Apuntes sobre la Orden Ejecutiva del Presidente Biden para el desarrollo y uso seguro y confiable de la Inteligencia Artificial

*****Por Sebastián Heredia Querro[1]

1. Introducción. Integración con otras normas

El 30 de Octubre de 2023, la Administración Biden firmó la Orden Ejecutiva Nº 14.110, publicada en el Boletín Oficial el 1 de Noviembre de 2023[2], fijando la posición y la visión del Gobierno Federal de EE.UU para el *desarrollo y uso seguro y confiable de la Inteligencia Artificial* (en adelante, la **OE**).

En tan solo trece artículos, la OE regula importantes aspectos asociados al desarrollo tecnológico de la Inteligencia Artificial (en adelante, **IA**)[3], a saber: Art. 1: *Propósito de la OE*; Art. 2: *Política y Principios*; Art. 3: *Definiciones*; Art. 4: *Asegurando la Seguridad y Confiabilidad de la Tecnología IA*; Art. 5: *Promoción de la Innovación y de la Competencia*; Art. 6: *Apoyo a los Trabajadores*; Art. 7: *Avanzando en Equidad y Derechos Civiles*; Art. 8: *Protegiendo a los Consumidores, Pacientes, Pasajeros y Estudiantes*; Art. 9: *Protegiendo la Privacidad*; Art. 10: *Promoviendo el uso de la IA por parte del Gobierno Federal*; Art. 11: *Fortaleciendo el liderazgo norteamericano en el extranjero*; Art. 12: *Implementación*; y Art. 13: *Normas Generales*.

Antes de analizar los puntos sobresalientes de la OE, debe tenerse en cuenta que la OE debe entenderse en vinculación con normas, marcos y posicionamientos preexistentes -que no se analizarán el presente, por exceder su marco-, tales como: (i) el Anteproyecto para una Declaración de Derechos de la IA[4]; (ii) el Marco de Gestión de Riesgos de la IA[5]; (iii) la Orden Ejecutiva para avanzar la equidad racial y el apoyo a las comunidades desatendidas a través del gobierno federal[6]; (iv) la Ley de Datos Gubernamentales Abiertos, Públicos, Electrónicos y Necesarios[7]; y, principalmente, (v) la Ley de Promoción de la IA[8]. También debe tenerse presente el avance regulatorio de la Unión Europea en la materia[9].

---

[1] *Sebastián Heredia Querro es Abogado (UCC), Magíster en Derecho Empresario (U. Austral) y Magíster en Finanzas con orientación Fintech (ESADE). Es cofundador de Wootic, una software factory boutique enfocada en DLTs y machine learning.*

[2] Disponible al 22/01/24 en https://www.govinfo.gov/content/pkg/FR-2023-11-01/pdf/2023-24283.pdf

[3] Para una clarificación de la terminología empleada y de los subcampos de investigación de la IA, véase Sebastián Heredia Querro, *Smart Contracts: Qué son, para qué sirven y para qué no servirán?* 1ra. Ed., Cathedra Jurídica, 2020, Bs. As, disponible *on line* gratuitamente al 23/01/24 en https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3875645, apartado 3.5.1.10.4.

[4] Confr. https://www.whitehouse.gov/ostp/ai-bill-of-rights/

[5] Confr. https://www.nist.gov/itl/ai-risk-management-framework

[6] Confr. https://www.whitehouse.gov/briefing-room/presidential-actions/2023/02/16/executive-order-on-further-advancing-racial-equity-and-support-for-underserved-communities-through-the-federal-government/

[7] Confr. https://www.congress.gov/bill/115th-congress/house-bill/1770

[8] Confr. https://www.congress.gov/bill/117th-congress/senate-bill/1353/text

[9] Para un análisis del marco regulatorio europeo de la IA, véase Sebastián Heredia Querro, *Apuntes sobre el nuevo Reglamento de Inteligencia Artificial de la Unión Europea,* en Diario La Ley del 29/12/2023, p. 1-4, disponible en https://biblioteca.csjn.gov.ar/cgi-bin/koha/opac-detail.pl?biblionumber=432298&query_desc=an%2Cphr%3A%201309

2. Principios y Política sobre IA

En primer término, el Art. 2 afirma que la OE reconoce tanto el extraordinario potencial de la IA como la urgencia de regular su desarrollo debido a su rápida evolución, pero busca especialmente mitigar los riesgos que la IA puede generar, como el fraude, la discriminación, los sesgos, la desinformación, la afectación a los trabajadores, limitar la competencia y hasta representar un peligro para la seguridad nacional, afirmando que esta tarea requiere un esfuerzo amplio, que involucra al Gobierno, el sector privado, la Academia y la sociedad civil.

En materia de principios que guiarán la política federal, la OE propone ocho:

(1) ***La IA debe ser segura y confiable***: esto requiere tests y evaluaciones confiables de los sistemas de IA, tanto antes de que sean puestos en funcionamiento como después mediante el monitoreo constante, especialmente para mitigar riesgos en áreas como biotecnología, ciberseguridad, infraestructuras críticas y seguridad nacional. En esta línea, el Gobierno Federal colaborará con la construcción de mecanismos que permitan clasificar el origen de los contenidos, para que los usuarios puedan saber cuándo ha sido creado con IA;

(2) ***Promover la innovación responsable, la competencia y la colaboración***: para liderar en IA, el Gobierno Federal promoverá inversiones en educación, I+D, entrenamiento y desarrollo de capacidades de IA, incluyendo la atracción de talento extranjero, y teniendo en cuenta cuestiones de propiedad intelectual para proteger a los creadores, cuidando la competencia en el mercado de IA, para que los emprendedores y las PyMEs puedan seguir innovando. A tal fin, se atacará la colusión y el abuso de posición dominante[10] en materia de semiconductores, poder de cómputo, almacenamiento en la nube y las *desventajas de datos* que afecten a los competidores;

(3) ***Apoyar a los trabajadores***: el desarrollo y uso responsables de la IA requiere adaptar los trabajos, mediante mucho entrenamientos y mucha educación, para que las nuevas oportunidades laborales que crea la IA sean accesibles para todos, velando porque el uso de la IA en el ámbito laboral no cercene los derechos de los trabajadores ni provoque fuertes disrupciones en el mercado laboral. Los sindicatos, los educadores, los empresarios y los trabajadores, deben velar por un desarrollo de la IA que mejore la vida de los trabajadores;

(4) ***Promover la equidad y los derechos civiles***: la IA no puede ser usada para agravar la situación de quienes ya no tienen iguales oportunidades. Ya se sabe cuál es el efecto dañino de los sesgos, y cómo la IA puede reproducir y aumentar las inequidades preexistentes, con lo cual de manera coordinada con otras normas federales, la OE promoverá evaluaciones técnicas robustas, supervisión cuidadosa, el involucramiento de las comunidades afectadas y una regulación rigurosa;

(5) ***Defender a los usuarios y consumidores de la IA***: las nuevas tecnologías no eximen a sus proveedores de sus obligaciones legales en materia de defensa del consumidor, especialmente en materias como salud, servicios financieros, educación, acceso a la vivienda,

[10] Confr. Art. 2.(b).

acceso a la Justicia, y transporte. Además, el Gobierno Federal buscará *elevar la calidad de los bienes y servicios basados en IA, bajar sus precios o ampliar la oferta de los mismos*;

(6) ***Proteger la privacidad***: la IA facilita la vigilancia de las personas, tratando información sensible sobre su identidad, ubicación, hábitos y deseos, lo que implica que los datos personales puedan ser usados, incluso expuestos. Se promoverán las tecnologías que aumentan la privacidad (i.e. *Privacy-Enhancing Technologies, PET*) cuando sea posible y se asegurará que la recolección, uso y retención de datos ocurran legalmente;

(7) ***Promover el uso de la IA por parte del Gobierno Federal***: se buscará atraer talento y desarrollar nuevos profesionales orientados a los servicios públicos que utilizan IA, en todos los ámbitos necesarios -tecnología, regulación, compras públicas, management- y se facilitará la forma de contratación de estos profesionales, buscando modernizar la infraestructura tecnológica del Gobierno Federal; y

(8) ***Promover un marco de gobernanza global para la IA****:* la OE afirma la vocación de liderazgo de EE.UU en previas eras de la disrupción tecnológica, y propone alianzas para desarrollar un marco de gobernanza para la IA que gestione adecuadamente sus riesgos y permita capturar los beneficios de la IA y no replicar ni aumentar la inequidad, ni afectar los derechos civiles de los ciudadanos.

