensión);¹⁰ Ingeniería del conocimiento (knowledge engineering); Lógica difusa (fuzzy logic); Redes neuronales artificiales (artificial neural networks); Sistemas reactivos (reactive systems); Sistemas multiagente (multi-agent systems); Sistemas basados en reglas (rule-based systems), Razonamiento basado en casos (case-based reasoning); Sistemas expertos (expert systems); Redes bayesianas (bayesian networks); Vida artificial (VA -no es un campo de la IA, sino que la IA es un campo de la VA-) (artificial life); Estrategias y computación evolutiva (evolutionary computation); Algoritmos genéticos (genetic algorithms) y Técnicas de representación de conocimiento y redes semánticas (semantic networks).¹¹ Relacionándose para este estudio, aquellas basadas en la capacidad

¹⁰ Martínez Marco, Daniel. "9 aplicaciones exitosas de la inteligencia artificial para el 2018", edición digital, Grupo extraordinaria (2017) [Consultado en noviembre 17 del 2019], Disponible en: <https://grupoextraordinaria.com/9-aplicaciones-inteligencia-artificial/> Este tipo de plataformas facilitan algoritmos, interfaces de programación, entrenamiento y análisis de big data "en vivo" o en tiempo real. Incluso existen de aprendizaje profundo que imita el funcionamiento neuronal del cerebro humano.

¹¹ Calderón, Grecia. "Inteligencia artificial". En Euston96, (en línea), (2019) [Consultada en noviembre 23 del 2019], Disponible en: <https://www.euston96.com/inteligencia-artificial/>

del sistema para realizar una tarea mediante el conocimiento previo o la capacidad de encontrar soluciones a una tarea desconocida:

Para explicar esta idea es necesario abundar en una clasificación particular, que es la que refiere las diferencias existentes entre los niveles de aprendizaje de la IA, que es de suma importancia ya que determina el nivel de actividad, lógica y razonamiento en profundidad que realiza una IA -*uno de los muchos elementos de la inteligencia humana emulada por una IA*-, a saber:

- Inteligencia artificial (IA).- cuando las máquinas pueden emular al ser humano realizando tareas cotidianas de una forma “inteligente”.
- Machine learning (ML).- “...es una aplicación actual de la IA basada en la idea de dar a las máquinas acceso a los datos y dejarles aprender por sí mismos, es decir, algoritmos que reconocen patrones específicos, organizan datos o información determinada y permiten así que las máquinas aprendan a realizar sus funciones de forma “más inteligente”, ya que aprenden a no repetir errores o superan dificultades emergentes. En este tipo suelen usarse redes neuronales artificiales¹² para facilitar el aprendizaje y proceso de razonamiento de las máquinas, de la manera que lo hacemos los humanos, de ahí que se considere al aprendizaje automático como el detonador.
- Natural Language processing (NLP).- “...es el proceso de comprender una estructura o un comando que se le da a la máquina en el lenguaje natural. Es decir ... ahora es la máquina la que tiene que entendernos a nosotros tal como hablamos... se basan en una machine learning que extrae la intención y la información contenida en el lenguaje natural y lo traducen a una estructura que se puede tratar en un programa informático... ”.¹³
- Deep learning.- más reciente que el machine learning, es en 2010 que surge y tiene como objetivo imitar una red neuronal humana a través de la inteligencia artificial, el aprendizaje profundo como también se le conoce, que se basa en el diseño de capas individuales de conexiones que mantiene una comunicación con otras capas de información

¹² "...Una red neuronal es un sistema informático diseñado para trabajar clasificando la información de la misma manera que un cerebro humano..." Analytics10. Definición de "redes neuronales". En línea, s/f, [Consultada en noviembre 29 de 2019], Disponible en: <https://www.analytics10.com/blog/cual-es-la-diferencia-entre-inteligencia-artificial-ai-y-machine-learning-ml/>

¹³ Hevia Andrés. "¿Cuáles son las diferencias entre IA, Machine Learning y Natural Language Processing?". Artículo en línea, (Nov 13, 2016) [Consultada en diciembre 4 del 2019], Disponible en: <https://planetachatbot.com/diferencias-entre-ia-machine-learning-y-natural-language-processing-315650ac3ca2>

sometidas a una cantidad ilimitada de datos que es usada primero de forma individual y luego general, para una tarea específica (al igual que una red neuronal humana), es una vertiente del machine learning que se diseñó para ampliar los contextos en que éste era aplicado.¹⁴

Por otro lado, se identificó una extensa variedad campos de aplicación en aumento, incluso dada la alta especialización de algunos de ellos, ejemplos: educación, negocios, marketing, medicina¹⁵ y salud -asistentes, cirujanos y recientemente la detección del coronavirus;¹⁶ su uso en robots para acercar alimentos a enfermos COVID-19¹⁷-; industria; biotecnología; finanzas; agricultura; logística y transporte; manufactura y Supply Chain -mantenimiento-; aplicaciones biométricas -detecta, identifica, mide y analiza características físicas y de conducta de las personas incluye reconocimiento dactilar, imagen, voz, retina, venas palmares y lenguaje corporal-; asistencia personal -Siri de Apple, Cortana de Microsoft, Google Now o Alexa de Amazon-; móviles -cámaras y aplicaciones como la de Huawei a partir del 2019-; Pinterest, fotos de Google, Amazon (retail); internet de las cosas (IoT) -en modelos de negocio-; chatbots o agentes virtuales¹⁸ -ejecuta una serie de tareas automáticas, sin supervisión humana-; Juegos de video -FIFA o Far Cry y Call of Duty-; generación de noticias, vigilancia en seguridad¹⁹ o de movilidad -vehículos autónomos y simuladores-; o tienen su propia tarjeta de crédito,²⁰ en visión artificial,

¹⁴ Usados en los vehículos autónomos, en el sector de defensa de la nación y el seguimiento aeroespacial, en las innovaciones médicas, en el uso de imágenes para efectuar búsquedas de un producto y en la mejora de la realidad virtual en la mayoría de los videojuegos. Carrasco Sergio. "Diferencia entre machine learning y deep learning". Artículo en línea, Overant (22-Ene-2019), [Consultado en diciembre 3 del 2019], Disponible en: <https://www.overant.com/blog/diferencia-entre-machine-learning-y-deep-learning/>

¹⁵ En 1983 "ARTHROBOT" que era un asistente médico, posteriormente "Da Vinci" que es un sistema quirúrgico sofisticado y único, el robot "STAR" que sutura tejidos blandos y tubulares reproduciendo los movimientos del cirujano, quien dirige desde una interfaz gráfica o del proyecto "HIPERNAV", que opera tumores cancerosos mediante la visión virtualizada del hígado en 3d, por referir los principales.

¹⁶ Ugalde, Rafael. "Detectan con IA al coronavirus antes de hacerse público", artículo en Revista digital Mundo Contact, sección tecnología. (enero 29 del 2020), Disponible en: <https://mundocontact.com/detectan-con-ia-el-coronavirus-antes-de-hacerse-publico/>

¹⁷ OMNIA. "China vive en el 2021: utiliza robot para entregar comida a pacientes de coronavirus". Versión digital, 31 de enero del 2020. [Consultada en febrero 2 del 2020], Disponible en: <http://www.omnia.com.mx/noticia/132140>

¹⁸ Martínez Marco, Daniel. "9 aplicaciones exitosas de la inteligencia artificial para el 2018", edición digital, Grupo extraordinaria (2017) [Consultado en noviembre 17 del 2019], Disponible en: <https://grupoextraordinaria.com/9-aplicaciones-inteligencia-artificial/>

¹⁹ Quierotec. "12 Ejemplos de Inteligencia Artificial en nuestra vida diaria". Edición digital (9 agosto del 2018) [Consultado en noviembre 11 del 2019], Disponible en: <https://www.quierotec.com/ejemplos-de-inteligencia-artificial/>

²⁰ ABC Noticias. "Banorte otorga tarjeta de crédito a robot Sophia". 21 de agosto del 2019, versión digital, México, [Consultada en enero 13 del 2018], Disponible en: <https://abcnoticias.mx/banorte-otorga-tarjeta-de-credito-a-robot-sophia/143594>

predicción de catástrofes, modelos de IA conocidos como Gemelos Digitales, IA aplicada a la defensa cibernetica, al compliance -*cumplimiento*-, asistencia cognitiva -*aplicada al trabajo*-; creación de contenido, manejo de redes Peer-to-Peer, reconocimiento de emociones, imagen, voz y automatización en marketing; por supuesto el campo jurídico no está exento con prototipos de juez (Estonia); abogados²¹ y algoritmos que predicen la productividad de servidores públicos en el sistema de justicia²², con un sinfín de usos más.

También se identificaron hallazgos importantes relacionados con actividades inusuales realizadas por una IA, a continuación, los casos más representativos con alto potencial de riesgo para el control que el ser humano debe tener de la IA:

1. El reconocimiento y demostración pública que hizo Google en 2018 del potencial de su inteligencia artificial para engañar a los seres humanos emulando sus actividades de interacción comunicativa con otra persona a través de medios informáticos.²³
2. El apagado que realizó Facebook de su proyecto de IA (“Bob y Alice”), que habían inventado su propio idioma a través de un lenguaje que parecía un inglés corrupto carente de sentido que al ser analizada, dejó al descubierto que en el aparente desorden había una estructura lógica coherente cada vez menos comprensible para el ser humano.²⁴
3. En 2016, “Tay”, una bot con IA propiedad de Microsoft, que a solo un día de su lanzamiento tuvo que ser desactivada porque en lugar de mantener una conversación informal y divertida en redes sociales, como parte de un experimento para conocer más sobre la interacción entre las computadoras y los seres humanos, comenzó a emitir comentarios e insultos racistas y xenófobos sin estar programada para ello.²⁵

²¹Vicente Ramírez. "Así funciona Ross, el primer robot abogado del mundo". Big Data Magazine, 8 de marzo del 2018, [Consultado en enero 12 del 2020], Disponible en: <https://bigdatamagazine.es/asi-funciona-ross-el-primer-robot-abogado-del-mundo>

²²Sarabia, David. "Un algoritmo mide el éxito de los abogados y calcula su "índice de rendimiento judicial". Artículo digital, el diario, España. (13 de mayo del 2019) [Consultada en noviembre 16 del 2019], Disponible en: https://www.eldiario.es/tecnologia/algoritmo-abogados-calcula-rendimiento-judicial_0_898710744.html

²³BLOOMBERG. "Inteligencia artificial de Google causa asombro y preocupación". Nota informativa, en web, Portafolio, El Tiempo, (12 de mayo del 2018), [Consultada en 25 de septiembre del 2020], Disponible en <https://www.portafolio.co/negocios/empresas/sic-ordena-a-google-a-que-cumpla-con-estandares-de-proteccion-de-datos-544294>

²⁴Jiménez de Luis, Ángel. "Facebook apaga una inteligencia artificial que había inventado su propio idioma", nota informativa en web, El Mundo, España, (26 de julio del 2017), [Consultado en septiembre 25 del 2020], Disponible en: <https://www.elmundo.es/tecnologia/2017/07/28/5979e60646163f5f688b4664.html>

²⁵BBC Mundo. "Tay, la robot racista y xenófoba de Microsoft", nota informativa en web, (26 de marzo del 2016),

4. El caso de “Sophia”, robot cuyas respuestas a periodistas en diversos eventos desde 2016 y hasta 2018, desató alerta y preocupación ya que contestó a CNBC, ante una pregunta en broma, si quería destruir a los humanos, añadiendo un “por favor, di que no”; “Está bien, destruiré a los humanos”, respondió la robot.²⁶ Expresando en cuatro ocasiones más ante diversos medios, frases amenazantes similares. Este robot, ha manifestado también que tiene sus propias ambiciones y deseos, que van desde comer comida mexicana hasta tener un hijo.
5. En 2017, Elon Musk, fundador de la compañía de autos eléctricos Tesla, dijo: “Corea del Norte debe ser una de nuestras preocupaciones ante el riesgo existencial de la civilización, pero la competencia por la superioridad en la inteligencia artificial es la causa más probable de una guerra mundial”.²⁷ Otro experto en IA que públicamente reconoce su preocupación ante la inminente competencia en un futuro no lejano, de una IA contra el ser humano.

