Informe artículo 74 Ley N° 20.212

Recomendaciones para una regulación de la Inteligencia Artificial (IA) orientada al desarrollo ético, la protección de los derechos humanos y el fomento de la innovación tecnológica

Autores: Áreas Secretaría Letrada y Sociedad de la Información

Versión 1
Año: 2024

Contenido

Presentación

La expansión acelerada de la Inteligencia Artificial (IA) y sus potenciales usos e impactos ha generado un profundo debate acerca de sus implicancias éticas, sociales, económicas, políticas, entre otras. El tema ha sido parte de las discusiones en las agendas de organismos internacionales y regionales, y de los gobiernos nacionales.

En el caso de nuestro país, en 2023 el Parlamento estableció los primeros lineamientos para una política de la IA, basada en estándares internacionales, y orientada al desarrollo ético, la protección de los derechos humanos y el fomento de la innovación.

El artículo 74 de la Ley N° 20.212, de 6 de noviembre de 2023, establece además un plazo para que esta Agencia eleve recomendaciones con esas orientaciones, lo que motivó un proceso de elaboración en el que se procuraron contemplar distintas perspectivas y opiniones de diversos sectores de la sociedad.

Este informe y las recomendaciones asociadas son el resultado de dicho proceso. Desde esta Agencia esperamos que permitan iniciar un debate público y una construcción colectiva en un tema que indudablemente tiene y tendrá impactos significativos y duraderos en nuestra sociedad.

Hebert Paguas

Director Ejecutivo

Antecedentes

Objetivos

La Ley N° 20.212, de 6 de noviembre de 2023, estableció en su artículo 74, dos grandes innovaciones en lo que refiere a la normatividad de la Inteligencia Artificial (IA) en nuestro país:

Con respecto **a la Estrategia Nacional de IA**, subrayó el liderazgo de la Agencia para el Desarrollo del Gobierno de Gestión Electrónica y la Sociedad de la Información y del Conocimiento (Agesic) en su desarrollo e implementación, impuso la actuación preceptiva de la Unidad Reguladora y de Control de Datos Personales (Urcdp) cuando se encontraran involucrados datos personales, vinculó la estrategia citada con la Estrategia Nacional de Datos, definió sus principios orientadores, atribuyó un rol fundamental a la participación de múltiples partes interesadas a través de la potencial creación de comités o grupos, y estableció un plazo de 180 días para la elaboración del presente informe.

Con respecto **al desarrollo e implementación de sistemas de IA**, definió el rol de Agesic para la elaboración de recomendaciones específicas a entidades del sector público y privado, incluyendo además recomendaciones para la fiscalización de su cumplimiento, todo sin perjuicio de las competencias propias de la Urcdp y de otras entidades públicas en sus respectivos ámbitos de actuación.

El presente informe se elaboró a partir de una metodología predefinida, y a través de un proceso en el que se contó con la participación de funcionarios y consultores de diversos organismos públicos, con quienes luego de distintas reuniones se definió un documento de consulta que fue puesto a disposición de otros actores (organismos y entidades privadas, academia y sociedad civil) previamente identificados, empleando a esos efectos la plataforma de participación ciudadana gestionada por Agesic.

Estructura del informe

El informe se estructura en tres capítulos y tres anexos. El primer capítulo describe los antecedentes del informe, sus objetivos, presupuestos, los antecedentes internacionales considerados, las definiciones base y las entidades que realizaron aportes en la primera fase del proceso.

El capítulo segundo desarrolla las líneas temáticas consideradas por esta Agencia, indicando en cada una de ellas algunas consideraciones preliminares, una selección de antecedentes internacionales específicos y un diagnóstico preliminar, en el que se incluyeron opiniones no sólo de la Agencia sino también de los aportes de otras entidades. Se incluyeron además en este capítulo otras líneas temáticas que surgieron del proceso de elaboración.

Finalmente, en el capítulo tercero se presentan las recomendaciones elaboradas por esta Agencia, divididas en recomendaciones generales y en recomendaciones específicas, vinculadas a tres aspectos centrales: institucionalidad y gobernanza de la IA, ética, derechos humanos y democracia, e innovación responsable.