3. Definiciones de la OE

El Art. 3 contiene 33 definiciones, entre las que resaltan las siguientes:

(1) *Inteligencia Artificial o IA*: un sistema basado en máquina que puede, para un conjunto determinado de objetivos definidos por humanos, hacer *predicciones, recomendaciones o decisiones que influyen en entornos reales o virtuales*. Los sistemas de IA utilizan entradas de máquinas y humanos para percibir entornos reales y virtuales; abstraer dichas percepciones en modelos mediante análisis de forma automatizada; y utilizar la inferencia de modelos para formular opciones de información o acción;

(2) *Modelo de IA*: significa un componente de un sistema de información que implementa tecnología de IA y utiliza técnicas computacionales, estadísticas o de *aprendizaje automático*[11] para producir resultados a partir de un conjunto determinado de entradas;

(3) *Equipos rojos de IA*: significa un esfuerzo de prueba estructurado para encontrar fallas y vulnerabilidades en un sistema de IA, en un entorno controlado y en colaboración con desarrolladores de IA. La formación de equipos rojos de IA suele ser realizada por equipos dedicados que adoptan métodos contradictorios para identificar fallas y vulnerabilidades, como resultados dañinos o discriminatorios de un sistema de IA, comportamientos imprevistos o indeseables del sistema, limitaciones o riesgos potenciales asociados con el mal uso del sistema;

(4) *Sistema de IA*: significa cualquier sistema de datos, software, hardware, aplicación, herramienta o utilidad que funcione total o parcialmente utilizando IA;

(5) *Información comercialmente disponible:* significa cualquier información o datos sobre un individuo o grupo de individuos, incluido el dispositivo o la ubicación de un individuo, que se pone a disposición u puede obtenerse y venderse, alquilarse o otorgarse licencia al público en general o a entidades gubernamentales o no gubernamentales;

[11] Para mayores precisiones sobre qué es el Machine Learning y sus distintos diseños, véase supra nota 3.

(6) *Previsión de Delitos*: significa el uso de técnicas analíticas para intentar predecir delitos futuros o información relacionada con el delito. Puede incluir predicciones generadas por máquinas que utilizan algoritmos para analizar grandes volúmenes de datos, así como otras predicciones que se generan sin máquinas y basadas en estadísticas, como las estadísticas históricas de delitos;

(7) *Tecnologías críticas y emergentes* significa aquellas tecnologías enumeradas por el Consejo Nacional de Ciencia y Tecnología (NSTC)[12], y sus actualizaciones;

(8) *Infraestructura Crítica:* tiene el significado establecido en la sección 1016(e) de la Ley USA PATRIOT de 2001, 42 U.S.C. 5195c(e)[13];

(9) *Garantía de privacidad diferencial*: significa protecciones que permiten que se comparta información sobre un grupo al tiempo que se limita demostrablemente el acceso, uso o divulgación indebidos de información personal sobre entidades particulares;

(10) *Modelo básico de doble uso*: significa un modelo de IA que se entrena con datos amplios; generalmente utiliza la autosupervisión; contiene al menos decenas de miles de millones de parámetros; es aplicable en una amplia gama de contextos; y exhibe altos niveles de desempeño en tareas que representan un riesgo grave para la seguridad, la seguridad económica nacional, la salud o seguridad pública nacional, por: (i) reducir sustancialmente la barrera de entrada para que los no expertos diseñen, sinteticen, adquieran o utilicen armas químicas, biológicas, radiológicas o nucleares; (ii) permitir poderosas operaciones cibernéticas ofensivas mediante el descubrimiento y la explotación automatizados de vulnerabilidades contra una amplia gama de posibles objetivos de ciberataques; o (iii) permitir la evasión del control o supervisión humanos mediante el engaño o la ofuscación. Los modelos cumplen con esta definición *incluso si se les proporciona a los usuarios finales salvaguardas técnicas que intentan evitar que los usuarios aprovechen las capacidades inseguras relevantes*;

(11) *IA generativa*: significa la clase de modelos de IA que emulan la estructura y las características de los datos de entrada para generar contenido sintético derivado. Esto puede incluir imágenes, videos, audio, texto y otro contenido digital;

(12) *Aprendizaje automático*: significa un conjunto de técnicas que se pueden utilizar para entrenar algoritmos de IA para mejorar el rendimiento en una tarea basada en datos;

(13) *Tecnología de mejora de la privacidad (PET)*: significa cualquier solución de software o hardware, proceso técnico, técnica u otro medio tecnológico para mitigar los riesgos de privacidad que surgen del procesamiento de datos, incluso mejorando la previsibilidad, la capacidad de administración, la disociabilidad, el almacenamiento, la seguridad y la confidencialidad. Estos medios tecnológicos pueden incluir computación multipartita segura, cifrado homomórfico, pruebas de conocimiento cero (ZKP), aprendizaje federado, enclaves seguros, privacidad diferencial y herramientas de generación de datos sintéticos;

(14) *Contenido sintético:* significa información, como imágenes, videos, clips de audio y texto, que ha sido modificada o generada por algoritmos, incluida la IA;

(15) *Banco de pruebas*: significa una instalación o mecanismo equipado para realizar pruebas rigurosas, transparentes y replicables de herramientas y tecnologías, incluidas la IA y

[12] Confr. https://www.whitehouse.gov/wp-content/uploads/2022/02/02-2022-Critical-and-Emerging-Technologies-List-Update.pdf

[13] Confr. https://www.congress.gov/107/plaws/publ56/PLAW-107publ56.htm

los PET, para ayudar a evaluar la funcionalidad, usabilidad y rendimiento de esas herramientas o tecnologías y

(16) *Marca de agua*: significa el acto de incrustar información, que generalmente es difícil de eliminar, en productos creados por IA (incluidos productos como fotos, videos, clips de audio o texto) con el fin de verificar la autenticidad. del producto o de la identidad o características de su procedencia, modificaciones o transporte.

4. Directrices y Buenas Prácticas para el desarrollo seguro y confiable de la IA

El Art. 4 de la OE es el más extenso y medular: dividido en 8 apartados, llama a la acción a múltiples agencias y organismos del Gobierno Federal en los ámbitos de sus competencias, con un foco especial en seguridad y confiabilidad de los sistemas de IA, especialmente para aquéllos utilizados por el Gobierno Federal en infraestructuras críticas.

Así, el primer apartado del Art. 4, OE convoca[14] a la Secretaría de Comercio, al NIST (i.e. *National Institute of Standards and Technology*), al Secretaría del Tesoro, a la Secretaría de Energía, a la Secretaría de Defensa, al Fiscal General, al Director Nacional de Inteligencia y a la Secretaría de Seguridad Interior, según la materia, a desarrollar directrices y buenas prácticas para promover el consenso de la industria sobre estándares comunes de desarrollo de la IA, incluyendo marcos para (a) evaluar la gestión de riesgos, (b) el desarrollo seguro de software en materia para la IA generativa y para modelos de doble uso, (c) evaluar y auditar los usos y riesgos de la IA, especialmente en materia de energía, ciberseguridad y bioseguridad con foco en *PETs*, y (d) conformar equipos rojos para testear el despliegue de casos de uso y crear bancos de pruebas en el ámbito de la Secretaría de Energía, con foco en amenazas o peligros nucleares y de no proliferación de armas nucleares, biológicas y químicas, y riesgos para infraestructuras críticas y de seguridad energética. Se instruye a la Secretaría de Energía a trabajar con la Academia, laboratorios de IA, la sociedad civil y terceros evaluadores interesados.