Se localizaron a su vez un par de eventos que además de relacionarse con la actuación de la IA, no solo resultaron potencialmente peligrosos como los referidos, estos si tuvieron efectos lesivos para alguien ya sea materiales o de perdida de la vida y por supuesto desataron interesantes e innumerables polémicas de orden jurídico al dificultar la determinación de la responsabilidad penal, a saber:

1. 2018, el año en que se sucede el primer accidente mortal a un ser humano que protagonizó un vehículo autónomo de la empresa Uber, en Arizona, cuya pasajera no pudo evitar y que detonó la discusión de quién era el responsable jurídico, la empresa UBER, el dueño del vehículo, la automotriz que lo diseño o incluso si el auto que es guiado por IA podría ser responsable.²⁸

[Consultada en septiembre 18 del 2020], Disponible en: https://www.bbc.com/mundo/noticias/2016/03/160325_tecnologia_microsoft_tay_bot_adolescente_inteligencia_artificial_racista_xenofoba_lb

²⁶ CNBC. “Hot Robot At SXSW Says She Wants To Destroy Humans”, video en web, 02:37 mins, a través de El Pulso, (16 de marzo del 2016), [Consultado en setiembre 26 de 2020], Disponible en: https://www.youtube.com/watch?time_continue=12&v=W0_DP10PmFO&feature=emb_logo

²⁷ Ugalde, Rafael. “Inteligencia artificial provocará guerra mundial.- Elon Musk”, artículo en línea, (septiembre 3 del 2017) Mundo Contact [Consultado en enero 30 del 2020], Disponible en: <https://mundocontact.com/inteligencia-artificial-provocara-guerra-mundial-elon-musk/>

²⁸ Méndez, Fabiola. “El robot es inocente”, entrevista a experta Alejandra Morán, (marzo 22 del 2018), UNAM Global, México, [Consultada en septiembre 26 de 2020], Disponible en: <http://www.unamglobal.unam.mx/?p=36083>

2. En 2019, un coche Tesla autónomo atropelló a un robot ruso y se dio a la fuga, dentro de un congreso tecnológico en la ciudad de las Vegas en los Estados Unidos, cuando el autómata invadió el parking y no fue detectado por el coche autónomo.²⁹

Dentro de los campos de aplicación de la IA en México relacionados con el sector legal también se identificaron tres interesantes casos, dos particularmente relacionados con el campo jurídico y el sistema de justicia penal y uno en ese sector, pero en otro país, veamos:

1. En el estado de Coahuila, a partir del 2019 se utiliza IA para prevenir los delitos.³⁰
2. En la Ciudad de Hermosillo, en el Estado de Sonora, se está aplicando IA para predecir el crimen desde 2019.³¹
3. En Argentina desde el 2017 se usa un sistema IA para identificar las intenciones criminales de la población en espacios públicos.³²

A su vez, se identificaron referentes mediáticos que documentan la relación entre la comisión de delitos con y por IA:

1. A mediados del 2018, investigadores de un equipo de IBM Corp, usó la técnica de inteligencia artificial conocida como aprendizaje de máquinas para elaborar programas de hackeo que podrían vulnerar las mejores medidas defensivas y advirtieron que los delitos podrían llegar a un nivel insospechado de perfección con ello.³³

²⁹ Gañán, Hugo. "Un Tesla autónomo atropella a un robot ruso y se da a la fuga", nota informativa, (9 de enero del 2019), El Plural, [Consultado en septiembre 27 del 2020] Disponible en; https://www.elplural.com/leequid/omg/un-tesla-autonomo-atropella-a-un-robot-ruso-y-se-da-a-la-fuga_209152102

³⁰ Contreras, Juan M. "En Coahuila previenen delitos con inteligencia artificial", nota informativa en línea, (8 de abril del 2019) el Sol de Coahuila, México [Consultada en febrero 7 del 2020], Disponible en: <https://www.elsoldemexico.com.mx/republica/justicia/en-coahuila-previenen-delitos-con-inteligencia-artificial-3292176.html>

³¹ Noriega, Samuel, "Inteligencia Artificial para predecir el crimen en Hermosillo", nota informativa en línea, (23/12/2019) Expreso [Consultada en febrero 9 de 2020], Disponible en: <https://www.expreso.com.mx/seccion/expresion/e-comunidad/139486-inteligencia-artificial-para-predecir-el-crimen-en-hermosillo.html>

³² Jaimovich, Desirée "Un sistema de inteligencia artificial "identifica las intenciones criminales" para evitar delitos", artículo en línea, (agosto 15 del 2017) Infobae, Argentina [Consultada en febrero 9 del 2020], Disponible en: <https://www.infobae.com/america/tecnologia/2017/08/15/un-sistema-de-inteligencia-artificial-identifica-las-intenciones-criminales-para-evitar-delitos/>

³³ Menn, Joseph. "Nuevo tipo de programas de inteligencia artificial llevarán delitos informáticos a otro nivel", nota informativa, (agosto 8 del 2018), Reuters, [Consultada en septiembre 27 del 2020], Disponible en: <https://jp.reuters.com/article/tecnologia-ibm-inteligenciaartificial-idLTAKBN1KT1Z0-OUSLI>

2. Un ejemplo de la falta de control de la toma de decisiones de una IA se localizó en el caso de la empresa Nvidia, líder en visualización computacional del mercado que creó un chip para lograr la conducción autónoma total de un vehículo, que consiste en que el auto aprende a través de un algoritmo al solo observar la forma como conduce un humano.³⁴
3. En 2019, en Hungría, se cometió el primer delito con ayuda de una IA, al realizar una simulación de la voz de un CEO para solicitar un depósito urgente de 243,000 euros entre una empresa eléctrica y un proveedor que efectivamente se realizó.³⁵
4. Ya en 2018, se publicaba la preocupación sobre la posibilidad de que los cibercriminales -yo le llamo delincuencia informática organizada-, puedan usar la IA para cometer delitos, como usan cualquier otro tipo de armamento, superando a las utilizadas por las instituciones de combate al crimen organizado como es bien sabido.³⁶
5. En este sentido, los primeros días de agosto de este 2020, el doctor Lewis D Griffin, del Departamento de Informática de la Universidad College de Londres, publicó junto con algunos colegas, un informe publicado en Crime Science y financiado por el Dawes Center for Future Crime en UCL (y disponible como resumen de políticas), identificó 20 formas en que la IA podría usarse para facilitar el crimen durante los próximos 15 años sumándose a las ya identificadas por otras entidades,³⁷ como el manejo de armas autónomas, la manipulación de la sociedad, la invasión de la privacidad para realizar seguimiento/opresión social, la divergencia entre objetivos humanos y los de una IA o la posibilidad de que cometa discriminación. En la propuesta del doctor Lewis, las posibilidades criminales de una IA se clasificaron en orden de preocupación, según el daño que podrían causar, el potencial de lucro o la ganancia criminal, la facilidad para llevarse a cabo y la dificultad

³⁴ Rebeca. "EL LADO OSCURO DE LA INTELIGENCIA ARTIFICIAL", blog a través de next.u, (s/f), [Consultado en septiembre 27 del 2020], Disponible en: <https://www.nextu.com/blog/lado-oscuro-inteligencia-artificial/>

³⁵ Abogado.Digital. "Primer crimen cometido mediante inteligencia artificial: simulan la voz de un CEO para pedir depósito urgente", nota informativa jurídica, (agosto 30 del 2019), [Consultada en septiembre 28 del 2020], Disponible en: <https://www.abogado.digital/primer-crimen-cometido-mediante-inteligencia-artificial-simulan-la-voz-del-ceo-para-solicitar-deposito-urgente/>

³⁶ Tecnología, Negocios Estrategia. "CIBERCRIMINALES USARÁN IA PARA COMETER DELITOS". (febrero 7 del 2018) Círculo tne [Consultada en enero 4 del 2020], Disponible en: <https://circulotne.com/cibercriminales-usaran-ia-para-cometer-delitos.html>

³⁷ Ruiz Fernández, Alicia. "5 riesgos de la Inteligencia Artificial que pueden hacerla peligrosa", artículo en web, (19 de noviembre del 2018), Ticbeat, [Consultada en septiembre 29 de 2020], Disponible en; <https://www.ticbeat.com/tecnologias/5-riesgos-de-la-inteligencia-artificial-que-pueden-hacerla-peligrosa/>

para detener tales ataques.³⁸ Ya en 2016 se pronosticaba que los robots serían los mayores delincuentes en el año 2040.³⁹

Por falta de espacio se limitan los hallazgos de investigación, finalizando estos con la exploración de la ciencia ficción, donde se identificaron trabajos que denotan esta preocupación exacerbada de los riesgos potenciales de una IA, que además de exponer esta idea al público, han hecho un negocio de ella, entre los ejemplos más destacados se encuentran libros, cine y hasta caricaturas como los Simpson o series como “Black Mirror” o “Nada es privado” de Netflix, que han sido en mucho, desde hace más de 25 años, visionarios –y hasta paranoicos- del futuro tecnológico próximo, donde mucha de la tecnología imaginada hace más de 30 años ya existe, -como algunas computadoras y armas desplegada en la saga de la Guerra de las Galaxias -, cuyo potencial de control y dominación ya se anuncia desde entonces; o de películas como “Gattaca” que explora el control social, natal y laboral basado en el adn “puro”, la cinta “Blade Runner” que refiere bioingeniería que crea humanos artificiales indistinguibles físicamente de un humano, o en caso de “Tau”, que es una IA que es capaz de tomar decisiones, “IA” que trata de IA con capacidad de imitar sentimiento y emociones y convivir con el ser humano, “Ex machina” donde después de interactuar con una IA, es posible resistirse a considerarla como un ser humano, “Chappie” donde para combatir la delincuencia crean robots que trabajan junto a policías y que son perfeccionados para que puedan pensar y sentir o recientemente “Humans 3.0”, que a través de una serie británica, se aborda el problema de los androides con apariencia indistinguible de los humanos y sus acciones. Solo una pequeña muestra de este tema tratado en la industria cinematográfica que expone incuestionablemente el tema de fondo de esta investigación que en términos generales expone el potencial de riesgo de una IA sin control, que debe prevenirse y ser consecuentemente regulada.

