



Documento para consulta

Bases para el desarrollo del informe previsto en el art. 74 de la Ley N° 20.212

Fecha: 30 de abril de 2024

Elaborado por: Agencia para el Desarrollo del Gobierno de Gestión Electrónica y la Sociedad de la Información y del Conocimiento (AGESIC)



0. Alcance

El presente documento resume las distintas líneas consideradas por Agesic en el marco de la elaboración del informe previsto en el artículo 74 de la Ley N° 20.212, cuyo alcance y contenido se describe más ampliamente en el capítulo de Antecedentes.

Las líneas definidas procuran ser además disparadoras de una discusión más amplia, que incluya múltiples actores y sirva de base para la preparación de las recomendaciones normativas que corresponde realizar a Agesic, en función de la norma citada.

En ese sentido, lo expresado en este documento se enmarca en un proceso de discusión en marcha, y así debe ser considerado por los distintos actores que participen en éste.

Por otra parte, el objetivo de este proceso, y en base a las consideraciones realizadas en este documento, es conocer la opinión de distintos actores de la sociedad civil, la academia, el sector público y el sector privado, en forma de respuesta a las siguientes preguntas:

1. ¿Cuáles son las recomendaciones específicas que podría realizar desde su experiencia para promover las líneas definidas en el presente documento?
2. ¿Existen deficiencias o incongruencias desde el punto de vista regulatorio que impacten en los aspectos evaluados en las líneas definidas en el presente documento y no hayan sido considerados?
3. ¿Ha identificado potenciales mejoras o modificaciones a la regulación vigente que puedan colaborar en el desarrollo de la IA en Uruguay?
4. ¿Existen otros aspectos que no encuentra considerados y que deban analizarse?

Los aportes realizados serán tenidos en cuenta como insumos para la elaboración del informe final que será presentado por Agesic al Poder Legislativo, y se anexarán a éste, como se describe en el capítulo siguiente.



1. Antecedentes

1.1 Marco de elaboración del informe

El artículo 74 de la Ley N° 20.212, de 6 de noviembre de 2023, pone de cargo de Agesic el diseño y desarrollo de una Estrategia de Inteligencia Artificial (IA) y Datos para el sector público y privado basada en estándares internacionales.

Se establecen como fundamentos de la estrategia un conjunto de principios, a saber: equidad, no discriminación, responsabilidad, rendición de cuentas, transparencia, auditoría e innovación segura, además de los principios de la protección de datos previstos en la Ley N° 18.331, de 11 de agosto de 2008 (legalidad, veracidad, finalidad, previo consentimiento informado, seguridad de los datos, reserva y responsabilidad proactiva).

Dicho artículo comete además a Agesic la presentación ante el Poder Legislativo de un informe y recomendaciones para la regulación legal de la IA, orientada a su desarrollo ético, la protección de los derechos humanos y, al mismo tiempo, el fomento de la innovación tecnológica, otorgando un plazo de 180 días, **que vence el 28 de junio del corriente año** (considerando la vigencia de la Ley a partir del primero de enero de 2024).

1.2 Recomendaciones internacionales y su impacto en Uruguay

En el documento actualmente en proceso de revisión “Estrategia de IA para el Gobierno Digital”¹ Agesic define la IA como “*un término que se usa para describir un campo de estudio y un conjunto de tecnologías que estudian y desarrollan sistemas capaces de realizar tareas que normalmente se atribuyen a la inteligencia humana*”.

La importancia de la IA en nuestra sociedad ha sido reconocida en distintos instrumentos internacionales, donde además se han elaborado conceptos que sirven a los objetivos de este proyecto. En particular, la Recomendación del Consejo de la Organización para la Cooperación y el Desarrollo Económico (OCDE)

¹ <https://www.gub.uy/agencia-gobierno-electronico-sociedad-informacion-conocimiento/comunicacion/publicaciones/estrategia-inteligencia-artificial-para-gobierno-digital/estrategia-2>. Últ. Acceso el 09/02/2024.



en Inteligencia Artificial² establece un conjunto de definiciones respecto a qué debemos entender por Sistema de IA, Ciclo de vida de la IA, Conocimiento en IA y Actores de la IA, así como un conjunto de principios aplicables a la IA³.

Esta organización, realizó un conjunto de recomendaciones basadas en principios y orientadas en especial a pequeñas y medianas empresas (PYMES) para el desarrollo de políticas a nivel nacional y cooperación internacional, a saber: i. inversión en investigación y desarrollo de IA (incluyendo inversión pública a largo plazo y promoción de la inversión privada en investigación y desarrollo con foco en la innovación en IA responsable y en el uso de datos abiertos respetuoso de la protección de datos, sin sesgos, mejorando la interoperabilidad y el uso de estándares); ii. promover el ecosistema digital para IA (promoviendo en particular mecanismos como los fideicomisos de datos para compartir información de forma legal, ética y segura); iii. definir y habilitar un marco de políticas en el uso de IA (habilitar así la transición de la investigación y desarrollo a la implantación y operación a través de mecanismos como los entornos controlados y revisar y adaptar los marcos regulatorios y de políticas y los mecanismos de análisis a ser aplicados para promover la innovación y competencia en IA confiable); iv. generar capacidades y preparar la transformación del mercado laboral (trabajar con varios actores en la preparación de la sociedad y el mundo del trabajo a través del empoderamiento de las personas, elaborar programas de capacitación y mejorar la seguridad de los trabajadores y promover el emprendurismo, entre otros); v. cooperar internacionalmente para una IA confiable (cooperación con otros países y actores, trabajar en iniciativas comunes, utilizar métricas internacionalmente comparables y recolectar evidencia, entre otras).

Los principios de la OCDE han servido de base para otros desarrollos posteriores, mereciendo un destaque particular los once principios rectores para IA Avanzada ratificados por el G7 y conocidos como principios de Hiroshima⁴, que a su vez dieron lugar a un código de conducta para desarrolladores. Solo a modo de

² <https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0449>. Últ. Acceso el 09/02/2024.

³ A la fecha de elaboración del presente Uruguay se encuentra en proceso de adhesión a estos principios.

⁴ <https://www.mofa.go.jp/files/100573466.pdf>. Últ. Acceso el 12/02/2024.



referencia, corresponde indicar que conforme lo informado⁵, el marco político global del proceso de la IA de Hiroshima consta de cuatro pilares: 1. análisis de los riesgos prioritarios, los retos y las oportunidades de la IA generativa, 2. los Principios Rectores Internacionales del Proceso de Hiroshima para todos los agentes de la IA en el ecosistema de la IA, 3. Código de conducta internacional del Proceso de Hiroshima para las organizaciones que desarrollan sistemas avanzados de IA y, 4. cooperación basada en proyectos en apoyo del desarrollo de herramientas y mejores prácticas de IA responsables.

Recientemente, Uruguay adhirió⁶ a la Recomendación sobre la Ética de la IA de Organización de las Naciones Unidas para la Educación, la Ciencia y la Cultura (UNESCO)⁷, marco que fue adoptado por sus 193 miembros, y basado en 4 valores fundamentales: 1. Derechos humanos y dignidad humana; 2. Vivir en sociedades pacíficas, justas e interconectadas; 3. Garantizar la diversidad y la inclusión; 4. Florecimiento del medio ambiente y los ecosistemas. Esta recomendación fomenta una comprensión dinámica de la IA, definiéndola como “*aquellos sistemas con capacidad para procesar datos de forma similar a un comportamiento inteligente.*”

Interesa destacar a los efectos del informe comisionado dos aspectos de la Recomendación citada:

En primer lugar, la definición de 11 áreas significativas para la adopción de acciones relevantes por parte de los gobiernos, de forma de pasar de principios de alto nivel a estrategias prácticas. Dichas áreas de acción y las estrategias propuestas por UNESCO colaboran en la determinación de los pasos a seguir para la estructuración de un marco normativo que contemple otros aspectos más allá del institucional que son impactados por la IA en nuestras sociedades.

En segundo lugar, corresponde señalar que la Recomendación plantea dos metodologías prácticas que colaboran en su implementación: la [Metodología de Evaluación de Preparación](#) (*Readiness Assessment Methodology* o RAM) y la

⁵ <https://digital-strategy.ec.europa.eu/en/library/g7-leaders-statement-hiroshima-ai-process>. Últ. Acceso el 11/02/2024.

⁶ <https://www.gub.uy/agencia-gobierno-electronico-sociedad-informacion-conocimiento/comunicacion/noticias/uruguay-adhiere-recomendacion-etica-inteligencia-artificial-unesco>. Últ. Acceso el 09/02/2024.

⁷ <https://www.unesco.org/es/artificial-intelligence/recommendation-ethics>. Últ. Acceso el 09/02/2024.



Evaluación de Impacto Ético (*Ethical Impact Assessment* o EIA). En particular la RAM plantea preguntas en temas como la normatividad en materia de IA y la infraestructura a nivel país para habilitar la accesibilidad de las tecnologías de IA, y tiene por objetivo colaborar en la determinación de los cambios normativos e institucionales necesarios para aprovechar y también resguardarse en el uso de estas tecnologías⁸.

A la fecha de elaboración del presente, Uruguay está siendo evaluado en el marco de la citada metodología, con la colaboración del Banco de Desarrollo de América Latina (CAF)⁹.

Existen un conjunto de iniciativas que se están tratando en otros ámbitos, y que tendrán sin duda su impacto, como por ejemplo las negociaciones en el marco del Consejo de Europa para la elaboración de un Convenio Marco de IA a nivel internacional¹⁰, y en el que está participando nuestro país, o incluso la propuesta de Reglamento de la Unión Europea al respecto.

1.3 Soberanía de IA y la iniciativa de Infraestructura Pública Digital

El concepto de Soberanía de IA ha sido descrito por BELLI¹¹ como “(...) *la capacidad de un país determinado para entender, desarrollar y regular sistemas de IA (...) debería ser visto como esencial para retener el control, uso y autodeterminación sobre sistemas de IA*”¹².

⁸ <https://www.unesco.org/es/articulos/la-unesco-ayudara-mas-de-50-paises-elaborar-una-politica-etica-en-materia-de-ia-este-ano>. Últ. Acceso el 09/02/2024.

⁹ <https://www.unesco.org/es/articulos/unesco-apoya-proceso-de-revision-de-la-estrategia-de-etica-de-la-inteligencia-artificial-en-uruguay>. Últ. Acceso el 09/02/2024.

¹⁰ <https://www.coe.int/en/web/artificial-intelligence/cai>. Últ. Acceso el 09/02/2024.

¹¹ BELLI, Luca. “Exploring the Key AI Sovereignty Enablers (KASE) of Brazil, to build an AI Sovereignty Stack” en “THE QUEST FOR AI SOVEREIGNTY, TRANSPARENCY AND ACCOUNTABILITY. Official Outcome of the UN IGF Data and Artificial Intelligence Governance Coalition” disponible en https://www.intgovforum.org/en/filedepot_download/288/26421. Últ. Acceso el 30/04/2024.

¹² En el original mencionado, BELLI señala que define “*AI Sovereignty as the capacity of a given country to understand, develop and regulate AI systems. I argue that AI Sovereignty should be seen as essential to retain control, agency, and self-determination5 over AI systems*”.



El autor propone a estos efectos un marco de elementos interconectados (definido como KASE por las siglas “Key AI Sovereignty Enablers”) que permitirá a un país determinar su soberanía en la materia, y que refieren en concreto a: gobernanza adecuada de datos personales y de algoritmos, fuerte capacidad computacional, conectividad significativa, potencia eléctrica confiable, población educada en lo digital, sólida ciberseguridad y marco regulatorio apropiado.

El Foro Económico Mundial¹³ por su parte, consideró la aplicación de 6 pilares para obtener esta soberanía, a saber: infraestructura digital; desarrollo de la fuerza laboral; investigación, desarrollo e innovación (RDI por sus siglas en ingles); marco regulatorio y ético; estímulo a la industria de IA y cooperación internacional.

El argumento de la soberanía en materia de IA debe considerarse en especial al momento de promover iniciativas regulatorias que impactan en los ámbitos indicados y que determinarán, en definitiva, la posición del país frente al desarrollo de estas tecnologías.

Una iniciativa en desarrollo y se entiende de especial relevancia para la evolución de este concepto es la de Infraestructura Pública Digital, promovida desde el Programa de la Organización de las Naciones Unidas para el Desarrollo (PNUD)¹⁴, que se constituye en un pilar de la soberanía digital en general y de la soberanía de IA en especial, lo que se relaciona especialmente con la línea de Infraestructura y Ciberseguridad que se verá luego.

1.4 El antecedente de la Estrategia de IA para el Gobierno Digital

Desde el año 2020 Uruguay cuenta con una estrategia de IA para el Gobierno Digital, impulsada por Agesic. Dicha estrategia tiene como objetivo promover y fortalecer el uso responsable de la IA en la Administración Pública, estructurándose en un conjunto de principios, pilares, objetivos y líneas de acción. Interesa destacar, además de los principios (interés general, respeto de los derechos humanos, transparencia, responsabilidad, ética, valor agregado, privacidad por diseño y restantes principios de la protección de datos personales, y seguridad), los pilares

¹³ Ver al respecto: <https://www.weforum.org/agenda/2024/04/sovereign-ai-what-is-ways-states-building/>. Últ. Acceso: 30/04/2024.

¹⁴ Ver al respecto: <https://www.undp.org/digital/digital-public-infrastructure>, Últ. Acceso: 02/05/2024.



que la componen: 1. Gobernanza de IA en la Administración Pública; 2. Desarrollo de capacidades para la IA; 3. Uso y aplicación de la IA; 4. Ciudadanía Digital e IA¹⁵.

El artículo 74 de la Ley N° 20.212 dispone que Agesic revisará la Estrategia Nacional de IA, en el marco de los principios definidos, haciendo énfasis en un proceso con la participación de múltiples actores de los sectores público, privado, academia y de la sociedad civil (información disponible en la Plataforma de Participación Ciudadana Digital¹⁶). En lo hechos, Agesic ya había iniciado en el año 2023 este proceso de revisión, con el objetivo de construir una estrategia nacional más allá del ámbito público.

Resulta necesario destacar que la revisión de esta estrategia se está realizando conjuntamente con la creación de la Estrategia Nacional de Datos -por expresa previsión del artículo citado-, y en coordinación con la Estrategia Nacional de Ciudadanía Digital y la Estrategia Nacional de Ciberseguridad, todas ellas impulsadas desde Agesic.

1.5 Temáticas a considerar en la elaboración del informe

A efectos de establecer el alcance del informe a presentar ante el Poder Legislativo, se considera específicamente lo referido en el artículo 74 de la Ley N° 20.212: *“Como parte de esta estrategia nacional de inteligencia artificial, se establece un plazo de ciento ochenta días para la presentación ante el Poder Legislativo de un informe y recomendaciones para su regulación legal, orientada a su desarrollo ético, la protección de los derechos humanos y, al mismo tiempo, el fomento de la innovación tecnológica”*.

En consecuencia, desarrollo ético, protección de derechos humanos y fomento de la innovación tecnológica son pilares que deben orientar la preparación del informe y de las recomendaciones a elaborar.

Siguiendo dichos pilares resulta necesario no sólo realizar recomendaciones en aspectos vinculados a la institucionalidad de la IA en Uruguay, sino además en

¹⁵<https://www.gub.uy/agencia-gobierno-electronico-sociedad-informacion-conocimiento/comunicacion/publicaciones/estrategia-inteligencia-artificial>. Últ. Acceso el 12/02/2024.

¹⁶ <https://plataformaparticipacionciudadana.gub.uy/processes/estrategia-ia-datos>. Últ. Acceso el 12/02/2024.



otros ámbitos conexos de relevancia a efectos de potenciar su desarrollo, en forma respetuosa de los derechos humanos, para lo que se determinaron en una primera instancia líneas temáticas a ser consideradas conjuntamente con otras entidades públicas, a saber: i. institucionalidad y gobernanza; ii. derechos humanos; iii. trabajo y capacitación; iv. propiedad intelectual; v. responsabilidad civil y derechos del consumidor; vi. infraestructura y ciberseguridad; vii. medidas de promoción

Participaron en una primera etapa las siguientes entidades públicas: Presidencia de la República, Ministerio de Trabajo y Seguridad Social, Ministerio de Industria, Energía y Minería, Ministerio de Educación y Cultura, Ministerio de Economía y Finanzas, Agencia Nacional de Investigación e Innovación, Institución Nacional de Derechos Humanos y Defensoría del Pueblo, Secretaría de Derechos Humanos y la Unidad Reguladora de Servicios de Comunicaciones, con las cuales Agesic desarrolló reuniones de trabajo a efectos de recoger la visión y aportes de los organismos sobre las temáticas indicadas dentro del ámbito de sus competencias.