El segundo y el tercer apartados del Art. 4, OE hacen foco en cuestiones de seguridad interior, defensa y las infraestructuras críticas. A tal fin, encarga a la Secretaría de Comercio que exija[15] a las empresas que desarrollen posibles modelos de doble uso para el Gobierno Federal que: (a) informen cualquier actividad en curso o planificada relacionada con la capacitación, el desarrollo o la producción de modelos básicos de doble uso, incluyendo los pesos relativos al modelo, y detallando las protecciones físicas y de ciberseguridad tomadas; (b) informen los

---

[14] Se fijan plazos que van desde los 45, 90, 120, 150, 180, 240, 270, 365 y hasta los 540 días posteriores a la OE para presentar los informes que se solicitan.

[15] Para una visión crítica de este deber de información al Gobierno, véase MIT Technology Review, Tate Ryan-Mosley y Melissa Heikkilä*, Three things to know about the White House's executive order on AI.* Se critica en esta pieza que la OE exige que todas las empresas que desarrollen nuevos modelos de IA cuyo tamaño computacional exceda un cierto umbral notifiquen al gobierno federal cuando entrenen el sistema y luego compartan los resultados de las pruebas de seguridad de acuerdo con la ***Ley de Producción de Defensa***. Esta ley se ha utilizado tradicionalmente para intervenir en la producción comercial en tiempos de guerra o emergencias nacionales como la pandemia de covid-19, por lo que se trata de una forma inusual de impulsar regulaciones. Un portavoz de la Casa Blanca dice que este mandato será ejecutable y se aplicará a todos los futuros modelos comerciales de IA en los EE. UU., pero probablemente no se aplicará a los modelos de IA que ya se han lanzado. El umbral se establece en un punto en el que todos los principales modelos de IA que podrían plantear riesgos "para la seguridad nacional, la seguridad económica nacional o la salud y seguridad públicas nacionales" probablemente entren dentro de la orden, según la hoja informativa de la Casa Blanca.

resultados de desempeño y performance de cualquier modelo de base de uso dual desarrollado, junto con las pruebas relevantes del equipo rojo de IA, y una descripción de cualquier medida tomada para cumplir los objetivos de seguridad; (c) informen cuando *adquieran, desarrollen o posean* un potencial clúster informático a gran escala[16], informando existencia y ubicación y el monto total potencia de cálculo disponible; y (d) informen sobre cualquier modelo que haya sido entrenado utilizando una cantidad de potencia informática relevante[17], o que posea un clúster informático que tenga un conjunto de máquinas ubicadas físicamente en un único centro de datos, conectadas mediante una red de centros de datos de más de 100 Gbit/s y que tenga una capacidad informática máxima teórica de 10^{20} operaciones de números enteros o de punto flotante por segundo para entrenar IA.

Por otro lado, el Art. 4 EO también encomienda[18] a la Secretaría de Comercio que proponga una regulación que: (a) requiera a los proveedores de Infraestructura como Servicio de EE.UU. que presenten un informe cuando una persona extranjera realice transacciones con ese proveedor para entrenar un modelo de IA de gran tamaño con capacidades potenciales que podrían usarse en actividades cibernéticas maliciosas, (b) salvo excepciones aplicables, que prohíba a cualquier revendedor extranjero ofrecer esos productos, a menos que el revendedor extranjero presente antes un informe con la información que exija el Secretario de Comercio, identificando al cliente, documentando la forma de pago, incluyendo *wallets* criptográficas, y la forma de limitar el acceso a terceros no autorizados, y (c) determine el conjunto de condiciones técnicas para que un modelo de IA grande tenga capacidades potenciales que puedan usarse en actividades cibernéticas maliciosas: se considerará que un modelo tiene capacidades potenciales que podrían usarse en actividades cibernéticas maliciosas si requiere una cantidad de potencia informática superior a 10^{20}[19]

Además, la OE solicita informes a múltiples áreas del Gobierno Federal sobre riesgos intersectoriales potenciales relacionados con el uso de la IA en los sectores de infraestructura críticos, junto con planes de mitigación de los riesgos que se detecten. Específicamente pide al Secretario del Tesoro un informe respecto de las mejores prácticas para que las instituciones financieras gestionen de manera eficiente los riesgos de ciberseguridad específicos de la IA.

Dispone también el Art. 4 que el Gobierno Federal incorpore el *Marco de Gestión de Riesgos de la IA* desarrollado por el NIST[20] para su uso por parte de propietarios y operadores de infraestructuras críticas, y ordena al Secretario de Seguridad Nacional establecer una *Junta de Seguridad de Inteligencia Artificial* como comité asesor, donde se incluirán expertos en IA del sector privado, del mundo académico y del gobierno, proporcionarán al Secretario de Seguridad

---

[16] Hasta tanto las Secretarías de Comercio, Estado, Defensa, Energía y el Director Nacional de Inteligencia precisen los aspectos más técnicos, se considera que un cluster informático debe ser reportado si permite entrenar modelos con un poder de cómputo superior a la 10^{26}, o si usan secuencias de datos biológicos con un poder de cómputo superior a 10^{23}, o si es un conjunto de máquinas con más de Gbit/s y con capacidad de cómputo de 10^{20} o FLOPS para entrenar modelos de IA. Para entender qué es FLOPS, véase FLOPSWikipediahttps://en.wikipedia.org › wiki › F…

[17] Básicamente, según los mismos parámetros de poder computacional de la nota anterior.

[18] Plazo 90 días

[19] Básicamente, según los mismos parámetros de poder computacional descriptos en la nota 7.

[20] Confr. https://www.nist.gov/publications/artificial-intelligence-risk-management-framework-ai-rmf-10

Nacional y a la comunidad de infraestructura crítica del Gobierno federal asesoramiento, información o recomendaciones para mejorar la seguridad, la resiliencia y la respuesta a incidentes relacionados con el uso de IA en infraestructuras críticas. También pide a los Secretarios de Defensa y de Seguridad Interior que desarrollen en sus ámbitos de competencia planes para realizar y completar un *proyecto piloto operativo* para identificar, desarrollar, probar, evaluar e implementar capacidades de IA, como modelos de lenguaje grande o LLMs, para ayudar en el descubrimiento y remediación de vulnerabilidades en software, sistemas y redes críticos del Gobierno de los Estados Unidos, y presentar sendos informes con los resultados de las acciones tomadas, describiendo cualquier vulnerabilidad encontrada y solucionada y cualquier lección aprendida sobre cómo identificar, desarrollar, probar, evaluar e implementar capacidades de IA de manera efectiva para la ciberdefensa.

El cuarto apartado del Art. 4 de la OE aborda los riesgos del uso de la IA para desarrollar armas químicas, biológicas, radiológicas o nucleares, aunque con especial foco en armas biológicas. Especialmente, la OE pide informes a las áreas del Gobierno Federal sobre el uso potencial de la IA para el desarrollo o producción de éstas amenazas, pero también se pide *evaluar su uso para contrarrestar estas amenazas*, debiendo consultar con expertos en cuestiones de IA, laboratorios privados de IA, instituciones académicas y evaluadores de modelos externos, y en general, tener más información sobre cómo la IA puede aumentar los riesgos de bioseguridad, incluidos los riesgos de los modelos generativos de IA entrenados en datos biológicos, y cómo mitigar estos riesgos. Además, los informes que se solicitan deben permitir considerar las implicaciones para la seguridad nacional del uso de datos y conjuntos de datos asociados con patógenos y estudios ómicos para el entrenamiento de modelos generativos de IA, incluyendo *data sets* financiados directa o indirectamente por el Gobierno Federal y recomendar cómo mitigar los riesgos relacionados con el uso de estos datos y conjuntos de datos.