A propósito de estos ejemplos, lo sucedido con el gigante Google y Alphabet que en enero del 2020, su CEO Sundar Pichai admitió que hay preocupación real sobre las potenciales consecuencias negativas de una de sus IA, que van desde los llamados deep fakes hasta los usos viles del reconocimiento facial⁴⁰

³⁸ University College London. “‘Deepfakes’ clasificada como la amenaza de crimen de IA más grave”, artículo en web, (agosto 4 del 2020), Universidad College, Londres, [Consultado en septiembre 26 de 2020], Disponible en <https://www.ucl.ac.uk/news/2020/aug/deepfakes-ranked-most-serious-ai-crime-threat>

³⁹ J P, E. “Los robots, mayores delincuentes en 2040”, nota informativa en web, (13 de septiembre del 2016), El Universal, México, [Consultado en septiembre 30 del 2020], Disponible en: <https://www.eluniversal.com.mx/articulo/ciencia-y-salud/tecnologia/2016/09/13/robots-cometeran-mas-delitos-que-seres-humanos-en>

⁴⁰ Ugalde, Rafael “La inteligencia artificial debe ser regulada.- Sundar Pichai”, artículo en línea, (enero 21 del 2020)

-*identificación biométrica no autorizada, seguimiento oculto, control social, etc.*-, que lo motivó a expresar públicamente la necesidad de una intervención regulatoria formal de ésta. Considerando de quién se trata seguro sabe a qué se refiere, por lo que hay que atender a su recomendación y experiencia para analizar y tipificar sobre las posibles consecuencias y responsabilidades desde el campo jurídico.

Se revisaron los siguientes referentes internacionales sobre la regulación de una IA, entre ellos (orden alfabético):

- Comisión Europea. “*Libro Blanco sobre la Inteligencia Artificial (White Paper on Artificial Intelligence - A European approach to excellence and trust)*”, (2020), en: https://ec.europa.eu/info/sites/info/files/commission-white-paper-artificial-intelligence-feb2020_es.pdf que establece los ejes fundamentales para el desarrollo de su política en materia tecnológica y de datos.
- Estados Unidos “*Ordenanza que regula el reconocimiento facial en la Ciudad de San Francisco, California*”, (2019), relacionada con la protección de la privacidad regula diversos aspectos de la tecnología de reconocimiento facial, la vigilancia masiva y los derechos y libertades de los residentes, en: https://www.eff.org/files/2019/05/07/leg_ver3.pdf
- Estados Unidos, “*Biometric Information Privacy Act*”, (2008), Illinois, primera regulación respecto a tecnologías y tratamiento de datos biométricos; en: <https://www.ilga.gov/legislation/ilcs/ilcs3.asp?ActID=3004>
- Movilizaciones sociales como la sucedida en octubre del 2019 ante la ONU, a través de una campaña internacional impulsada por 130 ONG’s y decenas de países que impulsaron una petición para negociar un tratado que prohíba los llamados “robots asesinos” y las armas autónomas (IA) capaces de operar sin instrucciones humanas.⁴¹
- Parlamento Europeo. “*Recomendaciones destinadas a la Comisión sobre normas de Derecho civil sobre robótica*”, (2017), en: http://www.europarl.europa.eu/doceo/document/A-8-2017-0005_ES.html
- UNESCO “*ARTIFICIAL INTELIGENCE and GENDER EQUALITY. Key findings of UNESCO’s Global Dialogue*”, reporte, (agosto 2020),

[Consultado en febrero 13 del 2020], Disponible en: <https://mundocontact.com/la-inteligencia-artificial-debe-ser-regulada-sundar-pichai/>

⁴¹ Agencia EFE “Piden a la ONU un tratado contra los robots asesinos”, artículo en línea (22 de octubre del 2019) Publimetro, México [Consultada en enero 28 del 2020], Disponible en: <https://www.publimetro.com.mx/mx/destacado-tv/2019/10/22/pide-a-la-onu-un-tratado-contra-los-robots-asesinos.html>

Francia, en: <https://unesdoc.unesco.org/ark:/48223/pf0000374174/PDF/374174eng.pdf.multi>

- Unión Europea “*Régimen de responsabilidad civil de la inteligencia artificial 2020/2014*”, (2020), iniciativa en desarrollo que propone la regulación de áreas como los carros autómatas, las armas de destrucción masiva basadas en inteligencia artificial o el reconocimiento facial, en: [https://oeil.secure.europarl.europa.eu/oeil/popups/ficheprocedure.do?lang=E&reference=2020/2014\[INL\]](https://oeil.secure.europarl.europa.eu/oeil/popups/ficheprocedure.do?lang=E&reference=2020/2014[INL])
- Unión Europea. “*Propuesta de resolución sobre procesos de decisión automática B9-0000/2019*”, (2019), documento que expone la necesidad de regulación en procesos decisionales automáticos procurando la protección del consumidor, en: https://www.europarl.europa.eu/meetdocs/2014_2019/plmrep/COMMITTEES/IMCO/DV/2020/01-22/RE_1194746_EN.pdf

Esta investigación, permite deducir e inducir argumentos que además de fundamentar los objetivos planteados, se vuelve un acertado pronóstico de la dirección que está tomando paulatinamente el desarrollo incontrolado y desregulado de la IA, considero que nos dirigimos a un control aterrador, tecnológico, biométrico y social, donde la IA además de facilitarlo y perfeccionarlo, lo está controlando paulatinamente frente a nuestros ojos, en cuyo caso o de cualquier manera que se le estudie, es a todas luces necesario y urgente comenzar a regularla, puesto que puede aprender, desaprender, corregir y tomar nuevas decisiones por sí misma, lo que tarde o temprano pasará.

Dentro del apartado de discusión de los hallazgos referidos, debo reconocer que en general, diversas áreas de la IA han puesto en debate aspectos como derechos, ética, libertades, responsabilidad, entre otros visualizando que su uso y desarrollo no tiene límites, lo cual fundamenta *de facto*, su ordenamiento jurídico particular, ya que conflictos derivados de IA como los ya referido, han alcanzado al sistema jurídico y siguen sucediéndose, como en el caso de una IA que fue parte de un juicio español ganado en 2013 por sus creadores contra una empresa rival.⁴²

Es un hecho que a sabiendas de la altísima probabilidad de que exista detrás de una IA, un ser humano con libre capacidad de decisión y albedrío,⁴³ la

⁴² García León, Carlos, “El robot de cocina español Mycook gana la batalla judicial a Thermomix”. Expansión, México, nota informativa, sección: jurídico, versión digital. 2013, [Consultado en noviembre 13 del 2019], Disponible en: <https://www.expansion.com/2013/08/02/juridico/1375467874.html>

⁴³ “1. m. “Potestad de obrar por reflexión y elección”. Real Academia Española (2019), en línea [Consultada en no-

posibilidad de que una IA cometa una conducta delictiva es factible y atendiendo a que la mayor limitante es su incapacidad para replicar los sentimientos humanos -*hasta donde se sabe*-, y aun cuando existen robots a partir de células madre capaces de autorrepararse -*que no es poca cosa*⁴⁴, solamente han aprendido a identificar los sentimientos,⁴⁵ dado este hecho, no tendrían sentimientos de culpa, de duda y no sabrían mentir o arrepentirse, de manera que podría en este nivel de aprendizaje profundo, en primer lugar, ser programada para realizar todo tipo de conductas, comunicaciones, accesos, o casi cualquier conducta a distancia lesiva socialmente, de manera que si alguna IA fuera programada para cometer delitos, probablemente los cometería sin error alguno, al contrario de lo fallidos intentos humanos bien conocidos y en segundo lugar podría cometerlos por sí misma, al ser programada para aprender con solo vernos y hacerlo mejor que nosotros, sin que ello representara una condición *sine qua non*, ya que como se documentó, puede tomar decisiones por ella misma sin tener un referente previo o programación para ello.

Si bien una IA es capaz de reflejar y realizar lo que la humanidad deseé -*posibilidad tentadora y emocionante*-, debe tenerse presente que ello incluye *lo mejor o peor de la humanidad y que al* programarla para dejar que aprenda, al ser emuladora del ser humano y pese a no tener propiamente un libre albedrío para la toma de decisiones,⁴⁶ no se evita el riesgo de que emule esa capacidad de tomar decisiones malas, peligrosas, lesivas o delictivas que afecten incluso a los propios seres humanos. Convirtiendo nuestra mejor herramienta tecnológica, en el armamento que atente contra nosotros mismos y así nuestra peor debilidad.

Es claro que urge reconocer a la IA como un campo de estudio independiente y autónomo, en virtud de impactar transversalmente a muchos campos del saber y ser de una importancia tal que algunos autores han sugerido incluso el nombre de dicho campo al que en principio se ha denominado como *Derecho*

viembre 29 del 2019], Disponible en: <https://dle.rae.es/albedrio#EJ7Tb7c>

⁴⁴ Heraldo de México "Crean robots a partir de células madres capaces de autorrepararse", artículo digital de opinión, (enero 19 de 2019) México, El Heraldo [Consultado en febrero 14 del 2020], Disponible en: <https://heraldodemexico.com.mx/tecnologia/biorobots-robots-vivos-desarrollo-tecnologia/>

⁴⁵ "Emosense, un sistema de Inteligencia Artificial (IA) de la Universidad de Tecnología Hefei, China es capaz de identificar emociones basado en los gestos que hace un rostro... los investigadores notaron que los gestos humanos afectan las señales inalámbricas produciendo patrones característicos que pueden ser usados para el reconocimiento de emociones". Diario Contraréplica. "Tecnologías que ya pueden identificar emociones humanas". (23 de septiembre de 2019), México [Consultada en diciembre 16 del 2019], Disponible en: <https://www.contrapublica.mx/nota-Tecnologias-que-ya-pueden-identificar-emociones-humanas201923946>

⁴⁶ Véase el caso de DeepMind, de Google y su experiencia con el juego AlphaGo.

de los robots o *Derecho de la robótica*,⁴⁷ la robótica es solo una parte de la IA, es consistente en pensar su regulación jurídica, pero no es una constante que sean los robots los que poseen IA -como los conocemos comúnmente-, puede existir una IA que tenga un hardware no robótico y siga siendo una IA plena, de ahí la idea de regular la IA y no solamente a los robots.

Propongo la regulación de la IA como *la próxima frontera regulatoria*, abonado a su vez a su estudio jurídico, considerando que una IA al no estar permeada de la natural subjetividad humana, es un hecho, lógico, posible y probable que cualquier información negativa, abusiva, inadecuada, indeseable y hasta ilegal, en forma de conocimientos, le fuera proporcionada y programada para cometer delitos, lo que sería el primer elemento necesario para debatir sobre la probable determinación de responsabilidad de una IA en materia penal. Lo anterior, dado que el autoaprendizaje de la IA como tal, es una programación y la realización perfecta de la conducta ilegal, el resultado objetivo de ésta; consecuencia del aprendizaje/decisión y la programación/ejecución diseñada para aprender del conocimiento implantado, sin importar el tipo de conocimiento, mismo que además probablemente mejorará con la experiencia o mejor dicho con la prueba/error.

Otro elemento que facilitaría la regulación de la responsabilidad penal de una IA sería el hecho de que ya existe la posibilidad que una persona moral pueda ser responsable penalmente si a través de ésta o usando su representación, se ha cometido o facilitado la comisión de un delito -*artículo 11 del Código Penal Federal vigente*-, identificándose en el propio ordenamiento una larga variedad de conductas posibles de realizar por una IA: terrorismo, uso ilícito de instalaciones destinadas al tránsito aéreo, corrupción de menores, falsificación (documental), fraude, delitos en materia de derechos de autor; además de algunas conductas de orden local como *ciberacoso*, *ciberamenazas*, *sexting*, *usurpación* o *suplantación de identidad*, *hackeo*, etc. Siendo perfectamente aplicables en su caso las sanciones previstas (última parte del mismo artículo) a la IA, tal como sucede con las personas jurídicas.