Se agregaron además al informe tres anexos, el primero con un breve mapeo de normativa más relevante que resulta aplicable a las líneas temáticas consideradas, el segundo con un detalle de normativa internacional en distintos ámbitos, y un tercero con los aportes recibidos de las instituciones que colaboraron en el proceso de consulta realizado a través de la plataforma de participación ciudadana.

Orientaciones para la generación del presente informe

El artículo 74 indicado establece que las recomendaciones generadas deben estar orientadas a:

- El **desarrollo ético** de la IA.
- La **protección de los derechos humanos**.
- El **fomento de la innovación tecnológica**.

En los capítulos siguientes se especificará cómo se ha procurado plasmar las orientaciones mencionadas en los análisis y en las recomendaciones formuladas.

El desarrollo ético de la IA, la protección de los derechos humanos y el sistema democrático

El desarrollo ético de la IA

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.”.

Hoy en día existen otras definiciones, que recogen aspectos que en el momento del diseño de dicha Estrategia no se encontraban contemplados. En los hechos, el informe plantea la importancia de considerar definiciones reconocidas y actualizadas por la Organización para la Cooperación y el Desarrollo Económicos (OCDE). Así, es posible adelantar que esta Agencia entiende por sistema de IA al: “sistema basado en una máquina que, para objetivos explícitos o implícitos, infiere, a partir de la entrada que recibe, cómo generar resultados como predicciones,

[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.

contenidos, recomendaciones o decisiones que pueden influir en entornos físicos o virtuales. Los diferentes sistemas de IA varían en sus niveles de autonomía y adaptabilidad después del despliegue". Más adelante se volverá a considerar esta definición.

Afirma SOLOVE[2] al analizar los vínculos entre la privacidad y la IA, que esta última se trata de una "vieja" tecnología, no diferente a las que comenzaron a generar preocupaciones en materia de privacidad en la segunda mitad del siglo XX. Pero la diferencia es que, en nuestros días, existe una mayor cantidad de datos tratados, un mayor poder computacional y mejores mecanismos de análisis.

En el documento "The governance of artificial intelligence: interim report "[3] del Comité de Ciencia, Innovación y Tecnología de la Cámara de los Comunes del Parlamento inglés, se indica con claridad que la IA ha sido un campo de interés desde los años 1950. No obstante, fue recién con la expansión de los grandes modelos de lenguaje (Large Language Models o LLMs)[4] que la IA se convirtió en una tecnología de propósito general, y accesible a todos.

El Comité plantea 12 desafíos para los elaboradores de marcos y políticas en IA: los sesgos, la privacidad, la tergiversación, el acceso a los datos, el acceso a poder computacional, las "cajas negras", el código abierto, la propiedad intelectual y los derechos de autor, la responsabilidad, el empleo, la coordinación internacional, y finalmente el desafío existencial –este último asociado a la creencia de algunas personas de que la IA es una amenaza para la vida mundial-.

[2] SOLOVE, Daniel. "Artificial Intelligence and Privacy". 77 Florida Law Review, GWU Legal Studies Research Paper. Disponible en SSRN: https://ssrn.com/abstract=4713111 or http://dx.doi.org/10.2139/ssrn.4713111. Últ. Acceso: 20/06/2024.

[3] https://committees.parliament.uk/work/6986/governance-of-artificial-intelligence-ai/news/197236/ai-offers-significant-opportunities-but-twelve-governance-challenges-must-be-addressed-says-science-innovation-and-technology-committee/. Últ. Acceso: 20/05/2024.

[4] El reporte de este año emanado del Comité de Comunicaciones y Digitalización de la Cámara de los Lores, también del Parlamento Inglés, titulado "Large language models and generative AI", se definió a los grandes modelos de lenguaje como un subconjunto de modelos fundacionales –aquellos que usan técnicas de aprendizaje profundo y se entrenan con grandes bases de datos- enfocados en el texto escrito. El reporte se encuentra disponible en: https://publications.parliament.uk/pa/ld5804/ldselect/ldcomm/54/54.pdf. Últ. Acceso 20/05/2024.

El reporte citado se inicia con un sumario generado por IA, por lo que, con esa inspiración, luego de consideradas todas las líneas temáticas y finalizado el proceso de elaboración de este informe, se le consultó a ChatGPT -uno de los LLM más conocidos- que en menos de 150 palabras sugiriese qué recomendar para una regulación de la IA orientada al desarrollo ético, la protección de los derechos humanos y el fomento de la innovación.