Nótese que la OE hace especial foco en la biología sintética. Así, pide varios informes que deben mencionar las oportunidades de la IA aplicada a la biología sintética, evaluando cómo hacer para *reducir el riesgo de uso indebido de ácidos nucleicos sintéticos*, y mejorar las medidas de bioseguridad para la industria de la síntesis de ácidos nucleicos. Para reducir el riesgo de uso indebido de ácidos nucleicos sintéticos, se propone que crear un marco que defina criterios y *mecanismos para la identificación continua de secuencias biológicas que podrían representar un riesgo para la seguridad nacional*, para lo cual las autoridades competentes deben acordar -con la industria, las partes interesadas y los proveedores de secuencias de ácidos nucleicos sintéticos-: especificaciones para la detección eficaz de la obtención de síntesis de ácidos nucleicos; mejores prácticas y controles de seguridad y acceso para gestionar bases de datos de secuencias de interés; guías técnicas de implementación para una detección efectiva; mecanismos para la identificación continua de secuencias biológicas que podrían usarse contra la seguridad nacional, y los criterios para identificar a los clientes y compradores (KYC) de secuencias biológicas y mecanismos de evaluación de conformidad. Finalmente, se pone mucho foco en el diseño de mecanismos sectoriales que permitan detectar la adquisición de ácidos nucleicos sintéticos, condicionando todo fondeo federal al certificado de cumplimiento del marco sectorial que será implementado como consecuencia de la EO.

El quinto apartado del Art. 4 aborda los contenidos sintéticos, es decir, aquéllos generados con IA: se encarga un informe describiendo los estándares, herramientas, métodos y prácticas existentes y potenciales usados para autenticar el contenido y rastrear su procedencia; formas de etiquetar contenido sintético, como con el uso de marcas de agua; formas de detectar contenido sintético; y para impedir que la IA generativa produzca material de abuso sexual infantil o produzca imágenes íntimas no consensuadas de individuos reales y para auditar y mantener contenidos sintéticos. Encomienda a la Secretaría de Comercio generar directrices sobre las herramientas y prácticas de autenticación de contenido y detección de contenido sintético, incluyendo una guía para fortalecer la confianza pública en la integridad del contenido digital oficial del gobierno de los Estados Unidos, y para etiquetar y autenticar dicho contenido que producen o publican.

El sexto apartado del Art. 4 de la OE aborda específicamente los modelos de de doble uso, y encarga informes al SubSecretario de Comercio para Comunicaciones e Información solicitando aportes del sector privado, la academia, la sociedad civil y otras partes interesadas, con foco en los riesgos potenciales, beneficios, otras implicaciones y enfoques normativos y regulatorios apropiados para modelos de doble uso.

El séptimo apartado del Art. 4 busca mejorar el acceso a los datos públicos y gestionar los riesgos de seguridad. A tal fin, se encomienda al Consejo del Director de Datos, en consulta con el Secretario de Defensa, de Comercio, de Energía, de Seguridad Nacional y el Director de Inteligencia Nacional, desarrollar pautas para realizar revisiones de seguridad para identificar y gestionar los *riesgos potenciales de seguridad de la divulgación de datos federales* que podrían ayudar en el desarrollo de armas QBRN y de capacidades cibernéticas ofensivas autónomas, y *dispone realizar una* ***revisión de seguridad de todos los activos de datos en el inventario de datos integral***. Finalmente, el apartado 8 del Art. 4 de la OE dispone que varias agencias deben desarrollar una propuesta de *Memorando de Seguridad Nacional sobre IA* para el Presidente, con foco en la gobernanza de la IA utilizada como componente de un sistema de seguridad nacional, o con fines militares y de inteligencia, dando orientación al Departamento de Defensa, a otras agencias relevantes y a la comunidad de inteligencia sobre la adopción continua de capacidades de IA para la seguridad nacional y dirigir acciones para abordar el uso potencial de sistemas de IA por parte de adversarios.

5. Promoción de la Innovación y la Competencia

El Art. 5 hace foco, por un lado, en cómo atraer más talento digital calificado a EE.UU. Dispone, por un lado, agilizar los tiempos de procesamiento de peticiones de visa para los no ciudadanos que buscan trabajar, estudiar o realizar investigaciones en IA u otras tecnologías críticas y emergentes, y facilitar la disponibilidad continua de turnos para visas en un volumen suficiente. Además, se instruye al Secretario de Estado para que reglamente nuevos criterios para designar países y habilidades en la *Lista de Habilidades para Visitantes de Intercambio del Departamento de Estado*; debe implementar un programa de renovación de visa nacional para facilitar la llegada de solicitantes altamente calificados en IA y tecnologías críticas y emergentes;

debe establecer un programa para identificar y atraer los mejores talentos en IA y otras tecnologías críticas y emergentes en universidades, instituciones de investigación y el sector privado en el extranjero. Además, el Secretario de Seguridad Nacional deberá revisar la política y las vías de inmigración para expertos en IA y otras tecnologías críticas y emergentes, y también para fundadores de startups en IA y otras tecnologías críticas y emergentes que utilizan la *Regla Internacional del Emprendedor*, y deberá consultar con la industria y las comunidades aquéllas ocupaciones para las cuales *no hay un número suficiente de trabajadores estadounidenses preparados, dispuestos, capaces y calificados*.

Por otro lado, el Art. 5 hace foco en la promoción de la innovación en IA. Para promover asociaciones público-privadas, se pone en marcha un programa piloto para implementar el Recurso Nacional de Investigación de IA (NAIRR), desde el cual se acordará la infraestructura, los mecanismos de gobernanza y las interfaces de usuario para poner a prueba una integración inicial de recursos computacionales, de datos, de modelos y de capacitación distribuidos, *que se pondrán a disposición de la comunidad investigadora en apoyo de la investigación y el desarrollo relacionados con la IA*. También crearán al menos un motor de innovación regional de la Fundación Nacional de Ciencias, que priorice el trabajo relacionado con la IA, y creará al menos *cuatro nuevos Institutos Nacionales de Investigación de IA*, que se suman a los 25 actualmente financiados por el Gobierno Federal.

Además, se crea un programa piloto para mejorar los programas de formación para científicos, con el objetivo de formar *500 nuevos investigadores para 2025* capaces de satisfacer la creciente demanda de talento en IA. También se instruye a la Oficina de Patentes y Marcas de los Estados Unidos (USPTO) para que publique una orientación para los examinadores y solicitantes de patentes donde se aborde específicamente la inventiva y el uso de la IA, incluida la IA generativa, y otra orientación sobre cómo abordar otras consideraciones en la intersección de la IA y la propiedad intelectual. Se encomienda a la Oficina de Derechos de Autor de la Biblioteca del Congreso que publique un estudio sobre IA, que abordará las cuestiones de derechos de autor, debiendo analizar el alcance de la protección de las obras producidas utilizando IA y *el tratamiento de las obras protegidas por derechos de autor en el entrenamiento de sistemas de IA*[21]. Se instruye al Fiscal General a que desarrolle un programa de capacitación, análisis y evaluación para mitigar los riesgos de propiedad intelectual relacionados con la IA, con foco en el robo de propiedad intelectual relacionado con la IA. También se instruye al Secretario de Salud a que identifique y, según corresponda, priorice la concesión de subvenciones para apoyar el desarrollo y uso responsable de la IA con foco en herramientas que desarrollen *perfiles de respuesta inmune personalizados para pacientes*, que exploren formas de mejorar la calidad de los datos de atención médica para respaldar el desarrollo responsable de herramientas de inteligencia artificial para la atención clínica; y dispone organizar dos competencias nacionales de AI Tech Sprint de 3 meses de duración.