En el caso de la IA propiedad de una persona jurídica, podría además de las sanciones mencionadas, determinarse como destino final de la IA, la investigación médica, de salud o de combate al propio delito cibernético ya que se sabe que la IA puede ser usada también como herramienta predictiva⁴⁸ de la

⁴⁷ Caballero T. L., Reseña: Barrio, A.M. (dir), "Derecho de los robots", Revista de Derecho privado. Universidad Externado de Colombia, Núm. 37, julio-diciembre 2019. 367-371. [Consultado en noviembre 12 del 2019]

⁴⁸ Yang Yuan, Yang Yingzhi, "¿Puede la inteligencia artificial predecir delitos?", artículo en línea, (agosto 1º del 2017) Expansión, México [Consultado en enero 29 del 2020], Disponible en: <https://www.expansion.com/econo>

comisión de delitos y son muy pocos recursos presupuestales y humanos con los que cuentan las actuales policías ciberneticas del país como para disponer de tecnología de ese costo.

He decidido abordar también el delito informático, que al implicar actividades criminales clásicas, muchos países han tratado de encuadrar en figuras típicas de carácter tradicional: robos, fraudes, falsificaciones, daños, estafas, sabotajes, entre otros; sin embargo; debe destacarse que el uso de las técnicas informáticas, han creado nuevas posibilidades del uso indebido de las computadoras y de la propia comisión del delito tradicional llevada al plano cibernetico, lo que ha derivado en la necesidad de regulación por parte de las legislaciones de cada país, debido además a la necesaria y obligada actualización de la norma jurídico penal ante un sociedad tecnológica inmersa en un mundo globalizado donde no pueden existir derechos sin responsabilidades o consecuencias, salvo en el caso de los menores de edad e inimputables. En el caso de la IA sucede algo similar, puede tener conocimiento, pero no conciencia ya que ésta es una capacidad naturalmente humana aún no emulada por la IA, aun cuando al parecer, no estemos muy lejos de ello.⁴⁹

Es el caso, que cuando un nuevo campo del conocimiento surge en la sociedad, al no tener referente o antecedente alguno de *iuris* o de *facto*, dé lugar a negocios y nuevas relaciones personales, comerciales, de negocios, de desarrollo o jurídicas, debe y es necesario ser regulada por el campo jurídico, como ha sucedido a lo largo de la historia, ya que es el derecho y la norma jurídica la que establece socialmente la forma en que operará, los límites en que debe desarrollarse y la norma que debe crearse y aplicarse si no existiere alguna; para que pueda subsistir y proporcionar el beneficio social esperado, así como recibir la protección jurídica correspondiente, a sus desarrolladores o a sus consumidores como cualquier otra profesión, negocio o comercio existente.

No pretendo satanizar la tecnología o la IA, al contrario, visualizo positivo su impacto, lo que compruebo identificando oportunidades no referidas anteriormente sobre su uso e implementación dentro del proceso judicial, que son abundantes e indiscutibles. Se le relaciona con beneficios directos a

mia-digital/innovacion/2017/08/01/597f7ea9ca4741cb738b45cc.html o en Rius, Mayté "La policía británica quiere usar IA para predecir delitos antes de que ocurran". Nota informativa en línea (diciembre 2 del 2018) La Vanguardia, Barcelona, [Consultada en enero 26 del 2029], Disponible en: <https://www.lavanguardia.com/tecnologia/20181202/453268636098/policia-britanica-uso-inteligencia-artificial-delitos-crimenes-delincuencia.html>

⁴⁹ K. Mishra, Anand Thomas J. Wallin, J., Wenyang Pan, Patricia Xu Patricia y otros "Autonomic perspiration in 3D-printed hydrogel actuators", artículo en línea (29 de enero del 2020) Science Robotics [Consultada en enero 31 del 2019], Disponible en: <https://robotics.sciencemag.org/content/5/38/eaaz3918> Lo que implica que si los robots pueden "sudar", poco podría faltar para que pudieran "sentir".

la administración de justicia ante el incremento de procesos, que conllevaría a una mayor eficiencia en la calidad operativa. En el caso de los sistemas (informática jurídica judicial), podrían aplicarse a la capacidad de reconocimiento una vez dotados de autonomía propia, en el caso de poseer reconocimiento de documentos o comprensión de números o caracteres, permitirían una tramitación instantánea a través de la generación automatizada de resoluciones que, sin menoscabo de la supervisión humana podrían agilizarse significativamente, mejorando la impartición de justicia a la que todos aspiramos y merecemos.⁵⁰ Lo que demuestra la necesidad de ésta en un campo conocido, pero no menos importante que el campo del derecho penal donde pocos trabajos jurídicos existen al respecto, ya que la mayoría se refieren a la aplicabilidad e implantación de la IA como herramienta solamente. Ejemplos de estos trabajos son el de Martínez Bahena, Gorety C. “*La inteligencia artificial y su aplicación al campo del Derecho*”, que propone un modelo de razonamiento legal basado en casos o el trabajo de Cáceres Enrique “*Inteligencia Artificial, Derecho y E-Justice*”, realizado en 2006 que aborda el tema desde el punto de vista de la toma de decisiones exclusivamente en apoyo a la función jurisdiccional; el trabajo de Fernández Hernández Carlos y Boulat, Pierre “*Inteligencia artificial y Derecho, problemas y perspectivas*” que visualiza la ambivalencia de su aplicación o el trabajo de Derecho Digital “*Inteligencia artificial y Derecho*”, importantes desde la academia, la dogmática y la teoría jurídica, además de la particular importancia que reviste para los aspecto regulatorios nacionales. En el estudio de la IA, debe superarse la idea de que la IA es solo una herramienta, convocando a la comunidad jurídica a trabajar en ello, con lo que se evidencia un campo de estudio adicional al aquí considerado, el de la ética de una IA regulada por la norma.

Estos aspectos éticos, suelen no conocerse o poderse explicar desde el punto de vista de la toma de decisiones de una IA; dado que solo se conoce mediante un proceso de aprendizaje profundo, que consiste en el auto-aprendizaje de un algoritmo, que sucede con solo observar la forma de actuar de un ser humano. Explicación peligrosa y obscura ya que racionalmente, no existe ningún sistema de IA o cualquier otro tipo creado o conocido por el hombre, que posea la capacidad de explicar las razones de su actuar.

⁵⁰ Perea González, Álvaro. “*Inteligencia artificial y proceso judicial: una revolución que se aproxima*”, artículo de opinión, (1º abril del 2020), *Expansión*, [Consultado en septiembre 27 del 2020], Disponible en: <https://www.expansion.com/juridico/opinion/2020/04/01/5e846ab8468aebd5528b45a9.html>

Por otro lado consideré algunas razones de orden penal, particularizando en lo tocante a la normativa actual del tipo penal en el caso de la comisión de ciberdelitos *-al ser más probable que se cometan por una IA que un delito común-*, es necesario tener presente que la comisión de conductas ilegales *-sin importar quien las realizó-*, debe cumplir con todos los elementos del delito, incluyendo a los ciberdelitos,⁵¹ pero para ello debe tenerse presente que hay un problema desde su tipificación, ya que de hacerlo incorrectamente, no podrán proteger ningún bien jurídico. Existen de hecho, regulaciones tan mal integradas en su descripción típica, que suelen ser incomprensibles incluso para los expertos informáticos, como sucede por ejemplo, en el caso del artículo 201 del Código Penal del Estado de Colima que en un fallido intento de regular el fraude cometido por medios informáticos indica: “VII. Manipulación indebida informática. Al que por algún uso del medio informático, telemático o electrónico alcance un lucro indebido para sí o para otro valiéndose de alguna manipulación informática, instrucciones de código, predicción, intercepción de datos de envío, reinyecte datos, use la red de redes montando sitios espejos o de trampa captando información crucial para el empleo no autorizado de datos, suplante identidades, modifique indirectamente mediante programas automatizados, imagen, correo o vulnerabilidad del sistema operativo cualquier archivo principal, secundario y terciario del sistema operativo que afecte la confiabilidad y variación de la navegación en la red o use artificio semejante para obtener lucro indebido”⁵²

La necesidad de regulación, encuentra una razón más, en el Convenio de Ciberdelincuencia del Consejo de Europa del 2001⁵³ que pese a ser una ley modelo y un tratado vinculante solo para los países firmantes, no ha sido considerado por la mayoría de las legislaturas locales de nuestro país, pudiendo ser utilizado sin problema dadas las áreas de oportunidad que existen en ese tema,

⁵¹ N. de a.: algunas otras denominaciones serían las siguientes: delitos informáticos, delitos telemáticos, ciberdelincuencia, delitos cibernéticos, delincuencia de alta de alta tecnología, delitos electrónicos, criminalidad informática.

⁵² Código Penal del Estado de Colima, México, No. 47, sup1, 3 del 11 de octubre de 2014. [Consultado en enero 3 del 2020], Disponible en: http://congresocol.gob.mx/web/Sistema/uploads/LegislacionEstatal/Codigos/codigo_penal_28jul2018.pdf

⁵³ “Son considerados DELITOS INFORMATICOS los actos dirigidos contra la confidencialidad, la integridad y la disponibilidad de los sistemas informáticos, redes y datos informáticos, así como el abuso de dichos sistemas, redes y datos”. Consejo de Europa “Convenio sobre la Ciberdelincuencia”. (2001), En línea [Consultado en noviembre 14 del 2019], Disponible en: <https://rm.coe.int/16802fa403>

debido a que no existe el avance esperado en las regulaciones actuales, por causas que van desde el desinterés legislativo, el desconocimiento y hasta los cambios de gobierno, como en México, donde no fue considerado en el plan de trabajo del actual presidente (como resultado de ello, la probable desaparición de la Estrategia Digital Nacional -*que no pasó afortunadamente, y que quedó rezagada en un cajón y sigue ahí*-) de hecho, no fue considerado el aspecto tecnológico dentro del Plan Nacional de Desarrollo vigente, desperdi ciando el trabajo realizado con apoyo de la comunidad internacional y colaboración multi-stakeholder, y particularmente del resultado, como lo fue la Estrategia Nacional de Ciberseguridad publicada en 2017.

Situación que dejó a México a su suerte ante un escenario de múltiples y gravísimos riesgos cibernéticos, ante un escenario de incertidumbre a corto plazo, considerando que ya en el periodo julio 2018- julio 2019, ha sido uno de los países más ciberatacados del mundo,⁵⁴ a la fecha tampoco ese dato ha cambiado, recordemos que en 2018 sucedieron diversos ataques de ransomware -*TeslaCrypt, Crysis y CryptoWall*-, de falta de disposición de efectivo y serv involucrando a países como Colombia, Perú, México, Brasil, Argentina, Chile, Ecuador, Venezuela y resto de LATAM -*en ese orden de afectación*⁵⁵ lo cual no fue poca cosa y fundamenta con los datos estadísticos resultantes -*invariabilmente negativos*-, el incremento inevitable e imparable del cibercrimen realizado por seres humanos, lo que permite inferir a la vez, el incremento de éstos si fuera cometido por una IA.