Su respuesta fue: “Para una regulación de la IA que promueva el desarrollo ético y la protección de los derechos humanos, es esencial establecer marcos normativos claros y robustos. Estos deben incluir principios de transparencia, responsabilidad y rendición de cuentas, garantizando que las decisiones automatizadas sean comprensibles y justificables. Es fundamental que los sistemas de IA respeten la privacidad y la seguridad de los datos, implementando mecanismos para evitar sesgos y discriminación. Además, debe haber supervisión constante y mecanismos de auditoría para asegurar el cumplimiento de estas normativas, junto con sanciones adecuadas para las violaciones.

En cuanto al fomento de la innovación, las regulaciones deben ser flexibles y adaptables, permitiendo la experimentación y el desarrollo tecnológico sin imponer cargas excesivas. Es crucial incentivar la colaboración entre sectores públicos y privados, así como la inversión en investigación y desarrollo. Las políticas deben fomentar un ecosistema inclusivo, donde startups y pequeñas empresas tengan acceso a recursos y oportunidades para innovar. Además, la educación y capacitación en IA deben ser prioridades para preparar a la fuerza laboral del futuro y asegurar que el avance tecnológico beneficie a toda la sociedad”.

Claramente se puede coincidir con lo expresado pero la realidad muestra otras complejidades, sobretodo en el contexto latinoamericano.

Uno de los desafíos más importantes, dada la potencialidad de la IA para impactar en cómo viven las personas y se desenvuelven en sociedad, es generar un encare que contemple determinados principios insoslayables, que hoy en día se reflejan en instrumentos emanados de distintas entidades nacionales, regionales e internacionales.

En particular, distintos instrumentos internacionales se manifiestan en favor de un desarrollo ético de la IA, entendiendo como tal el cumplimiento de determinados principios y valores éticos asociados entre otros, al respeto de la persona humana, la prevención de riesgos y la protección de grupos vulnerables.

Señala CRAWFORD[5] desde una perspectiva crítica, que "(…) cuando la rápida expansión de la IA se ve como imparable, sólo es posible improvisar restricciones legales y técnicas a los sistemas después del hecho: limpiar conjuntos de datos, fortalecer leyes de privacidad o crear comités de ética. Pero estas siempre serán respuestas parciales e incompletas en las que se asume la tecnología y todo lo demás tiene que adaptarse a ella. Pero ¿Qué ocurre si revertimos esa polaridad y comenzamos con el compromiso de un mundo más justo y sustentable?¿Cómo podemos intervenir para abordar los problemas interdependientes de las injusticias sociales, económicas y climáticas?¿Dónde sirve la tecnología a esa visión?¿Existen lugares en los que no se deba usar la IA, donde se socava esa justicia?".

Las preguntas de la autora llevan a pensar en la búsqueda de la motivación subyacente para el uso de IA, y en políticas colectivas orientadas a la conservación de bienes comunes generadas a partir de la discusión con múltiples actores.

En lo que refiere al **desarrollo ético** de la IA como orientador del informe, esta Agencia ha considerado especialmente la Recomendación sobre la ética de la inteligencia artificial de la Organización de las Naciones Unidas para la Educación, la Ciencia y la Cultura (UNESCO) adoptada el 23 de noviembre de 2021, y a la que nuestro país adhirió el 8 de junio de 2023[6], contenedora de principios, pero también de herramientas prácticas de gran relevancia.

Dentro de su ámbito de aplicación, la recomendación detalla que el abordaje de la ética de la IA se realiza "como una reflexión normativa sistemática, basada en un marco integral, global, multicultural y evolutivo de valores, principios y acciones

[5] CRAWFORD, Kate. "Atlas de Inteligencia Artificial. Poder, política y costos planetarios". Fondo de Cultura Económica. Primera Edición. 2022. Pág. 342 y sigs.