---

[21] Este es un tema actualmente judicializado. Véase la causa THE NEW YORK TIMES COMPANY vs.MICROSOFT CORPORATION, OPENAI, INC., OPENAI LP, OPENAI GP, LLC, OPENAI, LLC, OPENAI OPCO LLC, OPENAI GLOBAL LLC, OAI CORPORATION, LLC, and OPENAI HOLDINGS, LLC, disponible en https://nytco-assets.nytimes.com/2023/12/NYT_Complaint_Dec2023.pdf. Veáse también https://www.vox.com/technology/2024/1/18/24041598/openai-new-york-times-copyright-lawsuit-napster-google-sony

Asimismo, el Art. 5 dispone que para fortalecer la resiliencia de EE.UU. contra los impactos del cambio climático y construir una economía con energía limpia equitativa para el futuro, se instruye al Secretario de Energía para que emita un informe público que describa el potencial de la IA para *mejorar la planificación, los permisos, la inversión y las operaciones de la infraestructura de la red eléctrica* y permitir el suministro de energía eléctrica limpia, asequible, confiable, resiliente y segura. También se le pide que desarrolle herramientas que faciliten la construcción de modelos de cimientos útiles para la ciencia básica y aplicada, incluidos *modelos que agilicen los permisos y las revisiones ambientales al tiempo que mejoran los resultados ambientales y sociales*; colabore, según corresponda, con organizaciones del sector privado y miembros del mundo académico y tome medidas para ampliar las asociaciones con la industria, la academia, otras agencias y aliados y socios internacionales, para utilizar las capacidades informáticas y los bancos de pruebas de IA del Departamento de Energía para construir modelos básicos que respalden nuevas aplicaciones en ciencia y energía, vinculando al Departamento de Energía con los 17 Laboratorios Nacionales.

Finalmente, la tercera sección del Art. 5 dispone promover la competencia en la IA y tecnologías relacionadas, así como en otros mercados. Se deberán abordar los riesgos que surgen del control concentrado de insumos clave, y tomar medidas para detener la colusión ilegal e impedir que las empresas dominantes perjudiquen a sus competidores. Se instruye a la Comisión Federal de Comercio para que garantice una competencia leal en el mercado de la IA, y para que garantice que los consumidores y trabajadores estén protegidos de los daños que pueda provocar el uso de la IA. En la misma línea pero en el marco de la *Ley de Incentivos Útiles para la Producción de Semiconductores* (CHIPS) de 2022, se manda implementar programas de tutoría para aumentar el interés y la participación en la industria de semiconductores, se dispone aumentar la disponibilidad de recursos para nuevas empresas y pequeñas empresas, y aumentar la financiación para instalaciones comerciales de investigación y desarrollo centradas en semiconductores. En la misma línea, se instruye al Administrador de la Administración de Pequeñas Empresas a priorizar la asignación de fondos del programa Regional Innovation Cluster para clusters que apoyan actividades de planificación relacionadas con el establecimiento de uno o más Institutos de Innovación y Comercialización de IA para Pequeñas Empresas, y asigna hasta U$S 2 millones en fondos de premios de bonificación del *Concurso del Fondo Acelerador de Crecimiento* para aceleradores que apoyen la incorporación o expansión de planes de estudio, capacitación y asistencia técnica relacionados con la IA, u otros recursos relacionados con la IA dentro de su programación, buscando revisar los criterios de elegibilidad para mejorar el apoyo a este tipo de *startups enfocadas en IA*.

6. Protección de los Trabajadores

El Art. 6 de la OE aborda la cuestión laboral frente al impacto de la IA. Para ello, se encarga al Consejo de Asesores Económicos un informe sobre los efectos de la IA en el mercado laboral. Además, para evaluar los pasos necesarios para que el Gobierno Federal aborde las interrupciones de la fuerza laboral relacionadas con la IA, el Secretario de Trabajo presentará un informe que analice las capacidades de las agencias para apoyar a los trabajadores desplazados por la adopción de la IA y otros avances tecnológicos, evaluando cómo los programas federales

actuales podrían usarse para responder a posibles futuras amenazas de IA, e identificar opciones para fortalecer o desarrollar apoyo federal adicional para los trabajadores desplazados por la IA. En consulta con el Secretario de Educación, se deberán *fortalecer y ampliar las oportunidades de educación y capacitación que brinden a las personas caminos hacia ocupaciones relacionadas con la IA*. Además, el Secretario del Trabajo deberá desarrollar y publicar principios y mejores prácticas para los empleadores para mitigar los daños potenciales de la IA al bienestar de los empleados y maximizar sus beneficios potenciales, incluyendo los riesgos de desplazamiento laboral, nuevas oportunidades profesionales relacionados con la IA, estándares laborales y calidad del trabajo, y las implicancias de la recopilación y el uso de datos sobre ellos relacionados con la IA por parte de la patronal.

Por otro lado, para ayudar a los empleados cuyo trabajo es monitoreado o aumentado por IA a recibir un salario adecuado, el Secretario de Trabajo deberá emitir directrices para dejar claro que los empleadores que implementen IA para monitorear o aumentar el trabajo de los empleados *deben continuar cumpliendo con las protecciones que garantizan que los trabajadores sean compensados por sus horas trabajadas*. Finalmente, para fomentar una fuerza laboral preparada para la IA, se dispone priorizar los recursos disponibles para apoyar la educación relacionada con la IA, buscando identificar nuevas oportunidades para que las agencias asignen recursos para esos fines.

7. Derechos y Garantías de los Ciudadanos

El Art. 7 de la OE aborda cuestiones de derechos y garantías civiles de los ciudadanos. En primer término, para prevenir la discriminación ilegal por parte de la IA, se instruye al Fiscal General para que coordine y apoye a las agencias en la implementación y aplicación de las leyes federales existentes para abordar la situación civil, violaciones de derechos y libertades civiles y *discriminación relacionadas con la IA*. Además, se impulsa una una reunión de los jefes de las oficinas federales de derechos civiles, para discutir cómo prevenir y abordar la discriminación en el uso de sistemas automatizados, incluida la discriminación algorítmica, y mejorar la participación de las partes interesadas externas para promover la conciencia pública sobre los posibles usos y efectos discriminatorios de la IA. Además, se deberá dar orientación, asistencia técnica y capacitación a investigadores y fiscales estatales, locales, y tribales sobre las mejores prácticas para investigar y procesar violaciones de derechos civiles y discriminación relacionadas con sistemas automatizados.

Por otro lado, para garantizar una justicia justa e imparcial para todos, se deberá presentar al Presidente un informe que aborde el uso de la IA en el sistema de justicia penal, incluyendo su uso para dictar sentencia, otorgar libertad condicional, libertad supervisada y libertad condicional; aceptar fianza, libertad provisional o dictar prisión preventiva; para evaluaciones de riesgos, incluidas liberación anticipada o prisión domiciliaria, vigilancia policial; la previsión del delito y vigilancia policial predictiva, incluida la incorporación de datos históricos sobre delitos en sistemas de inteligencia artificial para predecir “puntos calientes” de alta densidad; herramientas de gestión penitenciaria; y análisis forense. Dentro del informe, se deberá analizar las áreas donde la IA puede mejorar la eficiencia y precisión de la aplicación de la ley,

con la protección de la privacidad, los derechos civiles y las libertades civiles. Se busca también promover la presencia de expertos con conocimientos técnicos pertinentes (como ingenieros de aprendizaje automático, ingeniería de software e infraestructura, expertos en privacidad de datos, científicos de datos e investigadores de experiencia de usuario) entre los profesionales encargados de hacer cumplir la ley.

Finalmente, el Art. 7 instruye a las agencias federales a que prevengan la discriminación ilegal y otros daños que resulten del uso de la IA en los programas del gobierno federal y la administración de beneficios. Se instruye al Secretario del Departamento de Salud y Servicios Sociales a que aborde *el uso de sistemas automatizados o sistemas algorítmicos en la implementación por parte de los Estados y localidades de beneficios y servicios públicos administrados por su cartera*, para promover la evaluación del acceso a beneficios por parte de beneficiarios calificados, dando aviso a los destinatarios sobre la presencia y uso de dichos sistemas; regular la evaluación para detectar denegaciones injustas; establecer procesos para apelar denegaciones ante revisores humanos; y analizar si los sistemas algorítmicos utilizados por los programas de beneficios logran resultados equitativos y justos. Similar instrucción se da al Secretario de Agricultura, quien deberá preparar un informe y guías para los beneficios públicos estatales, locales, tribales y territoriales, que utilizan sistemas automatizados o algorítmicos en la implementación de beneficios o en la prestación de apoyo, para garantizar que los programas que utilizan esos sistemas maximizan el acceso al programa para los beneficiarios elegibles, pero también para poder identificar casos en los que los solicitantes y participantes pueden apelar ante un revisor humano, y permitir la auditoría y la corrección de la lógica utilizada para llegar a una decisión o determinación individual para facilitar la evaluación de las apelaciones.