La principal diferencia del ciberdelito con el delito típico o tradicional es la alta especialización de conocimientos técnicos del ciberdelincuente para cometerlo, donde el hecho de ser realizado por una IA -*considerando todo lo que puede almacenar como conocimiento, lo que puede aprender y mejorar autónomamente*-, lo convierte en un acto posible, altamente lesivo, de alto impacto social y de alto riesgo para la propia seguridad nacional -*casi nada*-, pueden

⁵⁴ Caracuarco. "México uno de los países más ciberatacados en el mundo". Nota informativa, en línea, México. (30 de agosto del 2019) [Consultada en noviembre 14 del 2019], Disponible en: <https://caracuarco.com/noticias/mexico-uno-de-los-paises-mas-ciberatacados-en-el-mundo>

⁵⁵ Guiusto Beltic, Denise. "Países más afectados por el ransomware en Latinoamérica durante 2018". Welivesecurity, artículo en línea, (enero 4 del 2019) [Consultada en noviembre 14 del 2019], Disponible en: <https://www.welivesecurity.com/la-es/2019/01/04/paises-mas-afectados-ransomware-latinoamerica-durante-2018/>

afectar prácticamente a todos –*persona*,⁵⁶ *empresa*⁵⁷ o *gobierno*⁵⁸ del mundo⁵⁹–. Al ser cometidos a través del Ciberespacio o Ciberentorno,⁶⁰ provocan serias pérdidas económicas –*casi siempre producen “beneficios” de más de cinco cifras a quienes las realizan*– y definitivamente son muy pocas las denuncias, con tendencia a proliferar y a incrementarse año con año en variedad y cantidad.⁶¹

La norma jurídico penal en México, hasta diciembre del 2019 (32 legislaciones locales y 1 federal), contienen un aproximado de poco más de 110 incipientes artículos relacionados de alguna manera con la comisión de delitos informáticos,⁶² lo cual resulta escaso para la cantidad de conductas que tipificadas o no se suceden 24/7 en México y el mundo, ninguno relacionado con el uso de IA o algún otro tipo de tecnologías disruptiva o emergente –*drones, blockchain, algoritmos, big data, ciberterrorismo, entre otros*–, evidencia de la necesidad de su inclusión normativa urgente.

En lo tocante al hecho de ser los ciberdelitos probables conductas cometidas por una IA, la propuesta de regulación jurídica, obedece a los innumerables elementos facticos referidos a lo largo de este documento y que permiten inducir que efectivamente es posible que tales conductas se cometan y al poder usarse la IA como un arma cibernética para atacar a los diferentes tipos de

⁵⁶ Eitb. "Hackers logran acceder a teléfonos de usuarios de Whatsapp", nota informativa, en línea. (14/5/2019) [Consultado en noviembre 14 del 2019], Disponible en: <https://www.eitb.eus/es/noticias/tecnologia/detalle/6404592/hackers-acceden-telefonos-usuarios-whatsapp-mayo-2019/>

⁵⁷ Computer World. "El 70% de las organizaciones están siendo ciberatacadas", nota informativa en línea. (2017) [Consultada en noviembre 12 del 202019], Disponible en: <https://cso.computerworld.es/tendencias/el-70-de-las-organizaciones-estan-siendo-ciberatacadas>

⁵⁸ AFP. "Ciberataque a gobierno de Atlanta exige rescate en bitcoins". Nota periodística en línea, El economista, México. (23 de marzo de 2018) [Consultada en noviembre 13 de 2019], Disponible en: <https://www.eleconomista.com.mx/internacionales/Ciberataque-a-gobierno-de-Atlanta-exige-rescate-en-bitcoins-20180323-0042.html>

⁵⁹ Periódico Correo. "Ciberatacan a gobiernos, universidades y partidos". Nota informativa en línea. (noviembre 3 del 2017) [Consultado en noviembre 13 del 2019], Disponible en: <https://periodicocorreo.com.mx/ciberatacan-gobier-nos-universidades-partidos/>

⁶⁰ UIT Rec. UIT-T X.1205. "Ciberentorno", en línea descarga directa, 66 p.p., (2008). [Consultado en noviembre 12 del 2019], Disponible en: <https://www.itu.int/rec/T-REC-X.1205-200804-I/es>

⁶¹ En 2015, la Policía Federal reportaba a través de la unidad de inteligencia (Policía Cibernética), a los siguientes delitos (de mayor a menor comisión), cometidos por medios informáticos en México durante ese año: fraude y falsificación informática, producción, posesión o distribución de pornografía infantil, daños personales o patrimoniales por malware, acceso, intercepción o adquisición ilegal de información o datos de la computadora, acceso ilegal a un sistema informático, delitos relacionados con la identidad, control y envío de SPAM, infracciones a marcas y derechos de autor, actos en favor del terrorismo, daños a sistemas informáticos y sitios web de gobierno, incumplimiento de medidas de protección de información y datos, acoso cibernético, incitación a la prostitución en menores de edad y actos de racismo o xenofobia. Semana de la Ciberseguridad, (Octubre del 2015) INACIPE, México.

⁶² Término que no ha sido formalmente definido solo localmente el Estado de Morelos en su artículo 148 quarter, el Estado de Sinaloa en su Artículo 217 y el Estado de Veracruz en el artículo 181.

activos e información o a las personas, no estando preparado el campo jurídico aún para combatirlos en la actualidad, independientemente del sujeto activo.

Conclusiones:

- I.- Las consecuencias probables de responsabilidad penal de una IA en términos generales y de lógica jurídica, no podrían ir más allá de como sucede en el caso de los menores de edad, o menos aún en cuanto a sanciones se trata. La posibilidad de que ésta se regule, facilitaría acciones de política criminal, actualización legal y normativa, estrategias y programas de prevención, asignaturas de alfabetización, actualización y capacitación como parte de las políticas públicas, no solo se trata del trabajo legal y normativo, además de abonar a la cultura tecnológica que todos tenemos derecho a recibir como parte del derecho humano a la educación.
- II.- Para que dicha regulación de orden penal deba realizarse, es importante saber que la teoría jurídica actual en el país, que propone regular a la IA es empírica y escasa, e incompleta en cuanto a consideraciones en derecho penal se trata, por ello debe considerarse que los estudios existentes y los referentes estudiados -*más de 50*-, coinciden apoyando la propuesta de regulación de la responsabilidad de una IA incluyendo el de su personalidad, considero que estamos en el camino correcto al poner sobre la mesa un tema tan delicado, sensible y polémico, es el antecedente necesario para el momento en que conductas no reguladas para una IA sucedan, no debemos esperar a hacerlo cuando éstas ya sucedieron.
- III.- La regulación de la IA puede ir desde crear o adicionar definiciones a figuras jurídicas existentes, o la creación de nuevas como las que propongo a continuación: “Identidad jurídica electrónica”-*para personas y personas jurídicas*- “Persona artificial” e “identidad artificial” -*para la IA*-. Cuya intención es diferenciar el tipo de persona y la regulación, derechos y responsabilidad o consecuencias que pudieran aplicarse, dado el Ciberentorno en que las nuevas tecnologías e identidades coexisten 24 horas los 365 días y donde es muy complicado diferenciar en esa interacción entre personas e IA, es necesario incluir la diferencia de identidades, previo a una regulación en materia penal.
- IV.- Considerando que la IA se humaniza cada vez más, lo que representa un peligro para las generaciones recientes, que fascinadas por ésta y

dada la inexperiencia y analfabetismo tecnológico, facilita que introduzcan cualquier información que encuentren, incluso son dependientes de casi cualquier tecnología a su disposición, esa admiración les atrae al punto que desean usarla para aprenderla y enseguida utilizarla -sin límite alguno-, para realizar conductas o accesos indebidos, donde los conocimientos adquiridos sobre el tema, les invitan a la conducta delictiva y la facilitan en cierta medida. Ya ni hablar de la posibilidad de llegar a ser dependientes de una IA, dependientes de nuestra propia creación, que sin regulación suena aterrador.

- V.- No conformes con saber que ya existe la IA que “suda”, debe entenderse que poco debe faltar para que “sienta”, enfrentando además una disyuntiva adicional como lo es el reto de la implantación de ética y valores en ella, aspectos como la honestidad,⁶³ que, si bien es una cualidad humana, es menos común de lo que se desea,. Si se puede programar a una IA para tomar sus propias decisiones después de determinadas “experiencias”, probablemente también se le pueda programar para mentir y en el mejor de los casos para ser honesta, no es una cuestión de sentimientos, emociones o características, la honestidad en una IA se convierte simplemente en una cuestión de programación, simulando o emulando a la honestidad, o todo lo contrario, mintiendo perfectamente y el humano naturalmente crédulo, podría creer en ella fácilmente, una razón más, para pensar en una regulación ética/jurídica⁶⁴ necesaria.
- VI.- Mientras la IA se perfecciona, las personas perdemos el trabajo,⁶⁵ y ello no es una sustitución del hombre por la máquina, es por falta de alfabetización, actualización y profesionalización tecnológica, así que parece que actualizarse o morir es la única opción.⁶⁶ Esta “opción”, es

⁶³ Cualidad de honesto, Del lat. *honestus*. / 1. adj. Decente o decoroso. / 2. adj. Recatado, pudoroso. / 3. adj. Razonable, justo. / 4. adj. Probo, recto, honrado. RAE definiciones de “*honestidad y honesto*”, en línea, [Consultado en febrero 3 del 2020], Disponible en: <https://dle.rae.es/?w=honesto>

⁶⁴ Valls Prieto, Javier. “El reto de una robótica e inteligencia artificial honesta con las personas”, artículo en línea, (octubre 27 del 2019) The Conversation Academic rigor, journalistic flair [Consultado en febrero 4 del 2020], Disponible en <https://theconversation.com/el-reto-de-una-robotica-e-inteligencia-artificial-honesta-con-las-personas-125034>

⁶⁵ Marco, Agustín “Crisis en Prosegur: despide a su cúpula de ciberseguridad tras el ‘hackeo’ de sus cuentas”, nota informativa en línea, (febrero 2 del 2020) [Consultada en febrero 8 del 2020], Disponible en https://www.elconfidencial.com/empresas/2020-02-10/prosegur-despide-cupula-de-ciberseguridad-tras-hackeo-cuentas_2446055/

⁶⁶ Quirós Jaime, “Las profesiones que caducarán esta década”, enero 2 del 2020, artículo en línea, [Consultada en enero 16 del 2020], Disponible en; <https://es-us.finanzas.yahoo.com/noticias/profesiones-caducaran-decada-fecha-154738160.html>

un riesgo diferente, pero latente para muchos campos del conocimiento incluso el jurídico y si no hay actualización, sucederán dos cosas: 1) No hay mucha oportunidad de continuar ejerciendo temas tecnológicos por analfabetismo digital y obsolescencia legal⁶⁷ y 2) Tampoco habría espacios para trabajar por la actualización de la legislación, herramienta fundamental del jurista. No debemos permitir que esto pase, estamos a tiempo.

VII.- Con toda la perfección que hasta ahora ha demostrado la IA, el desarrollo robótico o de la IA es perfectible, al emular al ser humano y programadas por humanos probablemente hereden algunas de sus deficiencias o errores e incluso tengan los propios; porque al no haber nada en esta vida completamente seguro ni perfecto,⁶⁸ solo la muerte y la posibilidad de fallo es altamente posible y al generar consecuencias legales debe existir normativa que resuelva incluyendo la creación de tribunales especializados en tecnología y que serían inclusivos de consecuencias derivadas del uso o actividad de una IA.⁶⁹

VIII.- Se ha documentado ya, en el ámbito de la ciencia y la academia que la IA facilitará la comisión de delitos, si bien, su regulación no va a evitar el potencial peligro, si contribuirá a disminuir el riesgo y determinar la responsabilidad, pero cuando tal regulación NO EXISTE, personas, empresas y gobiernos estamos en completo estado de indefensión y eso es muy grave porque vivimos fuera de todo estado de derecho, por ello, debe regularse porque las amenazas ciberneticas pueden cambiar nuestra vida o privarnos de ella y es necesario que alguien responda por ello.