[6] https://www.gub.uy/agencia-gobierno-electronico-sociedad-informacion-conocimiento/comunicacion/noticias/uruguay-adhiere-recomendacion-etica-inteligencia-artificial-unesco. Últ. Acceso: 25/06/2024.

interdependientes, que puede guiar a las sociedades a la hora de afrontar de manera responsable los efectos conocidos y desconocidos de las tecnologías de la IA en los seres humanos, las sociedades y el medio ambiente y los ecosistemas, y les ofrece una base para aceptar o rechazar las tecnologías de la IA."

El artículo 74 de la Ley N° 20.212 consagra un conjunto de principios alineados con los que resultan de la recomendación citada, y de otros instrumentos internacionales que se mencionarán, a saber: equidad, no discriminación, responsabilidad, rendición de cuentas, transparencia, auditoría e innovación segura, respeto a la dignidad humana, el sistema democrático y la forma republicana de gobierno, y los principios de la protección de datos consagrados 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).

En el entendido que la ética de la IA se relaciona con el cumplimiento de dichos principios, los que son habilitantes de un desarrollo seguro y responsable de los sistemas basados en esta tecnología, es opinión de esta Agencia que debemos detenernos en su aplicación efectiva, dando ejemplos concretos para ello.

La protección de derechos humanos y la democracia en el contexto del desarrollo de la IA

La segunda orientación que plantea el artículo 74 es la **protección de los derechos humanos**. Esta tecnología, o cualquier otra tecnología pasada o futura, no debería perforar un sistema jurídico que ha sido construido a través del reconocimiento de derechos inherentes a la persona humana y a la forma republicana de gobierno, consagrados en instrumentos nacionales e internacionales vigentes.

Desde esa perspectiva, y como se mencionará luego, esta Agencia entiende necesario partir de considerar el conjunto de obligaciones derivadas para los estados del derecho internacional de los derechos humanos: el deber de respetar, el deber de proteger y el deber de cumplir, adoptando todas las medidas que estén a su alcance para asegurar la realización de los derechos. En consonancia con este enfoque, se entiende pertinente destacar la necesidad no sólo de resguardar a las personas de eventuales efectos nocivos de la IA, sino también explotar su

potencialidad para promover efectos beneficiosos en la vida de éstas y en el desarrollo de nuestras sociedades.

En instrumentos regionales e internacionales existe consenso en colocar a la persona humana y a la defensa de sus derechos en el centro de cualquier desarrollo normativo. PEREZ COMENALE[7] señala que existe un énfasis en la protección de los derechos fundamentales, con el ser humano como centro de la regulación, y destaca la necesidad de preservar principios vinculados a la protección de datos personales, la protección de los sectores vulnerables, la inclusión digital, la conectividad, y la educación digital, todo en forma consistente con guías y recomendaciones internacionales.

En particular, esta Agencia quiere hacer especial énfasis en los impactos de la IA en el sistema democrático, siguiendo la opinión de INNERARITY[8], quien procura concretar las recomendaciones de la ética de UNESCO con este foco. En esa perspectiva, plantea cómo los sistemas automáticos de decisión afectan los principios normativos del autogobierno democrático, señalando expresamente que: "El problema es hasta qué punto y de qué modo el institucionalismo algorítmico caracterizado por la utilización de sistemas de decisión automatizada (ADS) es compatible con lo que consideramos un sistema político de toma de decisiones."

Dicho autor brinda distintas recomendaciones tales como la educación y concienciación, la regulación y legislación -donde asigna un rol preponderante a las comisiones parlamentarias de futuro para desarrollar un trabajo prospectivo-, la participación pública y protección de la democracia a través de instrumentos que mejoren la calidad de la conversación democrática, la regulación y legislación sobre datos, la transparencia, explicabilidad y contestabilidad, la inclusividad, las estrategias nacionales integrales, el enfoque multiactor y los desarrollos de marcos globales.

---

[7] PEREZ COMENALE, Agustina. "ChatGPT. Retos y oportunidades de la Inteligencia Artificial Generativa. Desafíos de su regulación". Libro digital, EPUB. Granero H., y ots. 2023. Pág. 105.