Además, se instruye al Secretario de Trabajo para que publique una guía para los contratistas federales sobre la no discriminación en la contratación que involucre IA y otros sistemas de contratación basados en tecnología. También instruye al Director de la Agencia Federal de Financiamiento de la Vivienda y al Director de la Oficina de Protección Financiera del Consumidor para exigir a sus respectivas entidades reguladas, cuando sea posible, que utilicen metodologías adecuadas, incluidas herramientas de inteligencia artificial, para garantizar el cumplimiento de la ley federal, y para evaluar modelos de suscripción para detectar sesgos o disparidades que afecten a los grupos protegidos, buscando también *evaluar los procesos automatizados de valoración y tasación de garantías de manera que minimicen el sesgo*. Si se utilizan herramientas automatizadas o algorítmicas para tomar decisiones sobre el acceso a la vivienda, el Secretario de Vivienda y Desarrollo Urbano deberá abordar el uso de sistemas de selección de inquilinos de maneras que puedan violar la Ley de Vivienda Justa, la Ley de Informes Crediticios Justos u otras leyes federales relevantes, incluyendo cómo el uso de datos, como antecedentes penales, registros de desalojo e información crediticia, puede *conducir a resultados discriminatorios*. También se busca garantizar que las personas con discapacidad estén protegidas de los riesgos de la IA, por ejemplo evitando el trato desigual derivado del uso de datos biométricos como la dirección de la mirada, el seguimiento ocular, el análisis de la marcha y los movimientos de las manos.

8. Protección de los Consumidores, Pacientes, Pasajeros y Estudiantes

El Art. 8 de la EO encomienda a todas las agencias a proteger a los consumidores del fraude, la discriminación y las amenazas a la privacidad, y para abordar otros riesgos que puedan surgir del uso de la IA, incluidos riesgos para la estabilidad financiera y la responsabilidad de las entidades reguladas de *realizar la debida diligencia y monitorear cualquier servicio de IA de terceros que utilicen*, especialmente en materia de transparencia de los modelos de IA.

Así, se instruye a la Comisión Federal de Comunicaciones a considerar acciones relacionadas con cómo la IA afectará a las redes de comunicaciones y a los consumidores, analizando el potencial de la IA para mejorar la gestión del espectro, aumentar la eficiencia del uso del espectro no federal y ampliar las oportunidades para compartir el espectro no federal, con foco en cómo mejorar la seguridad, la resiliencia y la interoperabilidad de la red utilizando tecnologías de próxima generación que incorporan IA, incluidas redes de autorreparación, 6G y Open RAN. Se deberán elaborar normas para combatir las llamadas automáticas y los textos automáticos no deseados que son facilitados por la IA, y para implementar tecnologías de IA que sirvan para bloquear las llamadas automáticas y los textos automáticos no deseados.

En materia de salud, solicita un plan estratégico al Secretaría de Salud donde deberá incluir políticas, marcos y regulaciones con foco en el despliegue y uso responsable de la IA en el sector de servicios humanos y de salud, analizando específicamente: (i) el desarrollo, mantenimiento y uso de tecnologías predictivas y generativas basadas en IA en la prestación y financiación de la atención sanitaria, para medir la calidad, la mejora del rendimiento, la integridad del programa, la administración de beneficios y la experiencia del paciente; (ii) el monitoreo de la seguridad y el desempeño en el mundo real de las tecnologías habilitadas por IA; (iii) incorporar los principios de equidad en las tecnologías habilitadas por IA, utilizando datos desglosados sobre las poblaciones afectadas y conjuntos de datos de población representativos al desarrollar nuevos modelos, *monitoreando el desempeño algorítmico contra la discriminación y el sesgo*; (iv) incorporar estándares de seguridad, privacidad y protección en el ciclo de vida del desarrollo de software para la protección de información de identificación personal; (v) el desarrollo, mantenimiento y disponibilidad de documentación para ayudar a los usuarios a determinar usos apropiados y seguros de la IA en entornos locales en el sector de servicios humanos y de salud; (vi) trabajar con agencias de servicios humanos y de salud estatales, locales, tribales y territoriales para promover casos de uso positivos y mejores prácticas para el uso de la IA en entornos locales; y (vii) identificar usos de la IA para promover la eficiencia y la satisfacción en el lugar de trabajo en el sector de la salud y los servicios humanos, incluida la reducción de las cargas administrativas.

Por otro lado, el Secretario de Salud deberá desarrollar una estrategia para determinar si las tecnologías habilitadas por IA mantienen niveles apropiados de calidad; y para establecer una política de garantías para evaluar aspectos importantes del rendimiento de las herramientas de salud basadas en IA, junto con las necesidades de infraestructura para permitir la evaluación ***previa a la comercialización y la supervisión posterior*** a la comercialización del rendimiento del sistema algorítmico de tecnología sanitaria basada en IA frente a datos del mundo real.

Asimismo, deberá promover el cumplimiento de las leyes federales contra la discriminación por parte de proveedores de servicios de salud que reciben asistencia financiera federal, y establecer un programa de seguridad de IA que, en asociación con organizaciones voluntarias de seguridad del paciente, establezca un marco común de enfoques para (a) identificar y capturar errores clínicos resultantes de la IA implementada en entornos de atención médica, así como especificaciones para un repositorio central de seguimiento de incidentes asociados que causan daño, incluso mediante prejuicios o discriminación, a pacientes, cuidadores o otros partidos, (b) analizar los datos capturados y la evidencia generada para desarrollar recomendaciones, mejores prácticas u otras pautas informales destinadas a evitar estos daños, y (c) difundir esas recomendaciones, mejores prácticas u otras orientaciones informales a las partes interesadas apropiadas, incluidos los proveedores de atención médica.

En materia de medicamentos, la OE pide al Secretario de Salud que desarrolle una estrategia para regular el uso de IA en los procesos de desarrollo de medicamentos, abordando cuestiones como (i) definir los objetivos, metas y principios de alto nivel necesarios para una regulación adecuada en cada fase del desarrollo de fármacos; (ii) identificar áreas donde la futura reglamentación pueda ser necesaria para implementar dicho sistema regulatorio; (iii) identificar el presupuesto, los recursos, el personal y el potencial existentes para nuevas asociaciones público-privadas necesarias para dicho sistema regulatorio; y (iv) considerar los riesgos identificados.

En materia de transporte, se instruye al Secretario de Transporte para que ordene al Consejo de Tecnología de Transporte Emergente y No Tradicional (NETT) que evalúe la necesidad de información, asistencia técnica y orientación con respecto al uso de la IA en el transporte. El Secretario de Transporte deberá ordenar al Consejo NETT que apoye iniciativas existentes y futuras para poner a prueba aplicaciones de IA relacionadas con el transporte, evaluando los resultados de dichos programas piloto para determinar cuándo habrá información suficiente para tomar acciones regulatorias. Además, el Secretario de Transporte deberá crear un nuevo Grupo de Trabajo Ejecutivo Intermodal, para solicitar y utilizar aportes relevantes de las partes interesadas relevantes. También se instruye a la Agencia de Proyectos de Investigación Avanzada-Infraestructura (ARPA-I) que explore las oportunidades y desafíos de la IA relacionados con el transporte y la movilidad autónoma, priorizando subvenciones a esas oportunidades, según corresponda.

En el sector de la educación, el Secretario de Educación deberá desarrollar recursos, políticas y orientación con respecto a la IA, abordando los usos seguros, responsables y no discriminatorios de la IA en la educación, con foco en las comunidades vulnerables y desatendidas. Debe desarrollar un "conjunto de herramientas de IA" para los líderes educativos que implementen las recomendaciones del informe IA y el futuro de la enseñanza y el aprendizaje del Departamento de Educación.