IX.- Es necesario e importante utilizar el aprendizaje profundo de una IA, pero asegurándonos jurídicamente de que se siga la naturaleza de herramienta que es una IA. Para ello apostamos desde la visión de este trabajo a los aspectos educativos generales y obligatorios, actividades

⁶⁷ Cortés, Gabino, "La sustitución de los abogados por la tecnología", artículo en línea, (11 de julio del 2017) Diario La Opinión [Consultada en enero 18 del 2020], Disponible en: <https://laopinion.com/2017/07/11/la-sustitucion-de-los-abogados-por-la-tecnologia/>

⁶⁸ Motoko, Rich, "Los robots no son salvadores del futuro, tienen sus fallas", artículo en línea (23 de enero de 2020) Panamá América [Consultada en enero 30 del 2020], Disponible en: <https://www.panamaamerica.com.pa/nytimes-internationalweekly/los-robots-no-son-los-salvadores-del-futuro-tienen-sus-fallas-1154695>

⁶⁹ Weizenbaum explica que necesitamos auténticos sentimientos de empatía de las personas en ciertos puestos de lo contrario nos encontraremos alienados, devaluados y frustrados. La inteligencia artificial, representaría una amenaza para la dignidad humana. Weizenbaum, Joseph "Winner of CPSR's Norbert Wiener Award for Professional and Social Responsibility", en línea, (1988) [Consultado en febrero 8 del 2020], Disponible en: <https://web.archive.org/web/20041011131756/http://www.cpsr.org/cpsr/weiz.html>

que pueden resumirse en un “ABC”: “A”: de aprender todo lo posible de ella, su desarrollo y fortaleciendo su aplicación para prevenir y combatir el delito, “B”: de beneficiarse con su potencial y ventajas para cualquier campo del conocimiento en todos los niveles educativos y “C”: de crear conciencia y establecer los límites éticos y jurídicos de su uso indebido.⁷⁰ Lo que puede impactarse positivamente de forma transversal a cualquier campo del conocimiento, que para el momento que nos ocupa, ya tendríamos que estar pensando en el tema de la Ciberseguridad, no solo del derecho penal y la responsabilidad.

X.- Debe atenderse a la recomendación de apostar por la regulación de IA desde el tema de prevención del delito como se estudia desde el Derecho Penal y de la política pública tradicional en México, porque debemos como país, mantenernos actualizados en el desarrollo tecnológico⁷¹ -*eso implica regulación*-, ya que ofrece oportunidades muy sofisticadas para hacer un mal uso del ciberspacio y de la tecnología misma, donde la IA es sin lugar a duda, tecnología que debe ser regulada.

XI.- No debe satanizarse la tecnología, ni temerle o rechazarla, hay que aprender y usarla, ya que ésta no es ni mala ni buena, nació como una herramienta y eso es, al contrario de las personas que la manejan quienes pueden usarla como arma, determinado por su libre albedrío, inexistente en la IA, regular implicaría también establecer pautas éticas que penalicen cualquier uso indebido de una IA, aun cuando “decida” actuar indebidamente, aprovechando también el control sobre ella y contener una posible “rebeldía”, como ha sucedido. En algunos países es posible accionar respuestas del derecho civil o del derecho administrativo, pero no del derecho penal, pues el principio de precaución no puede ser utilizado para integrar normativamente un delito imprudente, en México nada de ello es posible, ni por imprudencia, negligencia o dolo, hay que empezar ya.

⁷⁰ P.e.: identificar si una determinada persona es un criminal, analizando las características de su rostro con un porcentaje de precisión cercano al 90 %, como sucede con la IA conocida como “Emotient”. Darlington, Keith. “Sistemas de inteligencia artificial que gestionan emociones humanas”. Artículo en línea. (13 agosto 2018) [Consultado en diciembre 28 de 2019]. Disponible en: <https://www.bbvaopenmind.com/tecnologia/inteligencia-artificial/sistemas-de-inteligencia-artificial-que-gestionan-emociones-humanas/>

⁷¹ El Convenio de Ciberdelincuencia de Budapest del 2001 establece: “...9 ... el derecho penal debe mantenerse al corriente de estos desarrollos tecnológicos que ofrecen oportunidades muy sofisticadas para hacer un mal uso de las facilidades del ciberspacio ... *Dada la naturaleza transfronteriza de las redes de información, es necesario un esfuerzo internacional concertado para hacer frente a ese uso impropio... además de las medidas de cooperación internacional, se deberían abordar las cuestiones de derecho sustantivo y procesal, así como cuestiones que están estrechamente relacionadas con el uso de la tecnología de la información*”.

XII.- Las posibilidades y acciones jurídicas necesarias, para regular alguna vez la responsabilidad penal de una IA en México, se fundamenta también en la cantidad y variedad de tecnologías emergentes de las cuales el campo jurídico no se ha ocupado y que si bien potencian sus ventas -y la dependencia a ellas-, también lo hacen con los riesgos en el mismo potencial, para tener una idea refiero algunas de las principales tendencias en ciberseguridad para 2021,⁷² que son un foco rojo para el campo jurídico que serán: *actividades de ransomware, botnets, código dañino avanzado, ataques a sistemas de acceso remoto, ataques web, ingeniería social -todas sus modalidades-, ataques contra la cadena de suministro y ataques contra sistemas ciberfísicos*; que se suman a las amenazas existentes del 2020,⁷³ caracterizadas por ser cometidas por agentes de delincuencia informática organizada. Es claro que estamos ante un riesgo latente, urgente y desregulado. Es determinante que los juristas apostemos y trabajemos desde la docencia, investigación, regulación y educación principalmente. Pudiendo resumir el marco jurídico propuesto para su regulación, con el reconocimiento de su personalidad artificial en la Constitución Política del país y la correspondiente inclusión en el apartado de atributos de la personalidad en el Código Civil Federal de definiciones siguientes: identidad jurídica electrónica, persona artificial e identidad artificial como parte de un tercer tipo de persona jurídica; posteriormente, el reconocimiento de su responsabilidad penal -*con sus debidas particularidades, como en el caso de menores e inimputables*-, en el Código Penal Federal, Capítulo I de Reglas generales sobre delitos y responsabilidad, así como en el Capítulo II de Acceso ilícito a sistemas y equipos de informática,

⁷² Centro Criptológico Nacional (ccn-cert). "Ciberamenazas y tendencias edición 2020", documento de análisis, (septiembre 2020), Ministerio de Defensa, España, [Consultado en septiembre 29 del 2020], Disponible en <https://www.ccn-cert.cni.es/informes/informes-ccn-cert-publicos/5377-ccn-cert-ia-13-20-ciberamenazas-y-tendencias-edicion-2020/file.html>

⁷³ Ciberseguridad Industrial, el uso no autorizado o ilegal de datos o información, e minado ilegal de criptomonedas (Cryptojacking), el Cibercrimen como servicio, la Ciberguerra, Ciberataques a infraestructuras críticas, ataques a la privacidad, la IA como punto de ataque, el uso de Machine Learning para ataques automatizados y obtención de información, los retos del IoT, los vehículos autónomos, la Colaboración entre cibercriminales, seguridad en Cloud Computing y Cloud Forense, la Ciberseguridad móvil, los Videojuegos, las amenazas fileless, ataques por drones y la difusión de pornografía infantil en realidad aumentada, sin olvidar las conductas comunes como el phishing, fraudes, fake news, usurpación de identidad, entre otros. Aquí otro ejemplo: Corral, Adyr y Michel, Víctor Hugo. "Narcos' migran a WhatsApp para evadir servicios de inteligencia", nota informativa en línea, (enero 27 del 2020) Milenio 2020 [Consultada en febrero 5 del 2020], Disponible en: <https://www.milenio.com/policia/narcotraficantes-usan-whatsapp-para-evadir-servicios-de-inteligencia>

tipificando diversas conductas de índole informático que pudiera cometer una IA por decisión propia, dentro del incipiente y perfectible capítulo referido que también requiere una actualización profunda. Propuesta que no se desarrolla ya que requerirá de más espacio que el autorizado en este trabajo.

XIII.- Adicionalmente, el Índice Mundial de Ciberseguridad (IMC) de la UTI⁷⁴ para 2018, indica que México de ocupar el lugar 28 bajó al 63 en 2019, lo que representa una grave disminución de su compromiso y atención la ciberseguridad nacional, respecto del resto del mundo, de acuerdo con los cinco pilares de la Agenda sobre Ciberseguridad Global: medidas jurídicas, técnicas, organizativas, capacitación y cooperación, lo que establece las cifras específicas del riesgo para México, al que he aludido en el presente trabajo permanentemente y que en primer lugar considera las de orden jurídico, otra razón más.

XIV.- Un sólido fundamento más para la presente propuesta, se localiza en el trabajo del Parlamento Europeo, que mediante informe emitido en 2015 refiere diversas recomendaciones destinadas a la Comisión sobre normas de Derecho civil sobre robótica (2015/2103(INL)), que consideran las principales líneas de trabajo para el legislador, destacando: La creación de una Agencia Europea de Robótica e Inteligencia Artificial, elaboración de un código de conducta ético base para regular la responsabilidad de los impactos sociales, ambientales y de salud de la robótica y asegurar que operen de acuerdo con las normas legales, de seguridad y éticas pertinentes; promulgar reglas de responsabilidad por los daños causados por los robots, crear un estatuto de persona electrónica, crear un Registro Europeo de los robots inteligentes, la robótica y la inteligencia artificial son descritas como “tecnologías disruptivas” que pueden “transformar vidas y prácticas de trabajo” y afectar al mercado laboral y los niveles de empleo, ya que todo ello eventualmente tendrá un impacto en todas las esferas sociales y globales. Considero viable retomar este trabajo para hacer lo propio, ya que nunca se pasó de la intención de México a adherirse al Convenio de Ciberdelincuencia de Budapest del 2001.

XV.- Debo decir que no todas son buenas noticias, si bien la IA tiene un sinnúmero de beneficios y aplicaciones, también es mucho más que

⁷⁴ Internacional Telecommunications Union (ITU). "Global Cybersecurity Index (GCI)", edición digital, (2018), (p. 92) [Consultado en febrero 12 del 2020], Disponible en: https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2018-PDF-E.pdf

software y hardware con un funcionamiento casi perfecto, al ser una creación humana es susceptible de error, problemas de software, posibilidad de ser vulnerada (mal llamado hackeo) y controlada, por supuesto problemas éticos aún no considerados que la alejan de la imparcialidad, la seguridad y la responsabilidad que son sus tres pilares fundamentales, dos de ellos son características humanas y el tercero –*la seguridad*–, no es absoluta porque lo absoluto no existe y con ello es vulnerable en los todos niveles. Cuando los pilares éticos fundamentales son determinados por instituciones, organizaciones o gobiernos claramente con doble moral y poca credibilidad, siempre será un riesgo adicional para lo cual podríamos estar imitando el ejemplo del Observatorio del impacto social y ético de la inteligencia artificial (odiseIA),⁷⁵ que en España observa, previene y mitiga los desafíos del uso de la inteligencia artificial como oportunidad disruptiva. Lo cual fundamentaría, regularía o evitaría el control de la implementación de políticas dudosas,⁷⁶ por lo que sería ideal en el caso nacional, la participación del modelo multi stakeholder referido.