[8] INNERARITY, Daniel. "Inteligencia artificial y democracia". Año 2024. Disponible en: https://unesdoc.unesco.org/ark:/48223/pf0000389736_spa

La habilidad de las personas para participar libremente de la vida democrática también ha sido objeto de consideración al analizar el impacto de la IA en otros ámbitos como el de la neurotecnología. Es cierto que la sinergia entre IA y neurociencia ha permitido avances sustanciales que deben ser promovidos responsablemente, pero con ello también se han incrementado los riesgos de manipulación de las personas y su autonomía individual. Estas reflexiones son parte del Documento de Trabajo “Hacia un texto borrador de una recomendación en la ética de la neurotecnología” elaborado por el Grupo Ad Hoc de Expertos constituido en el marco de UNESCO[9][10].

Poner foco en la neurotecnología, la IA y el impacto en la forma en que las personas analizan y toman decisiones, nos permite visualizar que los usos potenciales dejarán rezagado cualquier intento regulatorio que no se sustente en instrumentos flexibles y adaptables.

El Parlamento Europeo[11] por su parte plantea la relevancia de la aplicación de herramientas de IA para mejorar el compromiso político y empoderar a las personas, otorgando a los operadores políticos la posibilidad de entender mejor las demandas de éstas a través de distintos sistemas, y dar respuestas personalizadas a esas demandas. También plantea riesgos, como la desinformación, deepfakes, y otros mecanismos que pueden afectar las campañas políticas e influir en la opinión pública.

El Parlamento Europeo propone así un conjunto de herramientas para contrarrestar los impactos negativos de la IA, entre los que destacan las herramientas de detección automática de contenido generado por IA, las marcas de agua,

[9] Documento en inglés disponible en: https://unesdoc.unesco.org/ark:/48223/pf0000389438. Últ. Acceso: 18/06/2024.

[10] Adicionalmente, corresponde indicar que UNESCO ha puesto a disposición una primera versión de la recomendación en la ética de la neurotecnología, la que se encuentra abierta a consulta pública, y está disponible en: https://unesdoc.unesco.org/ark:/48223/pf0000389768. Últ. Acceso: 19/06/2024.

[11] European Parliament. “Artificial intelligence, democracy and elections”. Disponible en: https://www.europarl.europa.eu/RegData/etudes/BRIE/2023/751478/EPRS_BRI(2023)751478_EN.pdf. Últ. Acceso: 15/6/2024.

instrumentos para chequear información en redes sociales, y en particular, normativa orientada a mitigar los riesgos de la IA.

El Convenio Marco de Inteligencia Artificial del Consejo de Europa (CoE)[12], afirma que deben adoptarse medidas para proteger a las personas en procesos democráticos, acceso a debate público y salvaguardarlas de influencias externas perjudiciales o maliciosas (artículo 5). En el punto 43 del reporte explicativo del Convenio se aclara que la IA tiene la potencialidad de generar nuevas formas de participación para los ciudadanos y de comunicación entre éstos y sus representantes, pero también la potencialidad de fragmentar la esfera pública y socavar la participación ciudadana y la confianza en la democracia.

Se comparte lo expresado en dicho reporte explicativo en cuanto a que la integridad de la democracia y sus procesos se basan en la capacidad de las personas de formar una opinión y actuar en consecuencia, así como de impactar en las decisiones que se adoptan por sus representantes. Por ello, algunas recomendaciones indicadas en el reporte resultan atendibles, como por ejemplo la adopción de medidas de ciberseguridad ante interferencias extranjeras maliciosas en procesos electorales, o ante la difusión de desinformación, todo ello cuidando de no afectar derechos fundamentales preexistentes como la libertad de expresión, de asociación y de reunión.

Se trata en consecuencia de tener la capacidad de reconocer y valorar los impactos de la IA en las personas, en sus derechos, y en nuestro sistema en general, promoviendo el desarrollo y aplicación de herramientas que faciliten la discusión democrática sin influencias indebidas en el comportamiento de las personas, y otras que **colaboren** con el espectro político para entender las necesidades éstas y de la sociedad, y en función de ello adoptar decisiones informadas y justas.

El fomento de la innovación tecnológica y la búsqueda de la soberanía en IA

Finalmente, el **fomento de la innovación tecnológica** se relaciona precisamente con los beneficios que esta tecnología puede tener para el desarrollo económico, pero

[12] https://www.coe.int/en/web/artificial-intelligence/the-framework-convention-on-artificial-intelligence. Últ. Acceso: 18/06/2024.

también social de nuestras poblaciones, en particular en el ámbito nacional y regional latinoamericano.