9. Cuestiones de Privacidad

El Art. 9 de la EO aborda los riesgos de privacidad potenciados por la IA, por la recopilación o el uso de información sobre individuos, o la realización de inferencias sobre individuos.

La EO instruye al Director de la Oficina del Presupuesto para que identifique la información comercialmente disponible adquirida por agencias, particularmente la que incluya identificación personal e incluyendo información obtenida de intermediarios de datos. Además, deberá evaluar, en consulta con el Consejo Federal de Privacidad y el Consejo Interagencial de Política Estadística, los estándares y procedimientos de la agencia asociados con la recopilación, procesamiento, mantenimiento, uso, intercambio, difusión y disposición de información comercialmente disponible que incluya identificación personal (salvo cuando se utiliza para fines de seguridad nacional), dando orientación a las agencias sobre formas de mitigar los riesgos de privacidad y confidencialidad de las actividades de las agencias relacionadas con ese tipo de información. Además, en consulta con el Fiscal General y el Asistente del Presidente para Política Económica deberá informar posibles revisiones de las directrices para las agencias sobre la implementación de las disposiciones de la Ley de Gobierno Electrónico de 2002, haciendo foco en cómo las evaluaciones de impacto en la privacidad pueden ser más efectivas para mitigar los riesgos a la privacidad. Se instruye también al Secretario de Comercio para que establezca pautas para que las agencias puedan utilizar *Privacy Enhancing Technologies* (PET) para salvaguardar la privacidad, y avanzar en la investigación, el desarrollo y la implementación de PETs.

Por otro lado, también se instruye a la Fundación Nacional de Ciencias y al Secretario de Energía para que financien una Red de Coordinación de Investigación (RCN) dedicada a promover la investigación sobre privacidad y, en particular, el desarrollo, implementación y escalamiento de PET. Se deberá identificar el trabajo en curso y las oportunidades potenciales para incorporar PET en las operaciones de todas las agencias a nivel federal.

10. Uso de IA por parte del Gobierno Federal

El Art. 10 regula el uso de la IA por parte del Gobierno Federal. A tal fin, el Director de la Oficina de Presupuesto deberá convocar y presidir un consejo interinstitucional para coordinar el desarrollo y el uso de la IA en los programas y operaciones de cada agencia, además del uso de IA en los sistemas de seguridad nacionales. Este consejo deberá emitir orientación a las distintas agencias para fortalecer el uso efectivo y apropiado de la IA, promover la innovación en IA y gestionar los riesgos de la IA en el Gobierno Federal. Esta orientación deberá hacer foco en: (i) la necesidad de designar en cada agencia a un Director de Inteligencia Artificial, que tendrá la responsabilidad principal en su agencia, de manera articulada con otros funcionarios responsables, de coordinar el uso de la IA por parte de su agencia; (ii) definir las funciones, responsabilidades, antigüedad, posición y estructuras de presentación de informes de los Directores de Inteligencia Artificial; (iii) para ciertas agencias, se prevé la creación de Juntas de Gobernanza de Inteligencia Artificial internas, con los líderes senior relevantes de toda la agencia; (iv) definir prácticas mínimas requeridas de gestión de riesgos para los usos gubernamentales de la IA que afecten los derechos o la seguridad de las personas, evaluando

la calidad de los datos; la forma de mitigar impactos dispares y discriminación algorítmica; el monitoreo y evaluación contínua de la IA desplegada; y otorgar la revisión humana para decisiones adversas tomadas utilizando IA; (v) detectar los usos específicos de la IA por parte del gobierno federal que se presume *por defecto* que afectan los derechos o la seguridad; e (vi) incluir recomendaciones a las agencias para reducir las barreras al uso responsable de la IA, incluyendo barreras en la infraestructura de tecnología de la información, los datos, la fuerza laboral, las restricciones presupuestarias y los procesos de ciberseguridad.

Además, en consulta con el Secretario de Comercio, el Secretario de Seguridad Nacional y los jefes de otras agencias según lo determine el Director de la Oficina de Presupuesto, deberán emitir recomendaciones a las agencias con respecto a: (i) pruebas externas de IA, incluida la formación de equipos rojos para la IA generativa, que se desarrollarán en coordinación con la Agencia de Seguridad de Infraestructura y Ciberseguridad; (ii) las pruebas y salvaguardias contra resultados discriminatorios, engañosos, inflamatorios, inseguros o engañosos, así como contra la producción de material de abuso sexual infantil y contra la producción de imágenes íntimas no consensuadas de individuos reales (incluidas representaciones digitales íntimas del cuerpo o partes del cuerpo de una persona identificable) para IA generativa; (iii) medidas razonables para marcar con agua o etiquetar de otro modo el *output* de la IA generativa; (iv) la forma de obtener una evaluación independiente de las afirmaciones de los proveedores de IA sobre eficacia de sus sistemas y sobre cómo mitigar los riesgos de sus sistemas IA; (v) pautas para la documentación y supervisión de la IA que sea adquirida por el Gobierno; (vi) una estrategia para maximizar el valor para las agencias cuando dependen de contratistas para usar y enriquecer los datos del Gobierno Federal con fines de desarrollo y operación de IA; (vii) la provisión de incentivos para la mejora continua de la IA adquirida; y (viii) formación en IA de acuerdo con los principios establecidos en la EO.

También se instruye al Director de la Oficina del Presupuesto a que desarrolle un método para que las agencias rastreen y evalúen su capacidad para adoptar la IA en sus programas y operaciones, gestionar sus riesgos y cumplir con la política federal sobre IA. Deberá también desarrollar las pautas, herramientas y prácticas para respaldar la implementación de las prácticas mínimas de gestión de riesgos detectados. Para mejorar la transparencia en el uso de la IA por parte de las agencias, el Director de la Oficina del Presupuesto emitirá, anualmente, instrucciones a las agencias para la recopilación, presentación de informes y publicación de los casos de uso de la IA de las agencias, de acuerdo con la sección 7225(a) de la Ley de Avance de la IA.

En relación al uso de la IA generativa por parte del Gobierno Federal, a medida que los productos de IA generativa estén ampliamente disponibles y sean comunes en las plataformas, la EO *disuade a las agencias de imponer prohibiciones o bloqueos* generales amplios sobre el uso de la IA generativa por parte de las agencias. Ahora bien, las agencias deberían limitar el acceso, según sea necesario, a servicios específicos de IA generativa en función de evaluaciones de riesgos específicas, y establecer directrices y limitaciones sobre el uso adecuado de la IA generativa, y, con las salvaguardias adecuadas, *deben brindar a su personal y programas acceso a capacidades de IA generativa seguras y confiables*, al menos para fines de experimentación y tareas rutinarias que conllevan un bajo riesgo.

En una materia muy relevante, para proteger la información del gobierno federal, la EO alienta a las agencias a emplear prácticas de gestión de riesgos, como capacitar a su personal sobre el uso, la protección, la difusión y la disposición adecuados de la información federal; a negociar condiciones de servicio apropiadas con los proveedores; y a implementar medidas diseñadas para garantizar el cumplimiento de los requisitos de mantenimiento de registros, ciberseguridad, confidencialidad, privacidad y protección de datos.

Además, el Art. 10 de la EO dispone que el Administrador de Servicios Generales, en coordinación con el Director del Presupuesto, y en consulta con el Comité Asesor Federal de Nube Segura, debe desarrollar y emitir un marco para priorizar las ofertas de tecnologías críticas y emergentes en el Programa de Gestión Federal de Riesgos y Autorizaciones, comenzando con ofertas de IA generativa que tienen el objetivo principal de proporcionar interfaces de chat basadas en modelos de lenguaje de gran tamaño, herramientas de generación y depuración de código, e interfaces de programación de aplicaciones asociadas, así como generadores de imágenes basados en mensajes. Se alienta a los directores de información de la agencia, los directores de seguridad de la información y los funcionarios autorizados a priorizar la IA generativa y otras tecnologías críticas y emergentes al otorgar autoridades para la operación de los sistemas de tecnología de la información de la agencia.