El objetivo de esta segunda etapa es recabar opiniones de actores relevantes del sector público, la sociedad civil, la academia y el sector privado, identificados con la colaboración de las entidades participantes, en base a las temáticas que se presentan a continuación, y otras que puedan surgir del proceso de consulta.

Documento para Consulta



2. Línea Institucionalidad y gobernanza

2.1 Consideraciones preliminares

El objetivo de esta línea es la determinación de los aspectos fundamentales para asegurar una adecuada institucionalidad de la Inteligencia Artificial en nuestro país.

En ese sentido, la institucionalidad no sólo refiere a la estructura orgánica que puede ser de aplicación, que debe contemplar objetivos a corto, mediano y largo plazo, y debe acompañarse de previsiones presupuestales de ser necesario, pero fundamentalmente, debe de contemplar la idiosincrasia local. Así, las estructuras que en otros países o regiones puedan resultar de aplicación efectiva, pueden no resultar eficientes, o directamente resultar inadecuadas para nuestro país y viceversa.

Un ejemplo de estructuras disímiles vinculadas a la gestión de los datos, y también a la inteligencia artificial, es la forma en que se ha regulado la organización de la protección de los datos personales. En nuestro país, la ley N° 18.331, de 11 de agosto de 2008, crea un órgano desconcentrado de la Agencia para el Desarrollo del Gobierno de Gestión Electrónica y la Sociedad de la Información y del Conocimiento, denominada Unidad Reguladora y de Control de Datos Personales, con competencia para determinar su propio presupuesto y autonomía técnica, sin dejar de estar bajo la estructura jerárquica de la Presidencia de la República.

En otros países de América Latina existen entidades autárquicas -basta ver por ejemplo la Agencia para el Acceso a la Información Pública de la República Argentina, la Autoridad Nacional de Protección de Datos de Brasil, o el Instituto Nacional para la Transparencia, Acceso a la Información y Protección de Datos Personales de México-, o entidades dependientes de Ministerios -como por ejemplo en el caso de Colombia, en el que la entidad de protección de datos es una delegatura de la Superintendencia de Industria y Comercio del Ministerio de Comercio, Industria y Turismo-. Algunas de estas entidades poseen competencias compartidas vinculadas a la protección de datos y del acceso a la información pública, algunas tienen facultades sancionatorias para todo el espectro de responsables y otras distinguen entre públicos y privados.



Este conjunto de diferencias, no obstante que puedan desarrollar sus actividades en sus respectivas jurisdicciones nacionales, representen a sus países en la materia, realicen recomendaciones e impongan las sanciones que correspondan por incumplimientos a la Ley.

El objetivo de este desarrollo es aclarar que la institucionalidad de la Inteligencia Artificial en nuestro país deberá contemplar sí los antecedentes internacionales y nacionales asociados al tema, pero reiteramos, ellos deberán analizarse a la luz de la idiosincrasia local.

Conjuntamente con la institucionalidad de la Inteligencia Artificial, es fundamental considerar la gobernanza de los datos, por ser ésta uno de los elementos esenciales para el desarrollo de los sistemas de IA. La gobernanza de los datos es un componente central que debe ser considerado, focalizando en los distintos tipos de datos -personales y no personales-, su gestión, las entidades actualmente generadoras y gestoras de esos datos, su reutilización, la interoperabilidad, y, en definitiva, los estándares a cumplir tanto por el sector público como el privado para el uso de datos que alimenten y que a su vez sean generados por sistemas de IA.

En este punto en particular, se debe hacer referencia no sólo a la determinación de la estructura dentro del Estado de la o las entidades a cargo de la definición de lineamientos en la materia, sino también a aquellas condiciones que son necesarias para asegurar efectivamente dicha institucionalidad.

2.2 Selección de antecedentes internacionales

El borrador de Convenio de IA del CoE establece en su artículo 1° que las partes deben adoptar y mantener medidas legislativas, administrativas u otras para dar efecto a las provisiones del convenio, las que deben graduarse y diferenciarse en función de la severidad y probabilidad de ocurrencia de impactos adversos en los derechos humanos, la democracia y el estado de derecho. El proyecto de Convenio plantea, con matices, la aplicabilidad de sus disposiciones para el ámbito público y privado.

En el marco del borrador de Convenio, deben adoptarse medidas para proteger a las personas en procesos democráticos, acceso a debate público y salvaguardarlas de influencias externas perjudiciales o maliciosas.



En materia de innovación, el proyecto de Convenio prevé la posibilidad de que se establezcan entornos controlados para el desarrollo y experimentación de sistemas de inteligencia artificial bajo la supervisión de autoridades competentes. En este punto, cabe recordar que el artículo 75 de la Ley N° 20.212 prevé la creación de entornos controlados de prueba o sandboxes regulatorios, que está en este momento siendo objeto de reglamentación por parte de Agesic con la colaboración de otras entidades.

La transparencia en el marco del proyecto de Convenio es fundamental, y que las personas conozcan efectivamente que están interactuando con un sistema de IA es parte de esa transparencia.

En lo que respecta al Reglamento Europeo en la materia¹⁷, el Título VI refiere a la gobernanza de la IA, creando en los capítulos que lo conforman el Comité Europeo de Inteligencia Artificial (órgano comunitario integrado por autoridades nacionales de supervisión), con facultades de asistir a las autoridades nacionales, coordinar orientaciones y análisis, y contribuir a la cooperación efectiva en la materia.

El capítulo 2 del Título VI del Reglamento Europeo refiere a las Autoridades Nacionales Competentes, que tienen como fin garantizar la aplicación y ejecución de éste y deberán preservar la objetividad e imparcialidad de sus actividades y funciones. Estas deberán tener recursos financieros y humanos adecuados, con conocimiento profundo en tecnologías de IA, datos, computación de datos, riesgos para derechos fundamentales, salud y seguridad, y conocimiento respecto de normas y requisitos legales vigentes.

En lo que refiere al sistema adoptado en los Estados Unidos, encontramos la Orden Ejecutiva en el desarrollo y uso seguro, fiable y confiable de sistemas de Inteligencia Artificial¹⁸. Esta orden ejecutiva pone énfasis en 8 principios que deben ser cumplidos por las entidades del Gobierno Federal para alcanzar los objetivos buscados. Por su parte, establece un conjunto de acciones que deben ser adoptadas por distintas agencias del gobierno federal, en sus respectivos ámbitos

¹⁷ <https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=celex:52021PC0206>. Ult. Acceso: 19/03/2024.

¹⁸ <https://www.whitehouse.gov/briefing-room/presidential-actions/2023/10/30/executive-order-on-the-safe-secure-and-trustworthy-development-and-use-of-artificial-intelligence/>. Ult. Acceso 19/3/2024.



de competencia, vinculadas a IA. No se prevé de esta forma una autoridad central exclusiva con competencias en IA, sino una distribución de las cuestiones asociadas a la IA en las instituciones que normativamente tienen competencia para ello.

Finalmente, y sólo recientemente el gobierno de Reino Unido publicó un documento en el que se procura una aproximación a la regulación de IA pro innovación¹⁹, que surge luego de una consulta pública realizada por un plazo de 1 año, sobre una propuesta regulatoria.

En el caso de Reino Unido, se creó una Oficina para la Inteligencia Artificial que es parte del Departamento de Ciencia, Innovación y Tecnología, al igual que la reciente Unidad de Adopción Responsable de Tecnología. En particular esta última, tiene como objetivo promover la innovación responsable en los sectores público y privado, desarrollando herramientas que permitan construir confianza a la interna de las organizaciones en los sistemas de IA y de gestión de datos. Durante varios años el Reino Unido contó con un Consejo de IA integrado por expertos de múltiples sectores (hasta junio de 2023), que tenía por objetivo el contribuir al desarrollo de la estrategia de IA.

Actualmente el gobierno de Reino Unido tiene además una Oficina Central Digital y de Datos que lidera las funciones digitales, de datos y de tecnologías para el gobierno y trabaja en particular en el desarrollo de la política y estrategia de IA, incluyendo estándares para el uso gubernamental.

Se observa en todas estas disposiciones un énfasis particular en la forma de empleo de los datos, y en los principios que deben orientar las regulaciones en la materia. Asimismo, existe una tendencia a generar esquemas de gobernanza con la participación de múltiples actores, sin perjuicio del liderazgo de un organismo dentro de la estructura estatal. Se observa también la necesidad de imprimir un fuerte énfasis al componente innovación -responsable- y garantizar la protección de los derechos humanos, siendo la capacitación de los cuerpos técnicos vinculados a esta entidad reguladora, un elemento central.

¹⁹ <https://www.gov.uk/government/consultations/ai-regulation-a-pro-innovation-approach-policy-proposals/outcome/a-pro-innovation-approach-to-ai-regulation-government-response>. Últ. Acceso 19/3/2024.



2.3 Diagnóstico preliminar en materia de Institucionalidad de la IA

De conformidad con las normas relevadas, desde el punto de vista institucional existen dos entidades con cometidos para establecer criterios generales en la materia, Agesic y la URCDP.

El artículo 74 de la Ley N° 20.212 dispone el diseño e implementación de la Estrategia de Datos y de Inteligencia Artificial poniendo de cargo de Agesic su liderazgo. Es en el marco de estas competencias que se le atribuye a Agesic la posibilidad de crear grupos de trabajo y otras instancias con distintos actores que colaboren en la implementación de estas estrategias.

Sin perjuicio de ello, el inciso final de este artículo prevé un cometido que excede el vinculado a la estrategia, y refiere en concreto al desarrollo de sistemas de inteligencia artificial, para lo que podrá establecer criterios y definir mecanismos de fiscalización de su cumplimiento.

Consecuente con esta disposición, se establece que esa competencia es sin perjuicio en primer lugar de las competencias de la URCDP, quien es el competente para la determinación de criterios en el uso de datos personales en cualquier operación de tratamiento, y en especial en aquellos que se establecen en el artículo 16 de la Ley N° 18.331 -tratamientos automatizados que generen, entre otros, perfiles de las personas-, de conformidad con el artículo 34 de la citada Ley.

El inciso final del artículo 74 indica también que ello es sin perjuicio de las competencias de otros organismos públicos en sus ámbitos particulares de actuación.

En lo que respecta a la institucionalidad en materia de gobernanza de datos en general, la competencia de Agesic en este punto se desprende de las normas en materia de intercambio de información e interoperabilidad, gobierno abierto y datos abiertos que se referencian más arriba, en el Anexo 1, entre otras. Asimismo, las unidades desconcentradas de la citada Agencia, la URCDP y la UAIP tienen competencia a nivel nacional en lo que respecta a la gestión de la información personal y también de la información pública.



3. Línea Derechos Humanos

3.1 Consideraciones preliminares

El objetivo de esta línea es plantear cuales son los riesgos que en el marco del desarrollo de una política pública en materia de Inteligencia Artificial no pueden soslayarse, y deben requerir -de entenderlo necesario- medidas especiales, por su impacto en los derechos de las personas y qué medidas podrían resultar pertinentes a efectos de aprovechar los sistemas de IA en beneficio de las personas y sus derechos, identificando aquellas de orden normativo. Para ello se considerarán las normas y obligaciones internacionales conexas del derecho internacional de los derechos humanos ratificados por el país, las recomendaciones específicas en materia de inteligencia artificial realizadas por organismos internacionales y la regulación vigente o en proceso de elaboración a nivel regional e internacional.

Los impactos de la Inteligencia Artificial en los derechos humanos ha sido parte de los análisis realizados en distintos foros. El Alto Comisionado de las Naciones Unidas para los Derechos Humanos, Volker Turk, en el Evento Paralelo de Alto Nivel del 53° Período de Sesiones del Consejo de Derechos Humanos²⁰ señaló que en nuestro mundo y en estos momentos, los derechos humanos están siendo puestos a prueba, y que la pregunta de dónde están los límites de la IA es una de *“(…) las cuestiones más acuciantes para nuestra sociedad, para los gobiernos y para el sector privado”*. El Alto Comisionado señala que existen dos escuelas sobre la regulación de la IA: a) una de ellas se centra en los riesgos, la autorregulación y la autoevaluación por los desarrolladores, lo que pone una responsabilidad muy grande en el sector privado; b) la segunda es un enfoque que integra los derechos humanos en todo el ciclo de vida de la IA, incorporando los principios de derechos humanos desde *“(…) la recopilación y selección de datos; así como al diseño, desarrollo, implementación y uso de los modelos, instrumentos y servicios resultantes”*.

²⁰ El discurso del Alto Comisionado puede encontrarse en: <https://www.ohchr.org/es/statements/2023/07/artificial-intelligence-must-be-grounded-human-rights-says-high-commissioner>. Últ. Acceso: 20/03/2024.



El Alto Comisionado en este punto hace algunas propuestas al respecto: 1) escuchar a grupos más vulnerables al uso de esta tecnología; 2) prestar atención al uso de IA en servicios públicos y privados en los que exista mayor riesgo de abuso de poder o intrusión en la privacidad; 3) exigir evaluación de riesgos y repercusiones para los derechos humanos antes, durante y después del uso de sistemas de IA (transparencia, supervisión independiente y acceso a remedios efectivos); 4) prohibir o suspender tecnologías de IA que no cumplan con la normativa internacional de derechos humanos; 5) aplicar la regulación de protección de datos y otras legislaciones sectoriales de protección ya existentes; 6) no permitir un enfoque que se sustente únicamente en la autorregulación; 7) crear un órgano asesor internacional.

A efectos de este documento, se propone considerar los primeros 6 puntos mencionados por el Alto Comisionado.

3.2 Selección de antecedentes internacionales

En el marco del sistema de las Naciones Unidas, la Organización de las Naciones Unidas para la Educación, la Ciencia y la Cultura (UNESCO) elaboró en el año 2021 la “*Recomendación sobre la ética de la inteligencia artificial*” que fue adoptado por los 193 estados miembros, e incorporada por nuestro país, en la que se destaca el rol de la protección de los derechos humanos para un desarrollo ético de sistemas de IA, basado en principios de transparencia y equidad.

En dicha Recomendación, se consideran los siguientes instrumentos: la Declaración Universal de Derechos Humanos (1948), los instrumentos del marco internacional de derechos humanos, entre ellos la Convención sobre el Estatuto de los Refugiados (1951), el Convenio sobre la Discriminación (Empleo y Ocupación) (1958), la Convención Internacional sobre la Eliminación de Todas las Formas de Discriminación Racial (1965), el Pacto Internacional de Derechos Civiles y Políticos (1966), el Pacto Internacional de Derechos Económicos, Sociales y Culturales (1966), la Convención sobre la Eliminación de Todas las Formas de Discriminación contra la Mujer (1979), la Convención sobre los Derechos del Niño (1989), la Convención sobre los Derechos de las Personas con Discapacidad (2006), la Convención relativa a la Lucha contra las



Discriminaciones en la Esfera de la Enseñanza (1960) y la Convención sobre la Protección y Promoción de la Diversidad de las Expresiones Culturales (2005), así como cualesquiera otros instrumentos, recomendaciones y declaraciones internacionales pertinentes. Se toma nota además de la Declaración sobre el Derecho al Desarrollo (1986); de la Declaración sobre las Responsabilidades de las Generaciones Actuales para con las Generaciones Futuras (1997); de la Declaración Universal sobre Bioética y Derechos Humanos (2005); de la Declaración de las Naciones Unidas sobre los Derechos de los Pueblos Indígenas (2007); de la resolución de la Asamblea General de las Naciones Unidas sobre el examen de la Cumbre Mundial sobre la Sociedad de la Información (A/RES/70/125) (2015); de la resolución de la Asamblea General de las Naciones Unidas titulada “Transformar nuestro mundo: la Agenda 2030 para el Desarrollo Sostenible” (A/RES/70/1) (2015); de la Recomendación relativa a la Preservación del Patrimonio Documental, comprendido el Patrimonio Digital, y el Acceso al mismo (2015); de la Declaración de Principios Éticos en relación con el Cambio Climático (2017); de la Recomendación sobre la Ciencia y los Investigadores Científicos (2017); de los indicadores sobre la universalidad de Internet (aprobados en 2018 por el Programa Internacional para el Desarrollo de la Comunicación de la UNESCO), incluidos los principios ROAM (aprobados por la Conferencia General de la UNESCO en 2015); de la resolución del Consejo de Derechos Humanos sobre “El derecho a la privacidad en la era digital” (A/HRC/RES/42/15) (2019); y de la resolución del Consejo de Derechos Humanos titulada “Las tecnologías digitales nuevas y emergentes y los derechos humanos” (A/HRC/RES/41/11) (2019).