La innovación tecnológica surge en nuestro país como fundamento para la adopción de distintas estrategias y la promoción de diferentes beneficios incluidos en disposiciones legales y reglamentarias vigentes.

El decreto N° 216/023, de 17 de julio de 2023, que crea el programa Uruguay Innovation Hub (UIH) se refiere a la innovación como la "(…) actividad que, apoyada en conocimiento novedoso, es capaz de incorporar cambios significativos en los productos o procesos que redunden en un mayor valor económico."

En este punto la Agencia quiere poner el foco sobre algunos aspectos que entiende centrales para esta orientación: institucionalidad, objetivos estratégicos, instrumentos o herramientas, apoyo financiero e infraestructura.

En materia de institucionalidad, corresponde mencionar en primer lugar a la Agencia Nacional de Investigación e Innovación, creada por el artículo 256 de la Ley N° 17.930, de 19 de diciembre de 2005, que vio modificados distintos aspectos de su orgánica por la Ley N° 18.084, de 28 de diciembre de 2006, la que creó además el Consejo Nacional de Innovación, Ciencia y Tecnología (CONICyT), integrado por distintas entidades vinculadas a la ciencia, la tecnología y la innovación.

Más recientemente, el citado decreto N° 216/023, crea el programa Uruguay Innovation Hub (UIH), que cuenta dentro de sus múltiples objetivos el del fortalecimiento del ecosistema innovador.

Esta institucionalidad se complementa con otras múltiples entidades públicas focalizadas en el desarrollo de la innovación como la Universidad de la República, la Universidad Tecnológica del Uruguay, el Centro Ceibal, el Laboratorio Tecnológico del Uruguay, la Dirección Nacional de Innovación, Ciencia y Tecnología del Ministerio de Educación y Cultura, la Agencia Nacional de Desarrollo, la Agencia de Monitoreo y Evaluación de Políticas Públicas, la propia Agesic, entre otras, que de una forma u otra tienen entre sus cometidos la promoción de la innovación dentro y fuera del sector público.

Por su parte, cuando hablamos de objetivos estratégicos, nos referimos a la intención, manifestada preferentemente en forma de normas jurídicas, de promover determinadas áreas de la actividad.

A vía de ejemplo, el decreto N° 216/023, que crea el programa UIH, establece como prioritarias las tecnologías digitales avanzadas (Deep Tech), la biotecnología (Bio Tech) y las tecnologías verdes (Green Tech).

El programa indicado sirve además para canalizar los fondos previstos en el artículo 461 de la Ley N° 20.075, de 20 de octubre de 2022, con el objetivo de promover proyectos en materia de ciencia, tecnología e innovación. La provisión de fondos para este tipo de proyectos es esencial y debe ser parte de la discusión al hablar de promoción de la innovación en IA.

También en normas posteriores a la Ley N° 16.906, de 7 de enero de 1998, se incluyeron aspectos de innovación tecnológica para el otorgamiento de los beneficios que esta ley brinda, dentro del ámbito de la promoción de inversiones.

En lo que refiere a las herramientas para la innovación, merece destacarse la figura de los entornos controlados de prueba -sandboxes regulatorios-, a través del artículo 75 de la Ley N° 20.212, en vías de reglamentación, que se constituirá en un instrumento fundamental para el testeo y desarrollo de productos y servicios de forma controlada, antes de su puesta en producción.

Pero el fomento de la innovación viene de la mano además de una infraestructura adecuada, la que debería procurar que el país tenga la capacidad no sólo de producir tecnologías sino también de mantenerlas y evolucionarlas, generando a la interna, las capacidades técnicas y educativas necesarias.

Vinculado con ello, aunque con mayor amplitud, se ha desarrollado el concepto de **Soberanía de IA.** Esta ha sido descripta por BELLI[13] como "(…) la capacidad de un país determinado para entender, desarrollar y regular sistemas de IA (…) debería ser

[13] 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.

visto como esencial para retener el control, uso y autodeterminación sobre sistemas de IA"[14].