En materia de empleo federal, se instruye al Director de la Oficina de Gestión de Personal para que desarrolle una guía sobre el uso de IA generativa para el trabajo de la fuerza laboral federal. Además, se instruye a la Junta de Modernización de Tecnología a que considere priorizar el financiamiento para proyectos de IA con el Fondo de Modernización de Tecnología por un período de al menos 1 año. Por otro lado, se busca facilitar el acceso a soluciones de adquisición de todo el Gobierno Federal para tipos específicos de servicios y productos de IA, para lo cual se deberá crear una guía de recursos u otras herramientas para ayudar a las oficinas de compra gubernamentales. También se dispone planificar un aumento nacional de talento en IA en el Gobierno Federal, para lo cual varias agencias deberán identificar áreas prioritarias para aumentar el talento de IA. A tal fin, se crea un *Grupo de Trabajo de Talento Tecnológico y de Inteligencia Artificial* multi-agencia, con la misión de acelerar y rastrear la contratación de IA y talentos que permitan incorporar la IA en todo el Gobierno Federal, mediante la difusión de mejores prácticas para que las agencias atraigan, contraten, retengan, capaciten y potencien el talento de IA, utilizar programas de becas y programas de talento tecnológico y equipos de capital humano, y convocar un foro entre multi-agencia para la colaboración continua entre profesionales de la IA para compartir las mejores prácticas y mejorar la retención. El objetivo es comenzar a implementar *planes para apoyar el reclutamiento rápido de personas como parte de un aumento de talento en IA en todo el gobierno federal* para acelerar la colocación de talentos clave en IA y habilitadores de IA en áreas de alta prioridad y para avanzar en las estrategias de tecnología y datos de las agencias. A tal fin, se revisarán y flexibilizarán las prácticas federales de contratación de talentos en materias tales como lugar de trabajo (trabajo remoto), esquema salarial y de sistemas de incentivos para puestos técnicos clave, y en materia de antecedentes, *priorizando antecedentes académicos no tradicionales*.

11. Liderazgo Global en IA

El Art. 11 de la EO busca potenciar el liderazgo global de EE.UU en materia de IA. Para ello, la EO dispone que distintas autoridades y agencias deberán ampliar los compromisos con aliados y socios internacionales en foros bilaterales y multilaterales para promover la comprensión de las orientaciones y políticas existentes y planificadas relacionadas con la IA en la EO y otras normas. Además, se busca liderar los esfuerzos para establecer un marco internacional sólido para gestionar los riesgos y aprovechar los beneficios de la IA, para desarrollar principios regulatorios comunes y otros principios de responsabilidad para naciones extranjeras, incluida la gestión del riesgo que representan los sistemas de IA.

La OE busca que EE.UU promueva estándares técnicos globales responsables para el desarrollo y uso de la IA -fuera de las áreas militares y de inteligencia,- enfocando en organizaciones de desarrollo de estándares, con la finalidad de desarrollar e implementar estándares de consenso, cooperación y coordinación, e intercambio de información relacionados con la IA, con foco en nomenclatura y terminología de IA, mejores prácticas en materia de captura, procesamiento, protección, privacidad, confidencialidad, manejo y análisis de datos; confiabilidad, verificación y garantía de los sistemas de IA; y gestión de riesgos de IA, de manera coordinada con los principios establecidos en el *Marco de Gestión de Riesgos de IA* del NIST y la Estrategia de estándares nacionales del gobierno de los Estados Unidos para tecnologías críticas y emergentes.

Finalmente, se instruye al Administrador de la Agencia de los Estados Unidos para el Desarrollo Internacional, en coordinación con el Secretario de Comercio, actuando a través del director del NIST, a que publiquen un *AI in Global Development Playbook* que incorpore los principios del Marco de Gestión de Riesgos de AI, las directrices y mejores prácticas en las condiciones sociales, técnicas, económicas, de gobernanza, de derechos humanos y de seguridad. Además, impulsarán una *Agenda Global de Investigación de IA*, para guiar los objetivos y la implementación de la investigación relacionada con la IA en el extranjero, con foco en cómo mejorar la cooperación para prevenir, responder y recuperarse de posibles interrupciones de la infraestructura crítica resultantes de la incorporación de IA en sistemas de infraestructura crítica o el uso malicioso de la IA.

12. El Comité de IA de la Casa Blanca

El Art. 12 crea el Comité de IA de la Casa Blanca, cuya función será coordinar las actividades de las agencias de todo el gobierno federal para garantizar la formulación, el desarrollo, la comunicación y la participación de la industria de manera efectiva, de cara a la implementación oportuna de políticas relacionadas con la IA en la EO y otras normas aplicables. El Comité será presidido por el Asistente del Presidente y Jefe Adjunto de Gabinete para Políticas y estará integrado por 29 agencias, secretarías o funcionarios de alto rango: el Secretario de Estado; el Secretario de Hacienda; el Secretario de Defensa; el Procurador General; el Secretario de Agricultura; el Secretario de Comercio; el Secretario del Trabajo; el Secretario del Salud y Servicios Sociales; el Secretario de Vivienda y Desarrollo Urbano; el Secretario de Transporte;

el Secretario de Energía; el Secretario de Educación; el Secretario de Asuntos de Veteranos; el Secretario de Seguridad Nacional; el Administrador de la Administración de Pequeñas Empresas; el Administrador de la Agencia de los Estados Unidos para el Desarrollo Internacional; el Director de Inteligencia Nacional; el Director de la Fundación Nacional de Ciencias; el Director de la Oficina del Presupuesto; el Director de la Oficina de Ciencia y Política Tecnológica; el Asistente del Presidente para Asuntos de Seguridad Nacional; el Asistente del Presidente para Política Económica; el Asistente del Presidente y Asesor de Política Interna; el Asistente del Presidente y Jefe de Gabinete del Vicepresidente;la Asistente del Presidente y Directora del Consejo de Políticas de Género; el Presidente del Consejo de Asesores Económicos; el Director Nacional Cibernético; el Presidente del Estado Mayor Conjunto; y los jefes de otras agencias, agencias reguladoras independientes y oficinas ejecutivas que el Presidente pueda designar o invitar de vez en cuando a participar.

13. Conclusiones

El importante paso que significa la OE -en términos de regulación comparada de la IA- es, sin duda, una clara señal de EE.UU al mundo, afirmando que se percibe como líder en el stack tecnológico de la IA. En la misma línea se inscribe el Reglamento de IA de la Unión Europea[22].

Sin dudas, los principios que guiarán la política del Gobierno Federal norteamericano sirven como una hoja de ruta interesante para otros gobiernos que analizan regular una tecnología que ya avanza rápidamente, y que lo hará aún más rápido cuando se apalanque con la computación cuántica, que lentamente comienza a estar comercialmente disponible en gran escala[23].

En este sentido, el esfuerzo por delinear nuevos marcos de buenas prácticas para la utilización segura de la IA, especialmente en conexión con infraestructuras críticas y discriminación algorítimica, y la necesidad de aumentar rápidamente talento digital enfocado en IA, incluso atrayéndolo de otros países, es una pauta de política pública que bien debiera ser imitada por la República Argentina. Igual reflexión amerita el fuerte impulso a las PET en conexión con sistemas de IA.

Finalmente, es muy interesante el Comité de IA de la Casa Blanca y el perfil y el rol que se le ha dado, y en esta misma línea, pueden inscribirse el Comité Nacional de Blockchain creando en 2022[24], y especialmente la recientemente creada Mesa Interministerial sobre Inteligencia Artificial[25]. El próximo paso será legislar, con mucho cuidado y conciencia, para desarrollar, promover y exportar el talento digital argentino en materia de IA.

---

[22] Véase *supra* nota 9.

[23] Ampliar en https://ide.mit.edu/insights/the-business-case-for-quantum-computing/

[24] Confr. https://www.boletinoficial.gob.ar/detalleAviso/primera/277417/20221207

[25] Confr. https://www.boletinoficial.gob.ar/detalleAviso/primera/293710/20230908