En base a estos antecedentes, UNESCO recomienda a los estados miembros, la aplicación de medidas adecuadas -legislativas y otras- para dar efecto a los principios y normas desarrollados, conforme al derecho internacional y en especial el derecho internacional de los derechos humanos.

Se explicita en particular en la Recomendación que los sistemas de IA deben mejorar la calidad de vida de los seres humanos, los que no deben sufrir ningún tipo de daño en ninguna etapa del ciclo de vida de los sistemas de IA. Se hace énfasis además en la necesidad de contar con medios para promover, defender y



ejercer los derechos humanos. Se proponen al efecto un conjunto de principios: proporcionalidad e inocuidad, seguridad y protección, equidad y no discriminación, sostenibilidad, derecho a la intimidad y protección de datos, supervisión y decisión humanas, transparencia y explicabilidad, responsabilidad y rendición de cuentas, sensibilización y educación y Gobernanza y colaboración adaptativas de múltiples partes interesadas. Dichos principios se encuentran asociados a medidas concretas que se analizarán más adelante, destacándose en particular a los efectos de este documento la Evaluación de Impacto Ético.

La Evaluación de Impacto Ético propuesta por UNESCO propone que los Estados miembros establezcan “(...) *marcos de evaluación del impacto como evaluaciones del impacto ético, para determinar y analizar los beneficios, los problemas y los riesgos de los sistemas de IA, así como medidas adecuadas de prevención, atenuación y seguimiento de los riesgos, entre otros mecanismos de garantía. Esas evaluaciones del impacto deberían revelar las repercusiones en los derechos humanos y las libertades fundamentales, en particular, aunque no exclusivamente, los derechos de las personas marginadas y vulnerables o en situación de vulnerabilidad, los derechos laborales, el medio ambiente y los ecosistemas, así como las consecuencias éticas y sociales, y facilitar la participación ciudadana, de conformidad con los valores y principios enunciados en la presente Recomendación*”.

Recientemente la Asamblea General de la Organización de las Naciones Unidas (ONU) adoptó por aclamación una resolución²¹ para la promoción de sistemas de IA seguros y fiables, que permitan alcanzar los Objetivos de Desarrollo Sostenible (ODS), que contiene en particular recomendaciones de medidas particulares a ser adoptadas por los Estados Miembros en esta materia.

Asimismo, también en el marco de la ONU, merece un destaque particular el documento de diciembre de 2023 “Interim Report: Governing AI for Humanity”²²,

²¹ Puede obtenerse más información en: <https://news.un.org/es/story/2024/03/1528511#:~:text=La%20Asamblea%20General%20de%20la%20ONU%20adopt%C3%B3%20por,que%20beneficien%20tambi%C3%A9n%20al%20desarrollo%20sostenible%20para%20todos.> Últ. Acceso: 25/03/2024.

²² Disponible en https://www.un.org/sites/un2.un.org/files/un_ai_advisory_body_governing_ai_for_humanity_interim_report.pdf. Últ. Acceso: 02/04/2024.



que contiene entre otros una categorización de riesgos desde la perspectiva de la vulnerabilidad existente o potencias para las personas, los grupos, la economía, los (eco)sistemas, los valores y normas y la sociedad. Ello más allá de la consideración de un principio guía de la gobernanza de la IA que son las normas internacionales de derechos humanos, y los compromisos asumidos en los Objetivos de Desarrollo Sostenible.

Al analizar otros antecedentes internacionales se valorarán las medidas consideradas en otras jurisdicciones y reflejadas en normas vigentes o cuya vigencia se espera en breve.

A nivel nacional, corresponde mencionar el Plan Nacional de Derechos Humanos 2023-2027, donde se menciona expresamente el impacto de la inteligencia artificial, entre otros, y la necesidad de avanzar hacia los ideales de la Declaración Universal de los Derechos Humanos. Este Plan complementa los objetivos plasmados en este documento, siendo que el primero procura establecer mecanismos de articulación, marcos normativos, protocolos de actuación que permitan incorporar el enfoque de derechos humanos en políticas públicas como la que se pretende institucionalizar en la temática de la IA. En función de ello, parece relevante acompañar el desarrollo de las directrices planteadas a efectos de incluir la temática en los objetivos definidos en cada una de ellas.

Recientemente, han surgido dos disposiciones normativas, una regulación comunitaria de un organismo regional como la Unión Europea y una regulación internacional en la forma de un Convenio en el marco del Consejo de Europa, cuyas soluciones merecen ser consideradas.

En lo que respecta a la Regulación de la UE, la Ley de Inteligencia Artificial aprobada por los países de la UE el 13 de marzo de 2024, establece algunos aspectos de relevancia a considerar a los efectos de este documento y que se refleja en el detalle realizado por la propia Unión Europea²³:

- 1) Reglas para distintos tipos de Riesgos:

²³ Ver al respecto: <https://www.europarl.europa.eu/topics/en/article/20230601STO93804/eu-ai-act-first-regulation-on-artificial-intelligence>. Últ. Acceso: 24/03/2024.



- a. Riesgos inaceptables, prohibidos por constituir una amenaza para las personas:
 - i. Manipulación cognitiva del comportamiento de grupos de personas vulnerables
 - ii. “Scoring” social
 - iii. Identificación y categorización biométrica de las personas
 - iv. Sistemas de identificación biométrica remota y en tiempo real -en este caso existen excepciones basadas en propósitos de policía-.
 - b. Riesgos altos, los que se dividen en dos categorías y requieren de una valoración previa a su puesta en producción:
 - i. Sistemas utilizados en productos que sean alcanzados por la legislación de seguridad de productos de la UE (juguetes, aviación, automóviles, dispositivos médicos y elevadores).
 - ii. Sistemas de áreas específicas que deben ser registrados en una base de datos de la UE:
 - 1. Gestión y operación de infraestructura crítica
 - 2. Capacitación vocacional y educación
 - 3. Trabajo, gestión de trabajadores y acceso a empleo
 - 4. Acceso y goce de servicios privados esenciales y servicios públicos y beneficios
 - 5. Cumplimiento de la ley
 - 6. Migración, asilo y gestión de control de fronteras
 - 7. Asistencia en la interpretación y aplicación legal de la ley
- 2) Requerimientos de transparencia. Algunos sistemas de IA, como la IA generativa, aun cuando no se consideren de alto riesgo, deben cumplir con requisitos de transparencia y normativa de propiedad intelectual:
- a. Revelar que el contenido fue generado por IA



- b. Diseñar el modelo para evitar que genere contenido ilícito
- c. Publicar resúmenes de datos sujetos a propiedad intelectual usados para entrenamiento

En caso de modelos de IA generales de alto impacto que puedan generar un riesgo sistémico, deberán ser evaluados y si sufren incidentes serios deben reportarse a la Comisión Europea.

Asimismo, el contenido generado y modificado con ayuda de IA debe ser etiquetado para que los usuarios tomen conocimiento de esa circunstancia.

- 3) Apoyo a la innovación. A través de la generación de condiciones que estimulen la prueba de modelos de IA previo a su puesta en producción.

Si bien aún no ha sido aprobado dado que la respuesta gubernamental al proceso participativo se produjo en febrero de 2024, también puede mencionarse en materia regulatoria el proyecto de Reino Unido²⁴, que se inició con White Paper en marzo de 2023, publicado por la Secretaría de Ciencia, Innovación y Tecnología. El objetivo del proyecto es alcanzar una aproximación que sea tanto pro-innovación como pro-seguridad.

El proyecto distingue 3 categorías: 1) riesgos sociales; 2) riesgos de mal uso; 3) riesgos de autonomía. Dentro de los primeros se hace referencia al mundo del trabajo, la innovación y la propiedad intelectual, la protección de las personas ante sesgos y discriminación, la protección de datos personales, confianza y seguridad en el contenido en línea, asegurar la competencia en los mercados digitales, mejores prácticas en el sector público. En cuanto al segundo tipo de riesgos se menciona salvaguardar la democracia de interferencia en los procesos electorales, prevenir el mal uso de la tecnología. Finalmente, en cuanto al último tipo de riesgos se menciona el alcance del control de las personas sobre los sistemas de IA.

²⁴ Por más información puede accederse a: <https://www.gov.uk/government/consultations/ai-regulation-a-pro-innovation-approach-policy-proposals/outcome/a-pro-innovation-approach-to-ai-regulation-government-response>. Últ. Acceso: 25/03/2023.



En octubre de 2023, el gobierno de los Estados Unidos emitió una Orden Ejecutiva en el Desarrollo Seguro y Confiable de la Inteligencia Artificial a ser aplicable por las agencias gubernamentales²⁵.

Dentro de las medidas previstas en la Orden Ejecutiva se encuentran:

1) Estándares en materia de Seguridad

- a) Requerir a desarrolladores de determinados sistemas que compartan información con el gobierno de Estados Unidos.
- b) Desarrollar estándares, herramientas y pruebas para asegurar que los sistemas son seguros y confiables antes de su puesta en producción.
- c) Protección contra los riesgos del uso de IA en materiales biológicos peligrosos.
- d) Protección a los americanos de fraudes y engaños habilitados por IA, Para ello se elaborarán guías de autenticación de contenido y marcas de agua para identificar contenido generado por IA.
- e) Establecer un programa avanzado de ciberseguridad para desarrollar herramientas de IA y colaborar en la detección y resolución de vulnerabilidades en software crítico.
- f) Ordenar el desarrollo de un Memorando de Seguridad Nacional para dirigir futuras acciones en IA y seguridad.

2) Protección de la privacidad de los estadounidenses

- a) Priorizar el apoyo federal para acelerar el desarrollo de tecnologías de preservación de la privacidad.
- b) Reforzar la investigación y tecnologías que preserven la privacidad
- c) Evaluar la forma en que las agencias recolectan y usan información disponible y reforzar las guías de privacidad para agencias federales

²⁵ El contenido de la Orden Ejecutiva puede consultarse en: <https://www.whitehouse.gov/briefing-room/presidential-actions/2023/10/30/executive-order-on-the-safe-secure-and-trustworthy-development-and-use-of-artificial-intelligence/> Últ.

Acceso: 24/03/2024.



- d) Desarrollar guías para que las agencias federales evalúen la efectividad de las técnicas de preservación de la privacidad
- 3) Avanzar en derechos civiles y equidad
 - a) Proveer guías para arrendadores, programas de beneficios federales y contratistas federales que eviten el uso de algoritmos discriminatorios
 - b) Atacar la discriminación algorítmica a través de asistencia técnica, coordinación y mejores prácticas
 - c) Asegurar la equidad en el sistema de justicia criminal
- 4) Proteger a los consumidores, pacientes y estudiantes
 - a) Avanzar en el uso responsable de IA en materia de salud
 - b) Diseñar recursos que apoyen la transformación de la educación a través de herramientas de IA.
- 5) Apoyo a los trabajadores
 - a) Desarrollar principios y buenas prácticas para mitigar los daños y maximizar los beneficios de IA para los trabajadores
 - b) Elaborar un reporte en el potencial impacto de la IA en el mercado laboral y estudiar e identificar opciones para reforzar al apoyo federal para trabajadores afectados por la IA
- 6) Promover la innovación y la competencia
 - a) Catalizar la investigación en IA en los Estados Unidos a través de un piloto de Recurso de Investigación Nacional en IA.
 - b) Promover un ecosistema justo, abierto y competitivo mediante asistencia técnica y recursos para pequeños desarrolladores.
 - c) Utilizar autoridades existentes para expandir las habilidades de inmigrantes y no inmigrantes altamente especializados con experiencia en áreas críticas para estudiar, permanecer y trabajar en Estados Unidos.
- 7) Avanzar en el Liderazgo de Estados Unidos en el extranjero



- a) Expandir los compromisos bilaterales, multilaterales, y multiactor para colaborar en IA.
 - b) Acelerar el desarrollo e implementación de estándares de IA vitales
 - c) Promover el desarrollo e implementación segura, responsable y centrada en derechos en el extranjero para resolver desafíos globales
- 8) Asegurar el uso gubernamental responsable y efectivo de la IA
- a) Establecer guías para el uso de IA por oficinas del gobierno
 - b) Apoyar a las agencias del gobierno para la adquisición de productos y servicios de IA
 - c) Acelerar la rápida contratación de profesionales de IA en el gobierno.

3.3 Diagnóstico preliminar en materia de IA y Derechos Humanos

Se considera pertinente orientar el diagnóstico en esta línea temática, en el análisis de 7 aspectos centrales, vinculados a los puntos mencionados por el Alto Comisionado de las Naciones Unidas para los Derechos Humanos, y detallados arriba.

1. ¿Sin perjuicio de que la aplicabilidad de las normas y principios de derechos humanos preexistentes en el ordenamiento jurídico al campo de la IA en lo pertinente, es necesario reforzar su aplicación a través de instrumentos normativos que expliciten y especifiquen su aplicación en este ámbito de manera transversal y/o como pilares de la política nacional más allá de la previsión establecida en el Art. 74 para la Estrategia Nacional en materia de IA?
2. ¿Es suficiente el enfoque de riesgos para atacar la problemática de la IA?
3. ¿Puede la autorregulación constituirse en un remedio efectivo para dirigir las acciones de entidades públicas y privadas en el desarrollo de IA?
4. ¿Existen sistemas de IA que por su impacto en los derechos de las personas deban ser prohibidos o limitados?



5. ¿Existe la posibilidad de imponer medidas especiales para determinados tipos de sistemas de IA?
6. ¿Cuáles son los alcances de la transparencia y explicabilidad a ser garantizados en el marco del desarrollo de sistemas de IA centrados en las personas?
7. ¿Cuáles son los criterios orientadores para la definición de la política pública asociada al desarrollo de la IA en nuestro país que permitirían potenciar el impacto positivo en los derechos humanos?

En relación al alcance en la aplicación de los principios, actualmente de conformidad con lo establecido en el artículo 74 de la Ley N° 20.212, estos son aplicables al diseño y desarrollo de la Estrategia Nacional de Inteligencia Artificial y de Datos. Ahora bien, y sin perjuicio de las normas del derecho internacional de derechos humanos ratificados por el país y las obligaciones internacionales derivadas en esta materia resultan aplicables al campo de la Inteligencia Artificial, en la medida en que estos principios fueron previstos expresamente en el artículo 74 en relación al desarrollo de las referidas Estrategias, corresponde considerar si resulta pertinente explicitarlos normativamente con un alcance más amplio. Esto es, especificar su contenido normativo específico en relación con la política de IA.

Los principios mencionados se encuentran alineados a los consagrados en el primer Convenio Internacional en la materia, elaborado por el Consejo de Europa (CoE), y que actualmente se encuentra en etapa de ratificación por el Comité de Ministros del citado organismo internacional, previo a su apertura a firma. En este convenio, se destacan los principios de dignidad humana y autonomía individual, transparencia y supervisión, responsabilidad y rendición de cuentas, equidad y no discriminación, privacidad y protección de datos personales, confianza y seguridad, e innovación segura. Los principios mencionados en el proyecto de Convenio del CoE se aplican según la propia definición de éste, a todos los sistemas de IA durante todo su ciclo de vida.