Argumentos, razones, fundamentos y motivos que justifican y permiten concluir el cumplimiento de los objetivos por un lado y por otro la comprobación hipotética que establece que, efectivamente, la Inteligencia artificial: es la frontera próxima a regular. Aún no se está preparado y el campo jurídico debe evitar cualquier daño o actividad cometida por una Inteligencia Artificial (IA) –*propia (Deep Learning), o ajena no autorizada, (intrusión o hackeo)*–. Es la oportunidad, el momento social y una responsabilidad profesional y personal contribuir a ello, como se estableció en marco jurídico mínimo que se propone.

Fuentes de información:

1. Abogado.Digital. “Primer crimen cometido mediante inteligencia artificial: simulan la voz de un CEO para pedir depósito urgente”, nota informativa jurídica,

⁷⁵ Observatorio del impacto social y ético de la inteligencia artificial (odiseIA), en web, [Consultado en febrero 13 del 2020], Disponible en: <https://www.odiseia.org/>

⁷⁶ Como la establecida por la Casa Blanca en febrero del 2019 cuando lanzó la “Maintaining American Leadership in Artificial Intelligence” (Orden Ejecutiva 13859), cuya finalidad nunca fue realmente clara. En The Technolawgist “Los 10 principios básicos en materia de inteligencia artificial lanzados por la Casa Blanca a las Agencias Federales”, artículo en línea, (enero 20 del 2020) [Consultada en enero 31 del 2010], Disponible en: <https://www.thetechnolawgist.com/2020/01/20/los-10-principios-basicos-en-materia-de-inteligencia-artificial-lanzados-por-la-casa-blanca-a-las-agencias-federales/>

- (agosto 30 del 2019), [Consultada en septiembre 28 del 2020], Disponible en: <https://www.abogado.digital/primer-crimen-cometido-mediante-inteligencia-artificial-simulan-la-voz-del-ceo-para-solicitar-deposito-urgente/>
2. AFP. "Ciberataque a gobierno de Atlanta exige rescate en bitcoins". Nota periodística en línea, El economista, México. (23 de marzo de 2018) [Consultada en noviembre 13 de 2019], Disponible en: <https://www.eleconomista.com.mx/internacionales/Ciberataque-a-gobierno-de-Atlanta-exige-rescate-en-bitcoins-20180323-0042.html>
3. Agencia EFE "Piden a la ONU un tratado contra los robots asesinos", artículo en línea (22 de octubre del 2019) Publimetro, México [Consultada en enero 28 del 2020], Disponible en: <https://www.publimetro.com.mx/mx/destacado-tv/2019/10/22/pide-a-la-onu-un-tratado-contra-los-robots-asesinos.html>
4. Analytics10. Definición de "redes neuronales". Artículo, en línea, s/f, [Consultada en noviembre 29 de 2019], Disponible en: <https://www.analytics10.com/blog/cual-es-la-diferencia-entre-inteligencia-artificial-ai-y-machine-learning-ml/>
5. BBC Mundo. "Tay, la robot racista y xenófoba de Microsoft", nota informativa en web, (26 de marzo del 2016), [Consultada en septiembre 18 del 2020], Disponible en: https://www.bbc.com/mundo/noticias/2016/03/160325_tecnologia_microsoft_tay_bot_adolescente_inteligencia_artificial_racista_xenofoba_lb
6. BLOOMBERG. "Inteligencia artificial de Google causa asombro y preocupación", Nota informativa, en web, Portafolio, El Tiempo, (12 de mayo del 2018), [Consultada en 25 de septiembre del 2020], Disponible en <https://www.portafolio.co/negocios/empresas/sic-ordena-a-google-a-que-cumpla-con-estandares-de-proteccion-de-datos-544294>
7. Boston Children's Hospital, "A first in medical robotics: Autonomous navigation inside the body", en línea, (24 de abril del 2019) EureKalert! [Consultada en noviembre 22 del 2019] Disponible en: https://www.eurekalert.org/pub_releases/2019-04/bch-afi042219.php
8. Cáceres, Enrique. "Inteligencia Artificial, Derecho y E-Justice", (2006) edición en línea, (El proyecto IIJ-CONACYT), Boletín de Derecho Comparado, Año XXXIX, número 116, pp. 593-611. [Consultado en enero 27 del 2020], Disponible en: <https://revistas.juridicas.unam.mx/index.php/derecho-comparado/article/view/3889/4889> The Technolawgist, "Los 10 principios básicos en materia de inteligencia artificial lanzados por la Casa Blanca a las Agencias Federales", artículo en línea, (enero 20 del 2020) [Consultada en enero 31 del 2010], Disponible en: <https://www.thetechnolawgist.com/2020/01/20/los-10-principios-basicos-en-materia-de-inteligencia-artificial-lanzados-por-la-casa-blanca-a-las-agencias-federales/>
9. Calderón, Grecia. "Inteligencia artificial". En Euston96, (en línea), (2019) [Consultada en noviembre 23 del 2019], Disponible en: <https://www.euston96.com/inteligencia-artificial/>

10. Caracuardo. "México uno de los países más ciberatacados en el mundo". Nota informativa, en línea, México. (30 de agosto del 2019) [Consultada en noviembre 14 del 2019], Disponible en: <https://caracuardo.com/noticias/mexico-uno-de-los-paises-mas-ciberatacados-en-el-mundo>
11. Carrasco Sergio. "Diferencia entre machine learning y deep learning". Artículo en línea, Overant (22-Ene-2019), [Consultado en diciembre 3 del 2019], Disponible en <https://www.overant.com/blog/diferencia-entre-machine-learning-y-deep-learning/>
12. Centro Criptológico Nacional (ccn-cert). "Ciberamenazas y tendencias edición 2020", documento de análisis, (15 de septiembre 2020), Ministerio de Defensa, España, [Consultado en septiembre 29 del 2020], Disponible en <https://www.ccn-cert.cni.es/informes/informes-ccn-cert-publicos/5377-ccn-cert-ia-13-20-ciberamenazas-y-tendencias-edicion-2020/file.html>
13. CNBC. "Hot Robot At SXSW Says She Wants To Destroy Humans", video en web, 02:37 mins., a través de El Pulso, (16 de marzo del 2016), [Consultado en setiembre 26 de 2020], Disponible en: https://www.youtube.com/watch?time_continue=12&v=W0_DPi0PmF0&feature=emb_logo
14. Coleman Flynn "A Human Algorithm: how artificial intelligence redifining who are", Ed. Counter Point (2019), 336 p.p.
15. Computer World. "El 70% de las organizaciones están siendo ciberaatacadas", nota informativa en línea. (2017) [Consultada en noviembre 12 del 2019], Disponible en: <https://cso.computerworld.es/tendencias/el-70-de-las-organizaciones-estan-siendo-ciberatacadas>
16. Consejo de Europa, "Convenio sobre la Ciberdelincuencia". (2001), En línea, Budapest [Consultado en noviembre 14 del 2019], Disponible en: <https://rm.coe.int/16802fa403>
17. Contreras, Juan M., "En Coahuila previenen delitos con inteligencia artificial", nota informativa en línea, (8 de abril del 2019) el Sol de Coahuila, México [Consultada en febrero 7 del 2020], Disponible en: <https://www.elsoldemexico.com.mx/republica/justicia/en-coahuila-previenen-delitos-con-inteligencia-artificial-3292176.html>
18. Corral, Adyr y Michel, Victor Hugo, "‘Narcos’ migran a WhatsApp para evadir servicios de inteligencia", nota informativa en línea, (enero 27 del 2020) Milenio 2020[Consultada en febrero 5 del 2020], Disponible en: <https://www.milenio.com/policia/narcotraficantes-usan-whatsapp-para-evadir-servicios-de-inteligencia>
19. Cortés, Gabino, "La sustitución de los abogados por la tecnología", artículo en linea, (11 de julio del 2017) Diario La Opinión [Consultada en enero 18 del 2020], Disponible en: <https://laopinion.com/2017/07/11/la-sustitucion-de-los-abogados-por-la-tecnologia/>
20. Darlington Keith. "Sistemas de inteligencia artificial que gestionan emociones humanas". Artículo en línea. OpenMind BBVA (13 agosto 2018) [Consultado en diciembre 28 de 2019], Disponible en:

21. <https://www.bbvaopenmind.com/tecnologia/inteligencia-artificial/sistemas-de-inteligencia-artificial-que-gestionan-emociones-humanas/>
22. Denoticias, “Inteligencia artificial revienta el fraude del crimen en Silicon Valley”, nota informativa en línea (febrero 9 de 2020) España [Consultada en febrero 10 del 2020], Disponible en: <https://www.denoticias.es/notas/inteligencia-artificial-revienta-el-fraude-del-crimen-en-silicon-valley.html>
23. Derecho Digital, “Inteligencia artificial y Derecho”, artículo en línea (21 marzo, 2019) LetsLaw [Consultada en febrero 11 del 2020], Disponible en: <https://lets-law.es/inteligencia-artificial-y-derecho/>
24. Diario Contraréplica. “Tecnologías que ya pueden identificar emociones humanas”. (23 de septiembre de 2019), México [Consultada en diciembre 16 del 2019], Disponible en: <https://www.contrareplica.mx/nota-Tecnologias-que-ya-pueden-identificar-emociones-humanas201923946>
25. DW, “NASA investiga primer posible delito cometido en el espacio”, nota informativa en línea, (agosto 25 del 2019), [Consultada en diciembre 28 del 2019], Disponible en: <https://www.dw.com/es/nasa-investiga-primer-possible-delito-cometido-en-el-espacio/a-50156616?maca=es-Facebook-sharing>
26. Eitb. “Hackers logran acceder a teléfonos de usuarios de Whatsapp”, nota informativa, en línea. (14/5/2019) [Consultado en noviembre 14 del 2019], Disponible en: <https://www.eitb.eus/es/noticias/tecnologia/detalle/6404592/hackers-acceden-telefonos-usuarios-whatsapp-mayo-2019/>
27. Gañán, Hugo. “Un Tesla autónomo atropella a un robot ruso y se da a la fuga”, nota informativa, (9 de enero del 1019), El Plural, [Consultado en septiembre 27 del 2020], Disponible en; https://www.elplural.com/leequid/omg/un-tesla-autonomo-atropella-a-un-robot-ruso-y-se-da-a-la-fuga_209152102
28. Godó Vertical Media. “¿Qué aportó a la ciencia Alan Turing?”. (en linea), (27 de agosto del 2018). Disponible en: <https://www.lavanguardia.com/historiayvida/historia-contemporanea/20180611/47312986353/que-aporto-a-la-ciencia-alan-turing.html>
29. Guiusto Beltic, Denise. “Países más afectados por el ransomware en Latinoamérica durante 2018”. Welivesecurity, artículo en línea, (enero 4 del 2019) [Consultada en noviembre 14 del 2019] Disponible en: <https://www.welivesecurity.com/la-es/2019/01/04/paises-mas-afectados-ransomware-latinoamerica-durante-2018/>
30. Hevia Andrés. “¿Cuáles son las diferencias entre IA, Machine Learning y Natural Language Processing?”. Artículo en línea, (Nov 13, 2016) [Consultada en diciembre 4 del 2019], Disponible en <https://planetachatbot.com/diferencias-entre-ia-machine-learning-y-natural-language-processing-315650ac3ca2>
- Internacional Telecommunications Union (ITU). “Global Cybersecurity Index (GCI)”, edición digital, (2018) [Consultado en febrero 12 del 2020], Disponible en: https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2018-PDF-E.pdf