Con respecto al enfoque de riesgos, esta perspectiva se encuentra presente en otros aspectos vinculados al uso de datos -elemento central en el desarrollo de sistemas de IA-, como, por ejemplo, en el caso de la protección de datos personales regulada por la Ley N° 18.331. La regulación en protección de datos



personales puede ser aplicable a los sistemas de IA, cuando se utilicen datos personales para alimentar dichos sistemas.

Así, el artículo 12 de la Ley N° 18.331, en la redacción dada por el artículo 39 de la Ley N° 19.670, de 15 de octubre de 2018, prevé la realización de evaluaciones de impacto en la protección de datos personales. El artículo 6° del decreto N° 64/020, de 17 de febrero de 2020 es claro en promover la realización de este tipo de evaluaciones ante tratamientos de datos personales que generan mayores riesgos para las personas, y el artículo 7° indica el contenido mínimo del instrumento, enfatizando en la evaluación del riesgo y las medidas de seguridad a adoptar.

En particular, el artículo 6° literal c del decreto prevé la realización obligatoria de evaluaciones de impacto ante tratamientos que impliquen: “(...) *una evaluación de aspectos personales de los titulares con el fin de crear o utilizar perfiles personales, en particular mediante el análisis o la predicción de aspectos referidos a su rendimiento en el trabajo, situación económica, salud, preferencias o intereses personales, fiabilidad de comportamiento y solvencia financiera y localización*”. El literal d agrega que estas evaluaciones son obligatorias cuando se trate de “(...) *tratamiento de grandes volúmenes de datos personales*”. El vínculo con la IA es innegable, y la aplicación de estas disposiciones a sistemas de IA que realicen perfilamiento de personas o que empleen grandes volúmenes de datos para su entrenamiento resulta indiscutible, tanto en el ámbito público como privado.

En lo que respecta a la autorregulación, también las normas en protección de datos personales pueden servir para ejemplificar en el ámbito de los datos, cómo funcionan estos mecanismos. Los códigos de conducta previstos en el artículo 36 de la Ley N° 18.331 son un ejemplo de ello. Sin perjuicio de lo indicado, parece más conveniente adoptar algún esquema de co-regulación, que establezca normativamente determinadas líneas rojas que no deben traspasarse, y otros mecanismos de supervisión necesarios. Estas definiciones pueden observarse en el trabajo de MANTELERO²⁶, quien propone considerar los distintos ámbitos de actuación de los gobiernos y el alcance de la regulación, comparando las propuestas del Consejo de Europa y la Comisión Europea, e indicando que

²⁶ MANTELERO, Alessandro. “Beyond Data - Human Rights, Ethical and Social Impact Assessment in AI” en “IT&LAW 36”. Disponible en: https://link.springer.com/chapter/10.1007/978-94-6265-531-7_4. Últ. Acceso: 25/03/2024.



además de la aproximación co-regulatoria, las propuestas se decantan hacia una aproximación basada en riesgos más que en una basada en principios.

Corresponde, en base a lo analizado, considerar si en el marco de este enfoque, es posible determinar la existencia de líneas rojas que no podrán cruzarse en el uso de sistemas de inteligencia artificial.

En lo que respecta a la imposición de medidas especiales, también ello se vincula con el análisis de los impactos en los derechos de las personas, y se relaciona con otras medidas que puedan servir para una más efectiva supervisión del funcionamiento de los sistemas. Desde la creación de registros de algoritmos, hasta la solicitud de una autorización especial previa, o incluso la obligación de realizar pruebas en entornos controlados antes de la implementación de sistemas, pueden ser instrumentos útiles para determinados tipos de sistemas.

En lo que hace relación con la transparencia y explicabilidad, éste es uno de los principios más mencionados en el ámbito de la IA, y también de la gobernanza de los datos. El Grupo de Expertos de Alto Nivel para la Inteligencia Artificial de la Comisión Europea (AI HLEG), en su Guía Ética para una Inteligencia Artificial Confiable señala que la explicabilidad -elemento central de la transparencia junto a la trazabilidad y la comunicación- es la habilidad para explicar tanto los procesos técnicos de un sistema de IA como las decisiones humanas vinculadas.

La explicabilidad en materia de IA y Datos tiene hoy en día una consagración normativa expresa en dos disposiciones de la Ley N° 18.331, en el ámbito de la protección de datos personales.

En efecto, el artículo 13 de la citada ley prevé el Derecho a la Información, y en su literal G establece que la obligación de brindar información a los titulares de los datos por parte de responsables y encargados alcanza, en el caso de *“(…) tratamientos automatizados de datos regulados por el artículo 16 de la presente ley, los criterios de valoración, los procesos aplicados y la solución tecnológica o el programa utilizado”*.

El artículo 16 por su parte, consagra el derecho a la impugnación de valoraciones personales, señalando que: *“Las personas tienen derecho a no verse sometidas a una decisión con efectos jurídicos que les afecte de manera significativa, que se base en un tratamiento automatizado de datos destinado a evaluar determinados*



aspectos de su personalidad, como su rendimiento laboral, crédito, fiabilidad, conducta, entre otros.

El afectado podrá impugnar los actos administrativos o decisiones privadas que impliquen una valoración de su comportamiento, cuyo único fundamento sea un tratamiento de datos personales que ofrezca una definición de sus características o personalidad.

En este caso, el afectado tendrá derecho a obtener información del responsable de la base de datos tanto sobre los criterios de valoración como sobre el programa utilizado en el tratamiento que sirvió para adoptar la decisión manifestada en el acto”.

Resulta necesario determinar si la previsión de este artículo es suficiente, o si deben contemplarse otros mecanismos, adelantando desde ya que se estima necesario considerar efectivamente soluciones más amplias para sistemas de IA que no realicen tratamientos de datos personales, o cuyos destinatarios no sean titulares de datos, pero deban estar en conocimiento de su interacción con dichos sistemas.

Por su parte, deberían establecerse los criterios orientadores para la política pública en la materia, que podrían asociarse al cumplimiento de los principios, pero además a la provisión de herramientas prácticas que permitan el desarrollo innovador de sistemas de Inteligencia Artificial, el control de su ajuste a las normas en materia de derechos humanos, y los mecanismos de supervisión que sean necesarios para ello. En este punto, la competencia para la determinación de recomendaciones en la materia ha sido otorgada por la ley a la Institución Nacional de Derechos Humanos y Defensoría del Pueblo a través del artículo 4° de la Ley N° 18.446, de 24 de diciembre de 2008 y a la Secretaría de Derechos Humanos de conformidad con el artículo 67 de la Ley N° 19.149, de 24 de octubre de 2013, y en materia de datos personales a la Unidad Reguladora y de Control de Datos Personales por el artículo 34° de la Ley N° 18.331, de 11 de agosto de 2008.



4. Línea Propiedad Intelectual

4.1 Consideraciones preliminares

Se señala por la Organización Mundial de la Propiedad Intelectual (OMPI)²⁷ que el concepto de Propiedad Intelectual refiere a las creaciones del intelecto, desde las obras de arte hasta las invenciones, los programas informáticos, las marcas y otros signos comerciales. Esta se divide en dos categorías: la propiedad industrial (patentes de invención, marcas, diseños industriales e indicaciones geográficas) y el derecho de autor y derechos conexos (obras literarias, artísticas y científicas, incluidas las interpretaciones, ejecuciones y radiodifusiones). A los efectos del presente se considerarán además los secretos comerciales,

Las conexiones entre la Propiedad Intelectual y la innovación son innegables²⁸, así como los impactos de la Inteligencia Artificial sobre ésta²⁹. El Plan Nacional de Inteligencia Artificial de la República Argentina³⁰ por ejemplo, ha indicado que la propiedad intelectual, junto con la protección de datos personales y los derechos de los consumidores son regulaciones en tensión respecto de las cuales debe propenderse a un equilibrio regulatorio, por su trascendencia en el desarrollo y aplicación de la IA.

En este sentido, la OMPI publicó recientemente un documento que procura reflexionar sobre estos aspectos, y plantea que el punto de partida debe provenir de:

- 1) Entender si las leyes nacionales permiten que un sistema de IA sea nombrado como inventor o si es necesaria la intervención humana;

²⁷ Ver documento “¿Qué es la Propiedad Intelectual?” disponible en: <https://www.wipo.int/publications/es/details.jsp?id=4528>. Últ. Acceso: 25/03/2024.

²⁸ Ver al respecto el “Informe mundial sobre la propiedad intelectual 2022: La dirección de la innovación” publicado por OMPI en 2022 y disponible en: <https://www.wipo.int/edocs/pubdocs/es/wipo-pub-944-2022-es-world-intellectual-property-report-2022-the-direction-of-innovation.pdf>. Últ. Acceso: 25/03/2024.

²⁹ Ver documento: “Getting the Innovation Ecosystem Ready for AI An IP policy toolkit” publicado por IMPO y disponible en: https://www.wipo.int/about-ip/es/frontier_technologies/. Últ. Acceso: 26/03/2024.

³⁰ Disponible en: <https://oecd-opsi.org/wp-content/uploads/2021/02/Argentina-National-AI-Strategy.pdf> Últ. Acceso: 26/03/2024.



- 2) Analizar si el estado de situación permite incentivos, considerando los beneficios económicos y sociales que procuren obtenerse.

Además, plantea un conjunto de preguntas vinculadas a la forma de responder ante las invenciones generadas por la IA.

En el primer punto la OMPI plantea mirar más allá de la pregunta sobre quién debe ser el inventor y da una lista de alternativas: 1) reconocer sólo invenciones realizadas por humanos; 2) permitir que la IA sea nombrada como inventor o co-inventor; 3) requerir que una persona jurídica sea creada y designada como inventora o co-inventora cuando la creación se realizó por la IA; 4) establecer un nuevo esquema de leyes de Propiedad Intelectual para las creaciones generadas por IA.

En cualquier caso, la propuesta de OMPI es trabajar en una perspectiva de múltiples actores, que permitan considerar las distintas opiniones, previo a trabajar en modificaciones a la normativa en la materia.

En materia de IA y creaciones intelectuales, siguiendo el mismo documento de OMPI, deben distinguirse las creaciones asistidas por IA, las basadas en IA y las generadas en IA. MANTEGNA³¹ en este punto propone distintas alternativas a considerar, con el fin de regular las creaciones asistidas por IA y aquellas generadas por IA, que van en línea con las alternativas propuestas por OMPI.

Sin perjuicio de ello, y considerando lo indicado por la citada autora, parece relevante definir el alcance de esta línea a través de la consideración de la autoría en los derechos de autor, la propiedad industrial y los secretos comerciales, el vínculo de estos últimos con las medidas en materia de transparencia y explicabilidad -que forman parte de los principios considerados por la ley para la IA-, la propiedad de las bases de datos empleados para la generación de las creaciones, y las medidas a adoptarse desde el punto de vista regulatorio en las etapas de desarrollo e implementación de sistemas generativos de IA.

Por su parte, y dado el impacto de la propiedad intelectual en el ámbito de desarrollos aplicados por el Estado al utilizar la IA para la provisión de sus servicios

³¹ MANTEGNA, Micaela. "ARTEficial: Creatividad, Inteligencia Artificial y Derechos de Autor". Ed. CDYT, 2022. Págs. 299 y sigs..



y el cumplimiento de sus cometidos, resulta necesario incorporar este aspecto en el alcance definido en el presente.

Es pertinente señalar la relevancia de la materia a nivel internacional de la temática y su impacto en la innovación, como se refleja en la reciente Resolución la Asamblea General de las Naciones Unidas “Aprovechar las oportunidades de sistemas seguros, protegidos y fiables de inteligencia artificial para el desarrollo sostenible”³², que establece: “*Alentando, cuando resulte apropiado y pertinente, la aplicación de salvaguardias adecuadas a fin de respetar los derechos de propiedad intelectual, incluido el contenido protegido por derechos de autor, promoviendo al mismo tiempo la innovación*”.

4.2 Selección de antecedentes internacionales

Recientemente se presentó un proyecto de ley para modificar la normativa en materia de propiedad intelectual en Francia, que se encuentra a análisis en su Parlamento, vinculada al impacto de la IA³³. En dicho proyecto, se plantean en pocos artículos, algunas disposiciones de gran significación: 1) en su artículo 1° se establece que la integración y explotación posterior por un sistema de IA de obras protegidas por derechos de autor, está sujeta a las disposiciones generales en materia de autorización de los autores de las obras utilizadas; 2) el artículo 2° indica que cuando las obras son creadas por sistemas de IA sin intervención humana, éstas pertenecen a los autores o titulares de derechos de las obras originales, y agrega que su gestión puede ser realizada por sociedades de autores u otros organismos de gestión colectiva; 3) el artículo 3° impone la utilización de una mención específica en la obra creada por un sistema de IA que diga que dicha obra fue generada por esta tecnología, además de los nombres de los autores de las obras originales; 4) el artículo 4° prevé una forma de compensación particular para los casos en que no puedan determinarse el origen de las obras que sirvieron de base a la nueva creación del sistema de IA, a beneficio de organismos de gestión colectiva, dejando a la reglamentación su determinación.

³² Proyecto disponible en: <https://digitallibrary.un.org/record/4040897?v=pdf>. Últ. Acceso: 02/04/2024.

³³ Disponible en: https://www.assemblee-nationale.fr/dyn/16/textes/l16b1630_proposition-loi. Últ. Acceso: 26/03/2024.



En el caso de la legislación de Reino Unido, el artículo 9 (3) de la Ley de 1988 de Derechos de Autor, Diseños y Patentes³⁴ en materia de autoría, establece que cuando la obra literaria, dramática, musical o artística fue generada por computadora -definida esta por aquella en la que no existe un autor humano-, el autor debe entenderse que es la persona a través de la cual se efectuaron los arreglos necesarios para la realización de dicha obra.

Esta postura no es compartida en todas las jurisdicciones, y la dificultad actualmente es que existe un cúmulo de propuestas al respecto, pero mayormente la temática ha sido objeto de distintos pronunciamientos de órganos administrativos y judiciales con distintas respuestas según el caso. La nueva regulación de IA de la Unión Europea por ejemplo no se pronuncia en este tema - aunque sí contiene algunas disposiciones en materia de minería de datos-.

Atento a lo expresado, parece razonable en este sentido apoyarse en las opiniones de los distintos organismos internacionales y regionales en cuanto a la necesidad de explorar las alternativas desde una perspectiva multisectorial y pro innovación.

4.3 Diagnóstico preliminar en IA y Propiedad Intelectual

En este punto, es dable destacar que en nuestro país existe efectivamente normativa que regula la inscripción de programas de ordenador, compilaciones de datos u otros materiales que se constituyan en creaciones intelectuales, expresión de ideas, informaciones y algoritmos formuladas en secuencias originales ordenadas para ser usadas por un dispositivo de procesamiento de información o de control automático, pronunciándose la normativa vigente por la protección brindada a través de los derechos de autor.

Por otra parte, la normativa vigente habilita a que la inscripción de esos derechos se realice por una persona física o por una persona jurídica, incluyendo además al Estado. También la norma prevé la situación de obras anónimas y, siguiendo las disposiciones del Convenio de Berna, pone al editor, o al empresario en su caso, como titular del derecho de autor, mientras éste no descubra su incógnito. Pero aún en ese caso, no se trata de una discusión sobre la originalidad o la presunta

³⁴ Disponible en: <https://www.legislation.gov.uk/ukpga/1988/48/contents>. Últ. Acceso: 27/03/2024.



autoría por parte de una persona de esa obra, sino sobre el desconocimiento de los detalles de su identidad.

Tal y como señalan Alexander CUNTZ y ots³⁵, no sólo se trata de una determinación respecto a quién elaboró la obra sino cómo las creaciones generadas íntegramente por IA cambian la naturaleza del proceso de innovación y cómo ese cambio afecta el balance de la necesidad de recursos e incentivos en el ecosistema innovador.

No obstante, y desde la perspectiva de esta línea, resulta prudente preguntarse si es posible atribuir la titularidad de los derechos al sistema de IA -a través de una especie de personalidad electrónica-, o atribuírsela a una persona física o jurídica en particular -desarrollador, usuario u otros- o atribuirla a un conjunto de personas, o entender que ésta debe ser del dominio público.

El otro aspecto relevante a considerar es el empleo de datos de entrenamiento en los modelos de IA, a efectos de determinar si la normativa vigente -tanto por el potencial uso de datos protegidos por derechos de propiedad intelectual como por el uso de información personal protegida por las normas en protección de datos personales- es suficiente para atender las necesidades en materia de datos de estos sistemas o si se requieren excepciones especiales -como puede encontrarse en el proyecto de ley de IA de Brasil³⁶-.

Por otra parte, resulta importante determinar cómo operan las exigencias de transparencia y explicabilidad con los derechos de propiedad intelectual.

En lo que respecta al secreto comercial, existen distintas normas vinculadas al tema³⁷, siendo en especial de destacar lo dispuesto por el artículo 39 del ADPIC.

³⁵ CUNTZ, Alexander y ots. "Artificial Intelligence and Intellectual Property: An Economic Perspective". Editado por OMPI en el marco de los Documentos de Trabajo en Investigación Económica. N° 77/2024. Disponible en: <https://www.wipo.int/publications/en/details.jsp?id=4715>. Últ. Acceso: 26/03/2024.

³⁶ Disponible en: <https://www25.senado.leg.br/web/atividade/materias/-/materia/157233>. Ver en particular el artículo 42. Últ. Acceso: 27/03/2024.

³⁷ Un detalle de las normas en materia de secretos comerciales e industriales puede encontrarse en la siguiente publicación de la Unidad de Acceso a la Información Pública: <https://www.gub.uy/unidad-acceso-informacion-publica/politicas-y-gestion/informacion-secreta-definida-ley>. Últ. Acceso: 26/03/2024.



Este tema no es novedoso, ya que ha sido tratado en materia de datos personales en el artículo 13 y 16 de la Ley N° 18.331, en los casos de tratamientos automatizados de datos personales que elaboren, entre otros, perfiles de las personas. El artículo 13 de la ley de protección de datos prevé que los responsables que utilicen estos sistemas deberán brindar información los criterios de valoración, los procesos aplicados y la solución tecnológica o el programa utilizado. En el caso del artículo 16, se establece que en el marco de una impugnación por decisiones fundadas en una operación de perfilamiento podrá obtener información de la base de datos, los criterios de valoración y el programa utilizado.

Como ya se mencionó, recientemente la Ley N° 20.212 en su artículo 75 estableció la creación de entornos controlados de prueba para la puesta en práctica de proyectos tecnológicos de innovación. Si bien la norma no hace referencia a las cuestiones de propiedad intelectual, parece razonable entender que éste es uno de los aspectos centrales a considerar en la futura reglamentación.

Finalmente, resulta pertinente determinar si las normas en materia de propiedad intelectual en el uso de aplicaciones por parte del Estado reflejadas en forma indirecta en las disposiciones sobre Software Público deben aplicarse en materia de sistemas de Inteligencia Artificial.



5. Línea Infraestructura y Ciberseguridad

5.1 Consideraciones preliminares

El desarrollo de la Inteligencia Artificial depende de varios factores. Uno de los más relevantes es contar con una adecuada infraestructura, poseyendo el Estado a estos efectos un rol central.

El Ministerio de Inteligencia Artificial de los Emiratos Árabes Unidos publicó en noviembre de 2020 un reporte³⁸ sobre el estado de la infraestructura de hardware para IA en ese país, señalando que los elementos esenciales para apoyar la innovación en la materia se reducen a 3: a) infraestructura de datos -en especial su disponibilidad y la existencia de plataformas de almacenamiento de alta performance-; b) red -en especial sistemas de redes de alta performance especializadas que conecten los servidores entre sí y con las unidades de almacenamiento-; y c) la infraestructura de hardware -en especial plataformas computaciones y chips de computadoras que aceleren el proceso de entrenamiento y desarrollo de aplicaciones de IA y soporten grandes cantidades de memoria-.

La Organización para la Cooperación y el Desarrollo Económico (OCDE) publicó en febrero de 2023 su reporte N° 350³⁹ de la serie de economía digital, planteando recomendaciones para la construcción de capacidades computacionales para la Inteligencia Artificial, reconociendo en esta línea de acción un elemento central para el desarrollo y evolución de esta tecnología. En dicho documento se resalta la necesidad de que los países que desarrollen planes de IA realicen un adecuado análisis de las capacidades computacionales domésticas para alcanzar los objetivos diseñados.

En función del análisis realizado por OCDE, corresponde en este punto considerar: 1) la revisión de las capacidades computacionales especialmente para IA en actores del sector público y privado, considerando el uso de servicios de nube en

³⁸ Disponible en: https://ai.gov.ae/infrastructure_report/. Últ. Acceso: 28/03/2024.

³⁹ Disponible en: https://www.oecd-ilibrary.org/science-and-technology/a-blueprint-for-building-national-compute-capacity-for-artificial-intelligence_876367e3-en. Últ. Acceso: 28/03/2024.



el país o en el exterior; 2) considerar el número de centros de datos existentes, definir estándares en materia de datos, analizar las capacidades de procesamiento y las necesidades de hardware en el país, entre otros; 3) determinar la demanda potencial de procesamiento para IA, de forma de adelantarse a las necesidades y planear de forma acorde; 4) distinguir las necesidades de procesamiento para IA de otras; 5) proveer capacidades y entrenamiento para trabajadores; 6) mapear y analizar las cadenas de suministro necesarias de forma de construir planes de contingencia y resiliencia.

Las alternativas manejadas por la OCDE son sin duda atendibles a los efectos de asegurar la efectividad de la estrategia que se diseñe. No obstante, el alcance de este documento se relaciona con eventuales recomendaciones de corte normativo en el marco del informe previsto en el artículo 74 de la Ley N° 20.212.

Sin perjuicio de lo indicado, dichas recomendaciones nos permiten determinar un conjunto de aspectos respecto de los cuales deberá analizarse el estado de la normativa actual, y que son:

- 1) Normas asociadas a la infraestructura para la gestión y el intercambio de datos
- 2) Normas asociadas al almacenamiento de información
- 3) Normas asociadas a obligaciones en materia de ciberseguridad
- 4) Normas asociadas a las redes de telecomunicaciones

5.2 Selección de antecedentes internacionales

No se observan antecedentes normativos que contemplen expresamente esta circunstancia a nivel internacional, más allá de la mención de aspectos puntuales específicos y en forma aislada en las normativas y proyectos de normas existentes, no encontrándose presente en las distintas estrategias de IA relevadas. En esa medida se confirma lo expresado en el reporte de la OCDE N° 350, referido en el capítulo de alcance, cuando afirma que muchos países han desarrollado estrategias nacionales de IA sin haber analizado en forma completa si tienen la suficiente infraestructura computacional y software para IA suficiente a fin de alcanzar sus objetivos.



Merece una mención específica la iniciativa de Infraestructura Pública Digital promovida desde el PNUD, que se mencionara anteriormente, y que se vincula según esta entidad a una combinación de estándares abiertos construidos con un fin de interés público, habilitación de gobernanza y una comunidad de actores de mercado competitivos e innovadores para fomentar la innovación, en especial a lo largo de distintos programas públicos. Los impactos de esta forma de considerar determinados mecanismos aplicables a soluciones de transformación digital han sido relevados en distintos documentos y pueden colaborar en la determinación de la orientación que deben tener los esfuerzos para una IA sustentada en una infraestructura segura, soberana y proinnovación.

5.3 Diagnóstico preliminar en materia de Infraestructura y Ciberseguridad para IA

Existen en nuestro país una institucionalidad fuerte en materia de políticas de telecomunicaciones, ciberseguridad, interoperabilidad y datos. La distribución de las competencias entre las distintas entidades públicas involucradas se observa como adecuada, sin perjuicio de ser necesaria una mayor coordinación entre ellas.

Por otra parte, no se han encontrado análisis actuales vinculados a las compras en materia de infraestructura física, ni normativa que regule específicamente los requerimientos para adquisiciones de sistemas de IA por parte de entidades públicas, ni planes de adopción de IA desde la perspectiva de este documento, ni información objetiva asociada al uso de las infraestructuras físicas para estas actividades por parte de entidades públicas o privadas⁴⁰.

Y aquí, los procesos de compras planeados y la determinación de las necesidades de las entidades se observa como un punto central que debe ser considerado.

Al respecto, si bien no se incluyó en el relevamiento normativo realizado (Anexo 1), correspondería destacar dos normas que podrían ser de trascendencia en este punto, como lo son: a) el artículo 74 de la Ley N° 19.149, de 24 de octubre de 2013,

⁴⁰ Ello sin perjuicio de información sectorial que puede colaborar en la definición de políticas como el “Informe de Mercado de Telecomunicaciones de Uruguay” que publica periódicamente la URSEC disponible en: <https://www.gub.uy/unidad-reguladora-servicios-comunicaciones/datos-y-estadisticas/estadisticas/informes-mercado-del-sector-telecomunicaciones>. Últ. Acceso: 29/03/2024.



por el que se atribuye a Agesic el cometido de informar preceptivamente sobre los planes de desarrollo y adquisiciones informáticas de las dependencias de la Administración Central, y proponer al Poder Ejecutivo requisitos técnicos generales a exigirse en las adquisiciones de bienes y servicios informáticos; y b) el decreto N° 431/022, de 27 de diciembre de 2022, por el que se crea el Comité de Gobernanza de Procesos y Soluciones Transversales -integrado por varias entidades públicas y entre ellas Agesic- con el fin de ejercer la rectoría funcional y tecnológica de los sistemas de información transversales y las plataformas tecnológicas de uso compartido, vinculados con la gestión interna de los incisos de la Administración Central.

La planificación de las compras asociadas a la infraestructura necesaria para el desarrollo de la IA colaboraría además con el cumplimiento de otras normas como el decreto N° 339/021, de 4 de octubre de 2021 (Plan Anual de Contratación).

En lo que respecta a otros ámbitos como la capacitación de personal y la estructura de gobernanza de los datos, se considerarán en otras líneas de acción del informe que se elaborará.

Sí corresponde indicar en lo que respecta al almacenamiento de información, que el decreto N° 92/014, de 7 de abril de 2014 ha sido aplicado por las entidades públicas en general -no sólo las pertenecientes a la Administración Central, ya sea por referencia expresa a sus previsiones o por la adopción de normas similares en sus respectivos ámbitos- como argumento para evitar contratar servicios de procesamiento de datos en la nube. Desde Agesic se ha procurado brindar mayor claridad en cuanto a los alcances del decreto⁴¹, pero debería considerarse la posibilidad de una actualización, en línea con los criterios definidos al respecto por la Agencia⁴².

⁴¹ Ver en particular la "Guía de interpretación del Decreto 92/014 en Ciberseguridad" disponible en <https://www.gub.uy/agencia-gobierno-electronico-sociedad-informacion-conocimiento/comunicacion/publicaciones/guia-interpretacion-decreto-92014-ciberseguridad/guia-interpretacion> y el documento "Uso de la Nube en la Administración Pública" disponible en <https://www.gub.uy/agencia-gobierno-electronico-sociedad-informacion-conocimiento/comunicacion/publicaciones/uso-nube-administracion-publica/uso-nube-administracion-publica>. Últ. Acceso: 30/03/2024.

⁴² Ver al respecto documento de "Principios generales de la Nube Pública en el Estado". Disponible en: <https://www.gub.uy/agencia-gobierno-electronico-sociedad-informacion-conocimiento/comunicacion/publicaciones/principios-generales-nube-publica>



En lo que respecta a la infraestructura habilitante del intercambio de información, actualmente Agesic tiene a disposición la Plataforma de Interoperabilidad, regulada por el artículo 17 del decreto N° 178/013, de 11 de junio de 2013, con el fin de garantizar intercambios de información en soporte electrónico, de forma segura y confiable. Si bien dicha plataforma se orienta a entidades públicas, podría ser también empleada por entidades privadas, en cuyo caso debería de cumplirse con las condiciones establecidas por Agesic y por las entidades que expongan en ella sus servicios para el consumo de información.

Finalmente, en materia de ciberseguridad, está en proceso el desarrollo de la Estrategia Nacional, por lo que deberá estarse a lo incluido en ésta.



6. Línea trabajo y capacitación en IA

6.1 Consideraciones preliminares

Los impactos de la Inteligencia Artificial en el mundo del trabajo y en los trabajadores necesitan ser evaluados y abordados desde distintas perspectivas para aprovechar las oportunidades y abordar los desafíos emergentes.

Esta línea se focaliza exclusivamente en identificar las medidas a recomendar con el fin de promover el fortalecimiento de las habilidades de las personas en el campo de la IA orientadas a prevenir y mitigar los impactos negativos en el empleo y el mercado laboral y potenciar el aprovechamiento de la IA en beneficio de la sociedad.

En ese sentido, en el reporte elaborado por la Organización para la Cooperación y el Desarrollo Económicos titulado “Perspectivas de empleo de la OCDE 2023: La inteligencia artificial y el mercado laboral”⁴³ indica que el impacto de la IA generará cambios en las necesidades de habilidades, y existe actualmente falta de habilidades por lo que las políticas públicas desempeñarán un papel importante para incentivar la capacitación por parte de los empleadores, y por ser esta capacitación parte de la educación formal.

Ello es compartido por la Organización de las Naciones Unidas para la Educación, la Ciencia y la Cultura (UNESCO) en la Recomendación sobre la ética de la Inteligencia Artificial⁴⁴, a la que adhirió nuestro país, que dentro del ámbito de actuación 10 establecen la necesidad de ampliar las competencias básicas e interdisciplinarias en todos los niveles educativos asociados al uso ético de la IA, apoyar acuerdos de colaboración con instituciones educativas, la industria, la sociedad civil, las organizaciones de trabajadores para reducir brechas y generar estrategias de capacitación en medianas empresas, entre otros. También propone el trabajo con empresas para colaborar en las transiciones equitativas a empleados en situación de riesgo mediante programas de perfeccionamiento y

⁴³ Ver en particular el capítulo 5° sobre aptitudes, disponible en: <https://www.oecd-ilibrary.org/sites/638df49a-en/index.html?itemId=/content/component/638df49a-en>. Últ. Acceso: 31/03/2024.

⁴⁴ Disponible en: https://unesdoc.unesco.org/ark:/48223/pf0000380455_spa Últ. Acceso: 31/03/2024.



reconversión laboral, entre otros. Ello además de otras medidas vinculadas a la investigación, la competitividad de los mercados y protección de consumidores, la provisión de financiamiento cuando sea necesario, etcétera.

6.2 Selección de antecedentes internacionales

El gobierno español, a través del Decreto-ley N° 2/2023, de 8 de marzo de 2023 estableció algunas medidas urgentes de impulso a la IA en la comunidad autónoma de Extremadura⁴⁵. En su artículo primero establece como finalidad principal y como carácter general elevar la capacidad técnica en IA a través de la alfabetización de la población incluyendo la formación de población activa y empleados públicos. Para ello, se propone la promoción del desarrollo de capacidades emprendedoras, creativas, sociales y culturales, el impulso de medidas de apoyo a empresas que realicen planes de formación y capacitación en la materia, y la inclusión de esta formación para personas desempleadas y para funcionarios públicos.

La Orden Ejecutiva para el Desarrollo Seguro y Confiable de IA⁴⁶ dictada en Estados Unidos sobre la materia, dentro de la Sección 10 (Avanzando hacia el uso de IA en el Gobierno Federal) plantea al más alto nivel de las agencias del gobierno federal, la implementación de programas de entrenamiento y familiarización en IA para empleados, gerentes y líderes, entre otros. Esos programas deberán empoderar a los empleados y otros a desarrollar y mantener el conocimiento operativo en tecnologías emergentes de IA. Asimismo, propone que las agencias provean oportunidades de desarrollo profesional, becas, fondos, para su personal.

6.3 Diagnóstico preliminar en materia de trabajo y capacitación para la IA

Existen distintas disposiciones a nivel nacional que prevé la promoción de la capacitación entre los trabajadores. Sin embargo, de la normativa analizada en principio no se desprende un énfasis particular en aspectos vinculados a la IA y la forma de gestionar sus impactos.

⁴⁵ Disponible en: <https://www.boe.es/buscar/doc.php?id=BOE-A-2023-8795>. Últ. Acceso: 31/03/2024.