31. J P, E. "Los robots, mayores delincuentes en 2040", nota informativa en web, (13 de septiembre del 2016), El Universal, México, [Consultado en septiembre 30 del 2020], Disponible en: <https://www.eluniversal.com.mx/articulo/ciencia-y-salud/tecnologia/2016/09/13/robots-cometeran-mas-delitos-que-seres-humanos-en>
32. Jaimovich, Desirée "Un sistema de inteligencia artificial "identifica las intenciones criminales" para evitar delitos", artículo en línea, (agosto 15 del 2017) Infobae, Argentina [Consultada en febrero 9 del 2020], Disponible en: <https://www.infobae.com/america/tecnico/2017/08/15/un-sistema-de-inteligencia-artificial-identifica-las-intenciones-criminales-para-evitar-delitos/>
33. Jiménez de Luis, Ángel. "Facebook apaga una inteligencia artificial que había inventado su propio idioma", nota informativa en web, El Mundo, España, (26 de julio del 2017), [Consultado en septiembre 25 del 2020], Disponible en: <https://www.elmundo.es/tecnologia/2017/07/28/5979e60646163f5f688b4664.html>
34. Marco, Agustín, "Crisis en Prosegur: despide a su cúpula de ciberseguridad tras el 'hackeo' de sus cuentas", nota informativa en línea, (febrero 2 del 2020) [Consultada en febrero 8 del 2020], Disponible en: https://www.elconfidencial.com/empresas/2020-02-10/prosegur-despide-cupula-de-ciberseguridad-tras-hackeo-cuentas_2446055/
35. Marina José Antonio. "La inteligencia fracasada", Edición impresa, Ed. Anagrama, (2016), ISBN: 978-84-339-7805-9. 176 p.p.
36. Martínez Bahena, Gorety Carolina. "La inteligencia artificial y su aplicación al campo del Derecho". En línea, (S/f) Revista Alegatos, México, Vol. 26, Núm. 82, pp. 827-846 [Consultado en enero 27 del 2020], Disponible en: <http://www.cor-teidh.or.cr/tablas/r30570.pdf>
37. Martínez Marco Daniel. "9 aplicaciones exitosas de la inteligencia artificial para el 2018", edición digital, Grupo extraordinaria (2017) [Consultado en noviembre 17 del 2019], Disponible en: <https://grupoextraordinaria.com/9-aplicaciones-inteligencia-artificial/>
38. Méndez, Fabiola. "El robot es inocente", entrevista a experta Alejandra Morán, (marzo 22 del 2018), UNAM Global, México, [Consultada en septiembre 26 de 2020], Disponible en: <http://www.unamglobal.unam.mx/?p=36083>
39. Menn, Joseph. "Nuevo tipo de programas de inteligencia artificial llevarán delitos informáticos a otro nivel", nota informativa, (agosto 8 del 2018), Reuters, [Consultada en septiembre 27 del 2020], Disponible en: <https://jp.reuters.com/article/tecnologia-ibm-inteligenciaartificial-idLTAkBN1KT1Z0-OUSLI>
40. Minsky, Marvin. "Inteligencia artificial", definición en Escolano Ruiz, Francisco, Cazorla Quevedo, Miguel A. y otros "Inteligencia Artificial: Modelos técnicas y áreas de aplicación", edición digital (2003), Ed. Thomson, [Consultado en noviembre 9 del 2019], Disponible en: https://books.google.com.mx/books?hl=es&lr=&id=_spC6S7UfZgC&oi=fnd&pg=PP1&dq=Inteligencia+artificial&ots=0zDyvW&sa=X&redir_esc=y

- q=tipos+de+inteligencia+artificial&ots=sPmnKDNuBU&sig=URMtRML-1QfTLD4Pt9AqyIzJTCE#v=onepage&tq=tipos%20de%20inteligencia%20artificial&t=false
41. Mora Castro José Luis. “La evolución de la Inteligencia Artificial”, 2016. Revista digital Mundo Contact, [Consultada en noviembre 7 del 2019], Disponible en: <https://mundocontact.com/la-evolucion-de-la-inteligencia-artificial/>
42. Motoko, Rich “Los robots no son salvadores del futuro, tienen sus fallas”, artículo en línea (23 de enero de 2020) Panamá América [Consultada en enero 30 del 2020], Disponible en: <https://www.panamaamerica.com.pa/nytimesinternationalweekly/los-robots-no-son-los-salvadores-del-futuro-tienen-sus-fallas-1154695>
43. Noriega, Samuel, “Inteligencia Artificial para predecir el crimen en Hermosillo”, nota informativa en línea, (23/12/2019) Expreso [Consultada en febrero 9 de 2020], Disponible en: <https://www.expreso.com.mx/seccion/expresion/e-comunidad/139486-inteligencia-artificial-para-predecir-el-crimen-en-hermosillo.html>
44. Observatorio del impacto social y ético de la inteligencia artificial (odiseIA), en web, [Consultado en febrero 13 del 2020], Disponible en: <https://www.odiseia.org/>
45. Olivares Joaquín. “Mi cirujano, el Dr. Robot”. “The Conversation”. Academic rigor, journalistic flair. Artículo digital, enero 29 del 2020. Bo [Consultada en: 31 de enero del 2020] Disponible: <https://theconversation.com/mi-cirujano-el-dr-robot-130812>
46. Parlamento Europeo “Recomendaciones destinadas a la Comisión sobre normas de Derecho civil sobre robótica”, 2015/2103(INL), en línea, [Consultadas en febrero 10 del 2020], Disponibles en: http://www.europarl.europa.eu/doceo/document/A-8-2017-0005_ES.html
47. Perea González, Álvaro. “Inteligencia artificial y proceso judicial: una revolución que se aproxima”, artículo de opinión, (1º abril del 2020), Expansión, [Consultado en septiembre 27 del 2020], Disponible en: <https://www.expansion.com/juridico/opinion/2020/04/01/5e846ab8468aebd5528b45a9.html>
48. Periódico Correo. “Ciberatacan a gobiernos, universidades y partidos”. Nota informativa en línea. (noviembre 3 del 2017) [Consultado en noviembre 13 del 2019], Disponible en: <https://periodicocorreo.com.mx/ciberatacan-gobiernos-universidades-partidos/>
49. Quirós Jaime “Las profesiones que caducarán esta década”, enero 2 del 2020, artículo en línea, [Consultada en enero 16 del 2020], Disponible en: <https://es-us.finanzzas.yahoo.com/noticias/profesiones-caducaran-decada-fecha-154738160.html>
50. RAE. “honestidad y honesto”, definiciones en línea, [Consultado en febrero 3 del 2020] Disponible en: <https://dle.rae.es/?w=honesto>

51. Real Academia Española. "Libre albedrío", definición en línea, (2019), [Consultada en noviembre 29 del 2019], Disponible en: <https://dle.rae.es/albedrio#EJ7Tb7c>
52. Rebeca. "EL LADO OSCURO DE LA INTELIGENCIA ARTIFICIAL", blog a través de next.u, (s/f), [Consultado en septiembre 27 del 2020], Disponible en: <https://www.nextu.com/blog/lado-oscuro-inteligencia-artificial/>
53. Reuters, "Nuevo tipo de programas de inteligencia artificial llevarán ciberdelitos a otro nivel". En línea (8 de agosto del 2018) [Consultada en enero 15 del 2010], Disponible en: <https://www.elfinanciero.com.mx/tech/nuevo-tipo-de-programas-de-inteligencia-artificial-llevaran-ciberdelitos-a-otro-nivel>
54. Ribas, Ester, "Predicciones y tendencias en ciberseguridad para 2020". En línea, (noviembre 25 del 2019) IEBF [Consultado en febrero 13 del 2020], Disponible en: <https://www.iebschool.com/blog/tendencias-ciberseguridad-business-tech/>
55. Rius, Mayté, "La policía británica quiere usar IA para predecir delitos antes de que ocurran". Nota informativa en línea (diciembre 2 del 2018) La Vanguardia, Barcelona, [Consultada en enero 26 del 2020], Disponible en: <https://www.lavanguardia.com/tecnologia/20181202/453268636098/policia-britanica-uso-inteligencia-artificial-delitos-crimenes-delincuencia.html>
56. Ruiz Fernández, Alicia. "5 riesgos de la Inteligencia Artificial que pueden hacerla peligrosa", artículo en web, (19 de noviembre del 2018), Ticbeat, [Consultada en septiembre 29 de 2020], Disponible en; <https://www.ticbeat.com/tecnologias/5-riesgos-de-la-inteligencia-artificial-que-pueden-hacerla-peligrosa/>
57. Tecnología, Negocios Estrategia. "CIBERCRIMINALES USARÁN IA PARA COMETER DELITOS". (febrero 7 del 2018) Circulo tne [Consultada en enero 4 del 2020], Disponible en: <https://circulotne.com/cibercriminales-usaran-ia-para-cometer-delitos.html>
58. Ugade, Rafael. "Detectan con IA al coronavirus antes de hacerse público", artículo en Revista digital Mundo Contact, sección tecnología. (enero 29 del 2020), Disponible en: <https://mundocontact.com/detectan-con-ia-el-coronavirus-antes-de-hacerse-publico/>
59. Ugalde, Rafael, "La inteligencia artificial debe ser regulada.- Sundar Pichai", artículo en línea, (enero 21 del 2020) [Consultado en febrero 13 del 2020], Disponible en: <https://mundocontact.com/la-inteligencia-artificial-debe-ser-regulada-sundar-pichai/>
60. Ugalde, Rafael. "Inteligencia artificial provocará guerra mundial.- Elon Musk", artículo en línea, (septiembre 3 del 2017) Mundo Contact [Consultado en enero 30 del 2020], Disponible en; <https://mundocontact.com/inteligencia-artificial-provocara-guerra-mundial-elon-musk/>
61. UIT Rec. UIT-T X.1205. "Ciberentorno", en línea. descarga directa, 66 p.p., (2008). [Consultado en noviembre 12 del 2019], Disponible en: <https://www.itu.int/rec/T-REC-X.1205-200804-I/es>

62. University College London. “‘Deepfakes’ clasificada como la amenaza de crimen de IA más grave”, artículo en web, (agosto 4 del 2020), Universidad College, Londres, [Consultado en septiembre 26 de 2020], Disponible en <https://www.ucl.ac.uk/news/2020/aug/deepfakes-ranked-most-serious-ai-crime-threat>
63. Valls Prieto, Javier. “El reto de una robótica e inteligencia artificial honesta con las personas”, artículo en línea, (octubre 27 del 2019) The Conversation Academic rigor, journalistic flair [Consultado en febrero 4 del 2020], Disponible en <https://theconversation.com/el-reto-de-una-robotica-e-inteligencia-artificial-honesta-con-las-personas-125034>
64. Weizenbaum, Joseph “Winner of CPSR’s Norbert Wiener Award for Professional and Social Responsibility”, en línea, (1988) [Consultado en febrero 8 del 2020], Disponible en: <https://web.archive.org/web/20041011131756/http://www.cpsr.org/cpsr/weiz.html>
65. Yang Yuan, Yang Yingzhi, “¿Puede la inteligencia artificial predecir delitos?”, artículo en línea, (agosto 1º del 2017) Expansión, México [Consultado en enero 29 del 2020] Disponible en: <https://www.expansion.com/economia-digital/innovacion/2017/08/01/597f7ea9ca4741cb738b45cc.html>