⁴⁶ Disponible en: <https://www.whitehouse.gov/briefing-room/presidential-actions/2023/10/30/executive-order-on-the-safe-secure-and-trustworthy-development-and-use-of-artificial-intelligence/>. Últ. Acceso: 31/03/2024.



En ese sentido, se estima que la institucionalidad existente permitiría llevar adelante políticas y programas vinculados a esta temática, y explorar alternativas de cooperación entre entidades públicas y privadas.

Visibilizar la problemática, establecer acciones coordinadas, definir una política específica e instrumentar una cooperación sostenida entre los distintos actores del ecosistema deben ser considerados a efectos de llevar adelante una estrategia exitosa en la materia.

Documento para consulta



7. Línea responsabilidad civil y derechos del consumidor

7.1 Consideraciones preliminares

La Inteligencia Artificial plantea interrogantes de difícil solución para muchos operadores jurídicos que, en países como el nuestro, procuran interpretar normas que -si bien es claro brindan la seguridad jurídica necesaria- fueron sancionadas en una realidad muy distinta a la actual.

La línea que se plantea en este punto refiere a dos aspectos que normativamente se encuentran bien regulados, como son la responsabilidad civil y las relaciones de consumo.

DE CORES⁴⁷, al analizar la función preventiva de la responsabilidad civil en nuestro derecho, indica que el propio concepto se señala como de “(...) *de gran polisemia, pero que en sentido amplio, puede definirse como la consecuencia que adviene por el incumplimiento de una norma, pudiendo así existir una responsabilidad no sólo civil sino penal, administrativa, e incluso política o moral*”.

JOSÉ DOS SANTOS⁴⁸ afirma que “(...) *la responsabilidad civil tiene la función de reestablecer el equilibrio, comprometido por la ocurrencia de daños morales o materiales causados por el agente causal*” y destaca que en el derecho brasileño, existe una responsabilidad civil subjetiva -que requiere una conducta maliciosa o culpable o una omisión por el autor de dicha conducta- y una responsabilidad objetiva -en la que basta la prueba del nexo causal entre la conducta y el daño, sin considerar la intención o culpa de quien lo causó-.

La autora se plantea qué ocurre con la responsabilidad civil de la IA, concluyendo respecto de la necesidad de considerar si los institutos actuales pueden responder a la evolución de ésta.

Dentro del concepto de responsabilidad civil, la distinción más común es la realizada entre la contractual -derivada del incumplimiento de un contrato entre dos

⁴⁷ DE CORES, Carlos. “La denominada función preventiva de la responsabilidad civil. Una crítica a su ubicación dogmática”. Disponible en: <https://eva.fder.udelar.edu.uy/mod/resource/view.php?id=49243&redirect=1>. Últ. Acceso: 30/03/2024.

⁴⁸ JOSÉ DOS SANTOS, Sonia “Inteligencia Artificial y Responsabilidad Civil” en “Inteligencia Artificial y Derecho” 1^ª. Ed. Ed. Hammurabi. 2020. Pág. 179 y sigs.



o más partes- o extracontractual -derivada del perjuicio ocasionado a alguien, sin existir dicho vínculo contractual-. El régimen de responsabilidad civil, como se verá más adelante, se encuentra regulado en Uruguay fundamentalmente en nuestro Código Civil.

En el caso de las relaciones de consumo, estas se encuentran definidas en el artículo 4° de la Ley N° 17.250, de 11 de agosto de 2000, como el vínculo entre el proveedor que a título oneroso provee un producto o presta un servicio y quien lo adquiere o utiliza como destinatario final. Se encuentra aquí desde el punto de vista subjetivo las figuras de proveedor y consumidor.

ARAMENDIA⁴⁹ señala que en el uso de la IA y los eventuales daños que puedan producirse por la utilización de estos sistema, existen 2 extremos a considerar: la inseguridad de las personas que son dañadas por el producto o servicio que contiene IA respecto a cómo proceder para ser indemnizadas, y la inseguridad de los diseñadores, desarrolladores, productores, financiadores, y demás integrante de la cadena que llevó ese producto o servicio al mercado respecto a su rol en la producción del evento dañoso.

Plantea la autora 3 retos: 1) la complejidad de los sistemas y la diversidad de factores que pueden ocasionar el error que a su vez ocasionó el daño; 2) la multiplicidad y diversidad de actores en la cadena, dificultando la trazabilidad; 3) el mecanismo para seguir impulsando la inversión, investigación y desarrollo en IA y a su vez asegurar a los que sufren un daño que podrán acceder a una justa indemnización.

Es precisamente la respuesta a esos tres retos lo que se procurará considerar en el presente, desde una perspectiva estrictamente normativa. Quedan fuera del alcance los impactos que la IA pueda tener en las relaciones de consumo, por cuanto de lo que se hará referencia en esta línea es de la problemática asociada a la responsabilidad de los proveedores y la reparación de daños a los consumidores.

⁴⁹ ARAMENDIA, Mercedes. "La Inteligencia Artificial ¿y la responsabilidad?" en "Estudios sobre los Desafíos Jurídicos ante la Digitalización" Tomo III. Coord. Mercedes Aramendía y Agustina Pérez Comenale. Ed. UM. Año 2023. Págs. 557 y sigs.



7.2 Selección de antecedentes internacionales

Resulta en este punto relevante considerar la propuesta de Directiva sobre Responsabilidad de la IA de la Unión Europea⁵⁰, que complementa el Reglamento recientemente aprobado. Señala CASALS⁵¹ que *“La Propuesta de Directiva actual, en cambio, se refiere solo a la responsabilidad por dolo o culpa por daños causados por sistemas de IA, que continúa estando sujeta a las reglas sustantivas nacionales. Por esa razón, no entra en conflicto ni con la aplicación de las normas nacionales ni con las derivadas de la Directiva sobre responsabilidad por los daños causados por productos defectuosos y, como se ha señalado, su ámbito objetivo es mucho más amplio”*. En este punto, la Comisión Europea⁵² ha señalado que: *“La Directiva simplifica el proceso jurídico para las víctimas a la hora de demostrar que la culpa de una persona ha provocado los daños, al introducir dos características principales: en primer lugar, en circunstancias en las que se haya probado una culpa pertinente y parezca razonablemente probable que exista un nexo causal con el rendimiento de la IA, la denominada «presunción de causalidad» abordará las dificultades experimentadas por las víctimas para tener que explicar detalladamente la manera en que se ha provocado el daño por una culpa u omisión concretas, lo que puede ser especialmente difícil al intentar comprender y lidiar con sistemas de IA complejos. En segundo lugar, las víctimas dispondrán de más herramientas para solicitar reparación legal gracias a la introducción de un derecho de acceso a las pruebas presentadas por empresas y proveedores, en los casos en que esté implicada IA de alto riesgo”*.⁵³

⁵⁰ Disponible en: <https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=CELEX%3A52022PC0496>. Últ. Acceso: 30/03/2024.

⁵¹ CASALS, Miguel Martín. “Las propuestas de la Unión Europea para regular la responsabilidad civil por los daños causados por sistemas de inteligencia artificial”. Disponible en: <https://indret.com/las-propuestas-de-la-union-europea-para-regular-la-responsabilidad-civil-por-los-danos-causados-por-sistemas-de-inteligencia-artificial/>. Últ. Acceso: 30/03/2024.

⁵² Disponible en: https://ec.europa.eu/commission/presscorner/detail/es/ip_22_5807. Últ. Acceso: 30/03/2024.

⁵³ Un análisis más extenso puede verse en La Ley Digital, artículo de Gonzalo ITURMENDI MORALES “Responsabilidad civil por el uso de sistemas de inteligencia artificial” disponible en <https://laleydigital.laleynext.es/Content/Documento.aspx?params=H4slAAAAAAAEAMtMSbF1CTEAAmNDCwsjl7WY1KLizPw8WYMDlwNDQyMDkEBmWqVLfnJIZUGqbVpiTnEqANKvjtl1AAAAWKE>. Últ. Acceso: 30/03/2024.



Un proyecto de ley presentado en la República Argentina⁵⁴ establece en sus artículos 19 a 23 un régimen de responsabilidad por daño o error de uso. Se plantea en el proyecto la responsabilidad de los desarrolladores y proveedores por los errores de uso de sus sistemas que causen daño si no han tomado medidas razonables para evitar el error o si han incumplido con las regulaciones y estándares establecidos, debiendo implementar medidas de seguridad y pruebas. Se prevé también la responsabilidad de los usuarios por el uso adecuado de los sistemas y de acuerdo con las instrucciones proporcionadas, con la diligencia debida; los usuarios serán responsables por daño a terceros en caso contrario. Se incluye además la obligación de contar un seguro de responsabilidad civil adecuado para cubrir posibles daños. Finalmente, existen normas en materia de transparencia y capacitación, y un mecanismo de denuncia de errores de uso de la inteligencia artificial.

No existen tampoco en este tema antecedentes normativos relevantes, más allá de las disposiciones del proyecto de directiva de la Unión Europea. Ello motiva a reflexionar sobre la necesidad de contar con un análisis específico y multi-actor de la legislación uruguaya, dada la sensibilidad que posee la estructura de responsabilidad civil para la seguridad jurídica.

7.3 Diagnóstico preliminar

El primer punto del diagnóstico es que claramente las normas no establecen una regulación específica para la problemática derivada de los daños que potencialmente puedan ocasionar los sistemas de IA. Salvo que el régimen de responsabilidad esté establecido claramente en los términos de un contrato, la regulación general en materia de responsabilidad civil que podría ser aplicable por analogía a buena parte de las situaciones derivadas del uso de sistemas de IA -en los que existe gran complejidad en la determinación de los integrantes de la cadena que deriva en la puesta en producción de un producto o servicio- es el artículo 1330 del Código Civil, que regula una especie de responsabilidad colectiva asociada a cosa que cae de un edificio. Dicho análisis en forma general, y su

⁵⁴ Disponible en: <https://www4.hcdn.gob.ar/dependencias/dsecretaria/Periodo2023/PDF2023/TP2023/2505-D-2023.pdf>. Últ. Acceso: 30/03/2024.



aplicación en vía analógica fue elaborado oportunamente por BORDOLI⁵⁵, aunque no relacionado específicamente al tema que nos ocupa sino a la asignación de responsabilidad en caso de que existe un grupo individualizado integrado por varias personas pero dónde no es posible identificar en concreto quien ocasionó el daño.

Este régimen parece ser insuficiente para realizar una adecuada adjudicación de responsabilidad a quienes ocasionaron el evento dañoso y una reparación del daño efectivo a las personas.

En el caso de las relaciones de consumo, será de aplicación el mencionado artículo 34 de la Ley N° 17.250, de 11 de agosto de 2000, que dispone: *“ Si el vicio o riesgo de la cosa o de la prestación del servicio resulta un daño al consumidor, será responsable el proveedor de conformidad con el régimen dispuesto en el Código Civil.*

El comerciante o distribuidor sólo responderá cuando el importador y fabricante no pudieran ser identificados. De la misma forma serán responsables si el daño se produce como consecuencia de una inadecuada conservación del producto o cuando altere sus condiciones originales”.

Otro aspecto a considerar refiere al daño ocasionado cuando el producto o servicio es ofrecido desde el Estado, siendo en dicha situación de aplicación lo dispuesto en los artículos 24 y 25 de la Constitución, como se indicó.

⁵⁵ BORDOLI, Carlos Rubens. “Responsabilidad Extracontractual Colectiva por Daño Causado por un Miembro Indeterminado de un Grupo” disponible en Revista de la FDER (30). Año 2014. Págs. 65 y sigs. Disponible en formato electrónico en: <https://revista.fder.edu.uy/index.php/rfd/article/view/87>. Últ. Acceso: 30/03/2024.



8. Línea de medidas de promoción para la IA

8.1 Consideraciones preliminares

El objetivo de esta línea es considerar el alcance y determinación de eventuales medidas de promoción asociadas a una política pública en IA.

¿Por qué plantear medidas de promoción de la IA? La respuesta se encuentra en los beneficios comprobados que esta tecnología puede tener para la sociedad. Si bien existe un énfasis en alertar sobre los potenciales riesgos que ella encarta para las personas, resulta también relevante ponderar sus múltiples beneficios.

Puede considerarse al respecto el reporte interino del Cuerpo Asesor en Inteligencia Artificial de la Organización de las Naciones Unidas de diciembre de 2023⁵⁶, que establece un conjunto de recomendaciones preliminares basadas en 5 principios: 1) gobernanza inclusiva, por y para el beneficio de todos; 2) gobernanza para el interés público; 3) gobernanza construida en conjunto con la gobernanza de datos y la promoción de los bienes comunes; 4) gobernanza universal, en red y arraigada a la colaboración de múltiples partes interesadas; 5) gobernanza anclada en la Carta de las Naciones Unidas, el derecho internacional de los Derechos Humanos y otros compromisos internacionales acordados como los Objetivos de Desarrollo Sostenible. Este documento, en cuanto a la promoción de la IA para la Humanidad, señala, entre otros, la necesidad de que el acceso y los beneficios vayan juntos, mediante la inversión nacional en talento, datos y recursos computacionales. Para ello se observa como relevante la cooperación y asistencia internacional en los sectores público y privado.

En definitiva, se procura considerar la pertinencia y alcance de eventuales medidas de promoción de IA, teniendo en cuenta: 1) la determinación de los objetivos a los que se dirija la promoción efectiva de la Inteligencia Artificial, poniendo como centro los desarrollos que colaboren a la construcción de una sociedad más justa y equitativa; 2) los instrumentos concretos que podrían emplearse a efectos de otorgar beneficios que colaboren en el desarrollo de los sistemas que se visualicen como destinatarios de dichos beneficios.

⁵⁶ Disponible en https://www.un.org/sites/un2.un.org/files/ai_advisory_body_interim_report.pdf. Últ. Acceso: 04/04/2024.



8.2 Selección de antecedentes internacionales

Dentro de los puntos más relevantes de la Orden Ejecutiva en el Desarrollo Seguro y Confiable de la Inteligencia Artificial a ser aplicable por las agencias gubernamentales de los Estados Unidos⁵⁷ se encuentra la promoción de la innovación y la competencia, a través de.

- a) Catalizar la investigación en IA en los Estados Unidos a través de un piloto de Recurso de Investigación Nacional en IA.
- b) Promover un ecosistema justo, abierto y competitivo mediante asistencia técnica y recursos para pequeños desarrolladores.
- c) Utilizar autoridades existentes para expandir las habilidades de inmigrantes y no inmigrantes altamente especializados con experiencia en áreas críticas para estudiar, permanecer y trabajar en Estados Unidos.

Lo antedicho sin perjuicio de otros puntos como la cooperación internacional y la colaboración entre entidades dentro del gobierno.

Por su parte, la propuesta de Ley de IA de la Unión Europea⁵⁸ señala expresamente el vínculo entre la gobernanza de datos, los datos abiertos y la promoción de la innovación impulsada por la IA. Dentro de las medidas de apoyo a la innovación propuestas se encuentran el desarrollo de espacios controlados de pruebas para IA, la habilitación de tratamientos de datos con determinadas finalidades, y algunas medidas para proveedores y usuarios a pequeña escala que van desde acceso prioritario a espacios controlados de prueba, actividades de sensibilización, canales específicos de comunicación y eventualmente, montos de tasas diferenciales para determinados servicios.

⁵⁷ El contenido de la Orden Ejecutiva puede consultarse en: <https://www.whitehouse.gov/briefing-room/presidential-actions/2023/10/30/executive-order-on-the-safe-secure-and-trustworthy-development-and-use-of-artificial-intelligence/> Últ. Acceso: 04/04/2024.

⁵⁸ Contenido disponible en <https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=celex:52021PC0206>. Últ. Acceso: 04/04/2024.



En Brasil, el proyecto de ley N° 2338/2023⁵⁹ pone énfasis en la promoción de la investigación y desarrollo con el fin de estimular la innovación en sectores productivos y en el poder público. También dentro de las medidas previstas se encuentra la creación de sandboxes regulatorios y las bases de datos públicas de inteligencia artificial.

Existen otras disposiciones a nivel internacional que comparten los criterios en materia de promoción reflejados en el presente, donde se incluye el concepto de desarrollo de la innovación, subrayando así el rol de los entornos controlados de prueba en ese sentido.

8.3 Diagnóstico preliminar

Actualmente existen pocas disposiciones que refieren específicamente a la promoción de la innovación en el campo de la IA. Se está elaborando a la fecha de este documento la reglamentación del artículo 75 de la Ley N° 20.212, por lo que se tendrán en cuenta las consideraciones realizadas en el marco del presente análisis.

Por otra parte, corresponde considerar la existencia de otro tipo de medidas que podrían ser eficientes para promover la innovación y sus desarrollos, tales como exoneraciones tributarias, análisis y promoción de sellos que acrediten la realización de auditorías y evaluaciones que permitan a su vez acceder a determinados beneficios, entre otros, todos estos elementos que requieren un análisis particular.

⁵⁹

Disponible

en

https://legis.senado.leg.br/sdleg-getter/documento?dm=9347622&ts=1702407086098&disposition=inline&_gl=1*1wg6j22*_ga*NTk0MjQwOTMwLjE3MDE3OTA5MTc.*_ga_CW3ZH25XMK*MTcwNjYxODMwOS4yLjEuMTcwNjY0NDgxOC4wLjAuMA. Últ. Acceso: 04/04/2024.



9. Aportes relevados de otras entidades públicas en la primera etapa de discusión

En el marco del proceso de construcción del informe del artículo 74 de la Ley N° 20.212 se realizaron varias reuniones con las entidades mencionadas en el presente documento, de las que pueden resumirse los siguientes aportes:

Línea Institucionalidad y gobernanza

Se plantea:

- La necesidad de un enfoque transversal, sin perjuicio de lo cual es importante contar con un organismo líder en la materia.
- Contar con un comité asesor, con el rol de asesoramiento en temáticas específicas y con la integración de distintos actores de acuerdo con las temáticas a abordar (por ejemplo, sector privado, organizaciones de sociedad civil, empresas de telecomunicaciones, empresas vinculadas al desarrollo de sistemas de IA, entre otros). Se plantea que el Comité integre grupos ad hoc, de acuerdo con la temática específica a abordar o de lo contrario convocar a expertos en el sector o área a considerar.
- Involucrar como aspectos a integrar en el análisis la defensa al consumidor, defensa al usuario, y la consideración de la persona como ciudadano digital (generador y usuario de IA)
- Integrar los datos en materia de telecomunicaciones, y contemplar este punto como servicio crítico.
- Incorporar en las discusiones al Ministerio de Defensa Nacional (MDN) por la defensa y el uso de la IA para ello, así como al Ministerio del Interior (MI) por aspectos de seguridad pública.
- Aplicar el mecanismo de las consultas públicas, con el fin de ampliar los actores involucrados, obteniendo y/o integrando otras visiones.
- Incluir y trabajar en el fortalecimiento de pequeñas y medianas empresas.



Línea Derechos Humanos

Se plantea:

- Considerar la generación de políticas para los sistemas de IA.
- En cuanto a la población vulnerable, prestar especial atención a niñas, niños, adolescentes y adultos mayores.
- Especificación respecto a que la toma de la decisión final sea de un humano, no del algoritmo y posibilidad de incorporar auditorías para analizar el impacto de la aplicación de la IA, y que las mismas sean institucionalizadas.
- Analizar la etapa del ciclo del proceso en la que debería presentarse una eventual auditoría.
- Determinar un organismo y/o institución que controle de forma independiente y para determinados casos de riesgos y/o de alto impacto.
- Analizar la viabilidad y/o pertinencia de dotar de mayores competencias a la INDDHH o establecer algún mecanismo de garantía en materia de DDHH.
- Incorporar una línea de trabajo que integre la IA para facilitar el acceso a los servicios del Estado.
- Identificando la importancia del sector trabajo, analizar cómo las empresas podrían tener un rol propositivo, planteando alternativas ante el reemplazo del trabajo humano por la IA, por ejemplo, a través de capacitaciones para abordar otras tareas y uso de nuevas tecnologías.
- Analizar el abordaje de los impactos ambientales.
- Considerar el enfoque de riesgos.

Línea trabajo y capacitación para IA

Se plantea:

- Hacer énfasis en el impacto en el empleo específicamente y en términos generales en el mundo del trabajo.



- Contemplar toda la Normativa Laboral Vigente (en particular normas en materia de combate a la discriminación en el ámbito laboral).

Línea Propiedad intelectual

Se plantea:

- Generar mayor discusión sobre el tema autoría e incorporar el tema plagio.
- Analizar el desarrollo de las excepciones para el uso de determinados datos como entrenamiento, y hacer salvaguardas cuando se trata de derechos de autor, definiendo su alcance y finalidad.
- Discutir una reforma a la Ley de derechos de autor N° 9739 a fin de contemplar la incidencia de la IA en la materia.
- En materia de patentes con intervención de IA, analizar la necesidad o no de indicar en la solicitud de patentes cómo interviene la IA en el proceso inventivo.
- Incentivar acciones para el desarrollo de la Propiedad intelectual.

Línea Responsabilidad Civil y derechos del consumidor

Se plantea:

- Determinar el alcance de la normativa vigente a efectos de contemplar los daños eventuales ocasionados en el uso de sistemas de IA y profundizar su análisis previo a la realización de propuestas normativas.
- Analizar la posibilidad de generar sensibilización hacia la ciudadanía, para que las personas puedan identificar cuando están en una relación de consumo vinculado a IA, así como que mecanismos existen para realizar reclamos y/o denuncias.

Línea Infraestructura y ciberseguridad

Se plantea:

- Definir claramente el concepto de IA aplicada al tema de infraestructura y ciberseguridad.



- Considerar temas como, el uso de reservorios de datos a nivel internacional, en el ámbito público y privado.
- Considerar y analizar la calidad de Software y Hardware en las instituciones públicas.
- Identificar otros tipos de empresas como las de servicios de almacenamiento.
- Considerar la IA aplicada a la normalización de la infraestructura de telecomunicaciones.
- Analizar la posibilidad de centros de capacidad de cálculo por región.
- Evaluar aspectos medioambientales y de uso de recursos naturales.
- Evaluar las capacidades del país en cada uno de los siguientes puntos:
 - o Normas para gestión e intercambio de datos
 - o Capacidad de almacenamiento, capacidad de cómputos
 - o Ciberseguridad
 - o Capacidad de conectividad e infraestructura: escalabilidad, flexibilidad y adaptabilidad a los cambios

Línea Medidas de promoción

Se plantea:

- Analizar y definir objetivos estratégicos a nivel nacional para el uso de la IA.
- Relevar medidas de promoción existentes en esta materia y en distintos aspectos vinculados a la IA.
- Analizar la posibilidad de contar con infraestructura a nivel nacional donde realizar pruebas (sandboxes y otros).
- Analizar la posibilidad de exoneraciones, incentivos tributarios asociados a la promoción del desarrollo y uso de la IA orientado a objetivos estratégicos del país en distintos ámbitos.



Sin perjuicio de lo indicado, corresponde señalar que en el marco del proceso de revisión de las temáticas se recibieron además aportes por escrito de algunas de las instituciones involucradas en el proceso, que serán detallados e incorporados en el informe final.

Adicionalmente, Agesic ha elaborado un conjunto de recomendaciones que fueron discutidas con los participantes de las distintas líneas, y serán presentadas conjuntamente con el informe final.

Documento para consulta



Anexo 1: Normativa

Institucionalidad de IA

Normas aplicables	Resumen de contenido
Artículo 74 Ley N° 20.212, de 6 de noviembre de 2023	Pone de cargo de Agesic el diseño y desarrollo de una estrategia nacional de datos y de IA. Además, en el inciso final se establece expresamente que ésta realizará recomendaciones específicas a entidades del sector público y del sector privado para el desarrollo e implementación de los sistemas de inteligencia artificial mencionados, y para la fiscalización de su cumplimiento, sin perjuicio de las competencias propias de la URCDP y de otras entidades públicas en sus respectivos ámbitos de actuación.
Artículo 34 Ley N° 18.331, de 11 de agosto de 2008, en la redacción dada por el artículo 63 de la Ley N° 20.075, de 20 de octubre de 2022.	Establece dentro de los cometidos de la URCDP el de establecer los criterios y procedimientos que deban observar los responsables y encargados, en el tratamiento automatizado de datos personales indicados en el artículo 16 de la ley N° 18.331.

Gobernanza de datos

Normas aplicables	Tema	Resumen de contenido
Ley N° 18.331, de 11 de agosto de 2008, modificativas y concordantes, y N° 19.670, de 15 de octubre de 2018.	Datos Personales	Se establecen las formas de tratamiento de los datos personales en el sector público y privado, asociados a un conjunto de principios.



Reglamentados por decretos N° 414/009, de 31 de agosto de 2009, y 64/020, de 17 de febrero de 2020.		
Ley N° 18.381, de 17 de octubre de 2008. Norma reglamentada por decreto N° 232/010, de 2 de agosto de 2010.	Información Pública	Se establece el carácter público de la información en poder del Estado, así como sus excepciones.
Artículos 157 a 160 de la Ley N° 18.719, de 27 de diciembre de 2010	Interoperabilidad e intercambio	Se establecen las condiciones para la interoperabilidad y el intercambio de información pública y privada en los términos de la reglamentación. Norma reglamentada por decreto N° 178/013, de 11 de junio de 2013.
Decreto N° 259/012, de 13 de agosto de 2012	Datos abiertos y Gobierno Abierto	Uruguay se adhiere a la "Declaración sobre Gobierno Abierto" de la "Sociedad de Gobierno Abierto" y se establece el primer plan de acción, que fue sucedido por otros planes posteriores.
Artículo 82 de la Ley N° 19.355, de 19 de diciembre de 2015	Datos Abiertos y Gobierno Abierto	Se establece la obligación de los organismos públicos de publicar la información contenida en el artículo 5° de la Ley N° 18.381, en formato de datos abiertos. Norma reglamentada por decreto N° 54/017, de 20 de febrero de 2017.



<p>Artículo 76 de la Ley N° 19.355, de 19 de diciembre de 2015 en la redacción dada por el artículo 2 de la Ley N° 19.670, de 15 de octubre de 2018</p>	<p>Interoperabilidad e intercambio</p>	<p>Se establece la obligación de los organismos públicos de no solicitar certificados, constancias, testimonios u otra documentación de similar naturaleza emitidos por otra entidad pública, cuando se pueda acceder a la información contenida en dichos documentos, a través de sistemas informáticos proporcionados por las entidades competentes. Norma reglamentada por decreto N° 353/023, de 9 de noviembre de 2023.</p>
<p>Decreto N° 357/016, de 7 de noviembre de 2016</p>	<p>Datos Abiertos y Gobierno Abierto</p>	<p>Se crea el Grupo de Trabajo de Gobierno Abierto integrado por un representante de cada uno de los siguientes organismos: Agesic, OPP, UAIP. MEF, MRREE, MIEM e INE. Se establecen además sus cometidos.</p>

Aplicación de principios en IA

Normas	Resumen de contenido
<p>Artículo 74 Ley N° 20.212, de 6 de noviembre de 2023</p>	<p>Pone de cargo de Agesic el diseño y desarrollo de una estrategia nacional de datos y de IA. El artículo en su inciso segundo establece que “<i>(l)a estrategia deberá fundarse en principios de equidad, no discriminación, responsabilidad, rendición de cuentas, transparencia, auditoría e innovación segura, respetando la dignidad humana, el sistema democrático y la forma republicana de gobierno. Los principios de la protección de datos personales incluidos en la Ley N° 18.331, de 11 de agosto de 2008, serán parte de la citada estrategia</i>”.</p>
<p>Artículo 5° Ley N° 18.331, de 11 de agosto de 2008.</p>	<p>El artículo establece dentro como principios de la protección de datos personales, que el artículo 74 incluye en la Estrategia de IA, los siguientes: legalidad, veracidad,</p>

	finalidad, previo consentimiento informado, seguridad de los datos, reserva y responsabilidad (proactiva).
--	--

Propiedad Intelectual

Normas aplicables	Resumen de contenido
Constitución Nacional, art. 33	Establece que el trabajo intelectual, el derecho del autor, del inventor o del artista, serán reconocidos y protegidos por la ley
Ley N° 9.739, de 17 de diciembre de 1937, modificada por Leyes N° 17.616, de 10 de enero de 2003, 19.857, de 23 de diciembre de 2019 y 20.212, de 6 de noviembre de 2023. Reglamentada por Decretos N° 154/004, de 3 de mayo de 2004, 295/017, de 16 de octubre de 2017, 404/023, de 12 de diciembre de 2023	Reconoce el derecho a los autores el dominio sobre las producciones de su pensamiento, ciencia y arte. Se incluyen dentro de la protección de la ley los programas de computadora o software y compilaciones de datos que por su contenido constituyan una creación intelectual. Se prevén derechos, un plazo de protección determinado, conductas lícitas e ilícitas y eventualmente sanciones. Las obras se registran en la Biblioteca Nacional, con la excepción de los programas de ordenador, compilaciones de datos u otros materiales que se constituyan en creaciones intelectuales, expresión de ideas, informaciones y algoritmos formuladas en secuencias originales ordenadas para ser usadas por un dispositivo de procesamiento de información o de control automático y las transmisiones de los derechos patrimoniales sobre estas obras, que se inscribirán en el Registro de Software de la DNPI.
Ley N° 14.910, de 19 de julio de 1979	Por la citada Ley se aprueban los convenios para la protección de la propiedad industrial, para la protección de las obras literarias y artísticas y para la propiedad intelectual (Convenios de París y Berna).



Ley N° 16.671, de 13 de diciembre de 1994	Se aprueban los acuerdos firmados resultantes de la Ronda Uruguay de Negociaciones Comerciales Multilaterales, contenidos en el Acta Final suscrita en Marrakech el 15 de abril de 1994, y en particular el Acuerdo sobre los aspectos de los derechos de propiedad intelectual relacionados con el comercio (ADPIC).
Ley N° 17.011, de 25 de setiembre de 1998. Reglamentada por decreto N° 34/999, de 3 de febrero de 1999.	Se regula la protección conferida a las marcas, definidas como signo con aptitud para distinguir productos o servicios de una persona física o jurídica de los de otra. Se establecen tipos de marcas, derechos, plazos de protección, registro, nulidades absolutas y relativas con respecto a determinados signos. Regula además los nombres comerciales, las indicaciones geográficas, las denominaciones de origen y las indicaciones de procedencia.
Ley N° 17.164, de 2 de setiembre de 1999. Reglamentada por decreto N° 11/000, de 13 de enero de 2000.	Se regulan los derechos y obligaciones respecto de patentes de invención, modelos de utilidad y diseños industriales. Se establecen, al igual que en el caso anterior, derechos, nulidades, plazos de protección, registro y eventuales sanciones.
Ley N° 18.036, de 20 de octubre de 2006.	Se aprueba el Tratado de la Organización Mundial de la Propiedad Intelectual (OMPI) sobre Derecho de Autor y Declaraciones Concertadas relativas al Tratado de la OMPI sobre Derecho de Autor.
Ley 18.253, de 20 de febrero de 2008	Aprobación del Tratado de la Organización Mundial de la Propiedad Intelectual sobre interpretación o ejecución y fonogramas, y declaraciones concertadas relativas al mismo.



<p>Ley N° 19.179, de 27 de diciembre de 2013. Reglamentado por decreto N° 44/015, de 30 de enero de 2015.</p>	<p>Regula el formato para el procesamiento y almacenamiento de información digital en determinadas entidades públicas y privadas.</p>
---	---

Infraestructura y Ciberseguridad

Normas aplicables	Resumen de contenido
<p>Ley N° 17.296, de 21 de febrero de 2001 artículos 70 a 94 bis, en la redacción dada por los artículos 143 y 418 de la Ley N° 18.719, de 27 de diciembre de 2010 y 256 a 273 de la Ley N° 19.889, de 9 de julio de 2020, entre otros. Reglamentado por decreto N° 212/001, de 4 de mayo de 2001.</p>	<p>Se establecen las competencias de la Unidad Reguladora de Servicios de Comunicaciones (URSEC) -actualmente servicio descentralizado-, del Ministerio de Industria, Energía y Minería (MIEM) y en particular de la Dirección Nacional de Telecomunicaciones y Servicios de Comunicación Audiovisual (DINATEL) en materia de telecomunicaciones. En lo que refiere a URSEC se estableció como principales cometidos regulación y el control las actividades y sectores referidos a las telecomunicaciones y postales. La definición de políticas corresponde a MIEM.</p>
<p>Ley N° 18.331, de 11 de agosto de 2008. Reglamentada por decretos N°</p>	<p>Se establece el marco general para la comunicación de datos personales entre entidades de los ámbitos público y privado, así como los requisitos básicos que deben cumplirse para dar seguridad a los tratamientos de datos personales. El decreto N° 64/020, de 17 de febrero de</p>

<p>414/009, de 31 de agosto de 2009 y 64/020, de 17 de febrero de 2020.</p>	<p>2020, en particular recomienda la adopción de determinadas medidas de seguridad en sus artículos 3° y 4°, sugiriendo expresamente la adopción del Marco de Ciberseguridad de Agesic.</p>
<p>Ley N° 18.719, de 27 de diciembre de 2010, artículo 149, en la redacción dada por el artículo 84 de la Ley N° 19.924, de 18 de diciembre de 2020.</p>	<p>Se encomienda a Agesic a dirigir las políticas, metodologías y mejores prácticas, y regular en materia de seguridad de la información y ciberseguridad a nivel nacional, así como fiscalizar, auditar su cumplimiento y brindar apoyo en las etapas de implementación de las mismas en todas las entidades públicas, y además, en las entidades privadas vinculadas a servicios o sectores críticos del país.</p>
<p>Ley N° 18.719, de 27 de diciembre de 2010, artículos 157 a 160. Reglamentados por decreto N° 178/013, de 11 de junio de 2013.</p>	<p>Se establecen reglas para la interoperabilidad entre organismos públicos. Se fija el rol de Agesic en la materia y sus competencias. La reglamentación determina la creación de una plataforma de interoperabilidad gestionada por esta agencia para el intercambio de información entre entidades públicas.</p>
<p>Decreto 92/014, de 7 de abril de 2014</p>	<p>Para el ámbito de la Administración Central, se establece la obligación de que los centros de datos seguros se sitúen en territorio nacional, exceptuando los que no constituyen un riesgo para el organismo. Asimismo, por Anexo, se establecen las condiciones físicas de seguridad que deben ponerse en práctica por las entidades públicas. Se prevé además la posibilidad de contemplar excepciones, siendo el otorgamiento de éstas, competencia de Agesic.</p>
<p>Ley N° 19.924, de 18 de diciembre de 2020, artículos 372 a 375 que</p>	<p>Se suprime la Secretaría Nacional de Ciencia y Tecnología y se modifica en el marco del Ministerio de Educación y Cultura la denominación y competencias de la Dirección para el Desarrollo de la Ciencia y el Conocimiento, que</p>



<p>suprimen la entidad creada por Ley N° 19.355, de 19 de diciembre de 2015, artículo 34, cuyas competencias se encontraban reglamentadas por el decreto N° 324/017, de 10 de noviembre de 2017.</p>	<p>pasa a llamarse Dirección Nacional de Innovación, Ciencia y Tecnología. La reglamentación de la Secretaría antedicha había establecido dentro de sus competencias, las de proponer proyectos de políticas de ciencia, tecnología e innovación, promover el mayor desarrollo de las capacidades de conectividad y telecomunicaciones y proponer infraestructuras en el campo de la ciencia, la tecnología y la innovación, en áreas estratégicas para el desarrollo del país.</p>
<p>Ley N° 20.075, de 20 de octubre de 2022 artículo 461, reglamentado por decreto N° 216/023, de 17 de julio de 2023</p>	<p>El artículo dispone una asignación presupuestal para el programa investigación, innovación y desarrollo experimental para promover proyectos en ciencia, tecnología e innovación, reglamentándose por el decreto citado la creación del Programa <i>Uruguay Innovation Hub</i>, dentro de la Agencia Nacional de Investigación e Innovación (ANII). Dentro de sus instrumentos se encuentran a modo de ejemplo la instalación de laboratorios abiertos, mediante apoyos financieros y operativos.</p>
<p>Ley N° 20.212, de 6 de noviembre de 2023, artículos 78 a 84.</p>	<p>Sin perjuicio de que existen múltiples normas que regulan aspectos de ciberseguridad, tanto a nivel legal como reglamentario, se destaca el impulso que brindan estos artículos a la materia, imponiendo determinadas obligaciones de rango legal a cargo de entidades públicas y de entidades privadas vinculadas a sectores o servicios críticos del país, así como instrumentos para el contralor y fiscalización de su cumplimiento a cargo de Agesic. Por otra parte, se establece la integración de dos entidades</p>



	asesoras de Agesic en materia de ciberseguridad y la definición de las bases para una Estrategia Nacional.
--	--

Trabajo y capacitación para la IA

Normas aplicables	Resumen de contenido
Ley N° 18.046, de 24 de octubre de 2008. Reglamentada por decreto N° 52/021, de 8 de febrero de 2021.	Ley de creación del Instituto Nacional de Empleo y Formación Profesional (INEFOP). Incluye entre sus cometidos el asesoramiento en la definición de políticas de capacitación y formación para generar y mejorar el empleo.
Ley N° 18.437, de 12 de diciembre de 2008. Reglamentada por decretos N° 334/009, de 20 de julio de 2009 y 294/013, de 11 de setiembre de 2013.	Se declara de interés general la promoción del goce y el efectivo ejercicio del derecho a la educación como derecho humano fundamental.
Ley N° 19.121, de 20 de agosto de 2013.	Se regula el Estatuto del Funcionario Público de la Administración Central, promoviendo la capacitación de los funcionarios públicos, lo que se considera fundamental para el acceso y el ascenso de cargo.
Decreto N° 340/018, de 22 de octubre de 2018.S	Se crea la Comisión Nacional de Certificación Ocupacional en la órbita de INEFOP.
Ley N° 19.973, de 13 de agosto de 2021.	Se establecen políticas de empleo para favorecer la actividad laboral remunerada de jóvenes, mayores de edad



Reglamentada por decreto N° 308/021, de 10 de setiembre de 2021.	y personas con discapacidad, incluyendo su capacitación y formación.
--	--

Responsabilidad civil y derechos del consumidor

Normas aplicables	Resumen de contenido
Código Civil	Las normas en materia de responsabilidad se encuentran en los artículos 1246 y siguientes del Código Civil, previéndose la responsabilidad contractual y extracontractual en la forma mencionada, previendo salvo excepciones un régimen de responsabilidad subjetiva para todos los tipos. En particular, cabe considerar en este tema el artículo 1330.
Ley N° 17.250, de 11 de agosto de 2000. Reglamentada por decreto N° 244/000, de 23 de agosto de 2000.	En el caso específico de las relaciones de consumo, se prevé también un régimen de responsabilidad subjetiva. Establece algunas especificidades vinculadas a la responsabilidad en los artículos 34 a 36.

Medidas de promoción

Normas	Resumen de contenido
Ley N° 16.906, de 7 de enero de 1998. Reglamentada por decreto N° 92/998, de 21 de abril de 1998.	Ley de inversiones y promoción industrial.



<p>Artículo 461 de la Ley N° 20.075, de 20 de octubre de 2022</p>	<p>Se asigna una partida anual de \$ 400.000.000 (cuatrocientos millones de pesos uruguayos), con cargo a Rentas Generales, con el objetivo de promover proyectos en materia de ciencia, tecnología e innovación, que sean aprobados por el Ministerio de Economía y Finanzas, con el asesoramiento de la Oficina de Planeamiento y Presupuesto, a propuesta de la Agencia Nacional de Investigación e Innovación.</p>
<p>Decreto N° 216/023, de 17 de julio de 2023</p>	<p>Se crea el Programa Uruguay Innovation Hub para promover el ecosistema emprendedor e innovador.</p>
<p>Ley N° 20.121, de 23 de agosto de 2023. Reglamentada por decreto N° 360/023, de 14 de noviembre de 2023.</p>	<p>Ley vinculada al fomento para la radicación en Uruguay, de técnicos y profesionales del sector de las tecnologías de la información</p>
<p>Artículo 75 Ley N° 20.212, de 6 de noviembre de 2023</p>	<p>Se promueve la creación de entornos controlados de prueba para proyectos que tengan como objetivo, entre otros, la construcción de sistemas que apliquen la IA.</p>



Anexo 2: Definiciones

Sistemas de Inteligencia Artificial

La Estrategia de Inteligencia Artificial para el Gobierno Digital conceptualizó la inteligencia artificial como *“un campo de estudio y un conjunto de tecnologías que estudian y desarrollan sistemas capaces de realizar tareas que normalmente se atribuyen a la inteligencia humana”*⁶⁰.

Atendiendo a la necesidad de contar con una definición técnica que refleje lo que los sistemas de IA son actualmente, pero al mismo tiempo, garantizar que ésta sea flexible frente a los constantes avances de la tecnología, el 8 de noviembre de 2023 la Organización para la Cooperación y el Desarrollo Económicos (OCDE), actualizó la definición de sistemas de inteligencia artificial incluida en la Recomendación de la OCDE sobre IA adoptada en 2019. La definición revisada y consensuada en este ámbito ha constituido la base técnica para distintos procesos a nivel internacional y regional.

A efectos de éste documento se adoptará la definición revisada de la OCDE, que es la siguiente: *“Un sistema de IA es un sistema basado en máquinas que, por objetivos explícitos o implícitos, infiere, a partir de la entrada que recibe, cómo generar salidas tales como predicciones, contenidos, recomendaciones o decisiones que pueden influir en entornos físicos o virtuales. Los distintos sistemas de IA varían en sus niveles de autonomía y capacidad de adaptación tras su despliegue”*⁶¹ (Traducción no oficial⁶²).

Tal y como ha sido analizado recientemente por el Comité de Inteligencia Artificial (CAI) del Consejo de Europa, esta definición actualizada, busca identificar las

⁶⁰ AGESIC. Estrategia de Inteligencia Artificial para el Gobierno Digital. 2020. Disponible en: <https://www.gub.uy/agencia-gobierno-electronico-sociedad-informacion-conocimiento/comunicacion/publicaciones/estrategia-inteligencia-artificial-para-gobierno-digital/estrategia-2>. Últ. Acceso: 16/4/2024.

⁶¹ OCDE, Recomendación de la OCDE sobre IA, OECD/LEGAL/0449, 2019, enmendada en 2023. Disponible en: <https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0449>. Últ. Acceso: 16/4/2024.

⁶² Texto original en inglés: *“An AI system is a machine-based system that, for explicit or implicit objectives, infers, from the input it receives, how to generate outputs such as predictions, content, recommendations, or decisions that can influence physical or virtual environments. Different AI systems vary in their levels of autonomy and adaptiveness after deployment”*.



características principales que permiten distinguir los sistemas de inteligencia artificial de otros sistemas de software más simples que posibilitan ejecutar operaciones automáticamente a partir de reglas pautadas por personas físicas⁶³. La misma ha constituido la base para las definiciones de sistemas de IA establecida por el Reglamento de Inteligencia Artificial de la Unión Europea⁶⁴, y el Draft del Convenio Marco sobre Inteligencia Artificial, Derechos Humanos, Democracia y Estado de Derecho⁶⁵ adoptado en el marco del CAI, en el cual Uruguay participa como observador⁶⁶.

Ciclo de vida de los sistemas de IA

La Recomendación de la OCDE 2019 indica que las fases del ciclo de vida del sistema de IA implican: *i) “diseño, datos y modelos”; que es una secuencia dependiente del contexto, que abarca la planificación y el diseño, la recopilación y el procesamiento de datos, así como la construcción de modelos; ii) “verificación y validación”; iii) “despliegue”; y iv) “operación y seguimiento”. Estas fases suelen tener lugar de forma iterativa y no necesariamente secuenciales. La decisión de retirar de funcionamiento*

⁶³ COE (2024). Draft Explanatory Report, Draft Framework Convention on artificial intelligence, human rights, democracy and the rule of law. CM(2024)52-addprov), Párr. 24. Disponible para descarga en: <https://www.coe.int/en/web/artificial-intelligence/cai>. Últ. Acceso: 16/4/2024.

⁶⁴ El artículo 3 del Reglamento de Inteligencia Artificial de la Unión Europea establece la siguiente definición: “«sistema de IA»: un sistema basado en una máquina diseñado para funcionar con distintos niveles de autonomía, que puede mostrar capacidad de adaptación tras el despliegue y que, para objetivos explícitos o implícitos, infiere de la información de entrada que recibe la manera de generar información de salida, como predicciones, contenidos, recomendaciones o decisiones, que puede influir en entornos físicos o virtuales”. Disponible en: https://www.europarl.europa.eu/doceo/document/TA-9-2024-0138_ES.pdf . Últ. Acceso: 16/4/2024.

⁶⁵ El artículo 2 del Convenio Marco sobre Inteligencia Artificial, Derechos Humanos, Democracia y Estado de Derecho, brinda la siguiente definición: “For the purposes of this Convention, “artificial intelligence system” is a machine-based system that for explicit or implicit objectives, infers, from the input it receives, how to generate outputs such as predictions, content, recommendations, or decisions that may influence physical or virtual environments. Different artificial intelligence systems vary in their levels of autonomy and adaptiveness after deployment”. Disponible en: <https://rm.coe.int/-1493-10-1b-committee-on-artificial-intelligence-cai-b-draft-framework/1680aee411> . Últ. Acceso: 16/4/2024.

⁶⁶ Se espera que el Convenio sea adoptado formalmente por el Comité de Ministros del Consejo de Europa el 17 de mayo de 2024.



*un sistema de IA puede ocurrir en cualquier momento durante la fase de operación y monitoreo (traducción no oficial)*⁶⁷.

IA Generativa

La inteligencia artificial generativa es un subconjunto del Deep Learning. La IA generativa aprende patrones en un contenido para poder generar contenido nuevo. La salida (output) de la IA se basará en los datos masivos con los que el modelo fue entrenado. El nuevo contenido puede presentarse en distinto formato, textos escritos en lenguaje natural, imágenes, audio, y código de software.

En palabras de UNESCO, *“la IA Generativa es una tecnología de inteligencia artificial que genera contenidos de forma automática en respuesta a instrucciones escritas en interfaces conversacionales de lenguaje natural (prompts)”*⁶⁸.

Las técnicas utilizadas en la IA generativa varían. Así, por ejemplo, explica la UNESCO, la IA generativa de textos, *“utiliza un tipo de red neuronal artificial conocido como transformador de propósito general, y un tipo de transformador de propósito general llamado modelo de lenguaje de gran tamaño. Por eso, los sistemas de inteligencia artificial generativa de texto suelen denominarse modelos de lenguaje de gran tamaño, (o LLM). El tipo de lenguaje de gran tamaño utilizado por la inteligencia artificial generativa se conoce como transformador generativo preentrenado o GPT, por sus siglas en inglés”* (UNESCO, 2023).

En un sentido similar, la Orden Ejecutiva de octubre de 2023 de Estados Unidos Sobre el desarrollo y el uso de la inteligencia artificial de forma segura y fiable, establece por IA generativa *“se entiende la clase de modelos de IA que emulan la estructura y las características de los datos de entrada para generar contenidos*

⁶⁷ *AI system lifecycle*: AI system lifecycle phases involve: *i)* ‘design, data and models’; which is a context-dependent sequence encompassing planning and design, data collection and processing, as well as model building; *ii)* ‘verification and validation’; *iii)* ‘deployment’; and *iv)* ‘operation and monitoring’. These phases often take place in an iterative manner and are not necessarily sequential. The decision to retire an AI system from operation may occur at any point during the operation and monitoring phase.

⁶⁸ UNESCO (2023). Kit de herramientas global sobre IA y el estado de derecho para el poder judicial. CI/DIT/2023/AIRoL/01. Glosario. Disponible en: https://unesdoc.unesco.org/ark:/48223/pf0000387331_spa. Últ. Acceso:16/4/2024.



sintéticos derivados. Esto puede incluir imágenes, vídeos, audio, texto y otros contenidos digitales’ (traducción no oficial)⁶⁹.

⁶⁹ Ver artículo 3, literal p.