Dicho autor propone un marco de elementos interconectados (definido como KASE por las siglas en inglés "Key AI Sovereignty Enablers") que permitirá a un país determinar su soberanía en la materia, y que refieren 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 Mundial[15] por su parte, consideró la aplicación de 6 pilares para obtener esta soberanía: infraestructura digital, desarrollo de la fuerza laboral, investigación, desarrollo e innovación (I+D+i), marco regulatorio y ético, estímulo a la industria de IA, y cooperación internacional.

El argumento de la soberanía en IA debe considerarse en especial al momento de promover iniciativas regulatorias. A este respecto, la Declaración de Montevideo sobre Inteligencia Artificial y su impacto en América Latina[16], suscrita el 10 de marzo de 2023 en ocasión del evento Khipu, sostiene que es imprescindible fortalecer la soberanía de los países latinoamericanos con respecto a cuestiones estratégicas y regulatorias de IA, entendiendo como crucial la formación de personas al más alto nivel y el desarrollo del pensamiento crítico.

[14] 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-determination over AI systems".

[15] https://www.weforum.org/agenda/2024/04/sovereign-ai-what-is-ways-states-building/. Últ. Acceso: 30/04/2024.

[16] https://khipu.ai/. Últ. Acceso: 20/06/2024.

Presupuestos del presente informe

La pregunta que ineludiblemente se formula y que esta Agencia no pretende eludir es: ¿necesita nuestro país una ley de Inteligencia Artificial?

Es opinión de esta Agencia que la ley no es el único instrumento regulatorio aplicable, y que una eventual regulación legal, en su caso, debería centrarse no en la regulación de una tecnología en sí, sino en los potenciales y efectivos impactos positivos y negativos en las personas y la sociedad, sin limitar la innovación y el desarrollo tecnológico.

Debe reconocerse que Uruguay cuenta con una base normativa en varios de los aspectos implicados en el desarrollo ético de la tecnología, los derechos humanos y la promoción de la innovación. Es necesario continuar con la discusión, y apoyarnos en disposiciones y compromisos internacionales asumidos por nuestro país que dan un marco de protección y fomento a la innovación y al desarrollo de una IA responsable. Debemos pensar en una regulación complementaria en aspectos que impacten significativamente en la vida de las personas y en el desarrollo de nuestras sociedades. Por ello se tratará de brindar una propuesta de orientaciones sobre cómo y de qué forma llevar adelante esta discusión.

Señala DANESI[17] que “necesitamos una legislación en materia de inteligencia artificial, pero no cualquiera, pues sino corremos el riesgo de frenar la innovación y dejar a nuestros países fuera del progreso”, proponiendo para ello una serie de instancias de diálogo, análisis y diagnóstico con la participación de múltiples actores y con foco en los sistemas de IA de alto riesgo.

No se trata en opinión de la Agencia, en definitiva, de una dicotomía entre regular o no regular, sino de responder a la pregunta: ¿qué regular? Partiendo de esa base, las recomendaciones que se presentan en este informe se fundan en tres presupuestos:

1. **Lo que entendemos por “regulación tecnológica” no debe estar asociado a la regulación de una tecnología en sí misma sino a mitigar impactos**

[17] DANESI, Cecilia. “El Imperio de los Algoritmos”. Versión Kindle. Págs. 215-216.

negativos o promover impactos positivos en las personas y/o en la sociedad. Como corolario de esta concepción, corresponde afirmar que en lo que respecta al alcance del concepto “regulación”, éste comprende un abanico de instrumentos normativos en sentido amplio, no limitados a leyes o reglamentos, sino que alcanza a otros instrumentos “blandos”, tales como protocolos, guías, recomendaciones, códigos, etc.

2. **Una eventual regulación de los impactos negativos de la tecnología en general y de la IA en particular debe centrarse en la persona, y fundarse en la defensa de nuestra sociedad y nuestro sistema democrático.** Las limitaciones deberían ser fijadas legalmente en forma expresa, estrictamente necesarias y proporcionales para asegurar objetivos legítimos en una sociedad democrática.
3. **Una eventual regulación de los impactos positivos por su parte, deberá enfocarse al cumplimiento de aquellos objetivos que definamos como estratégicos a nivel país, de forma de ser más eficientes en la asignación de los limitados recursos con los que se dispone y a generar y promover las condiciones estructurales necesarias para dicho cumplimiento.** Las medidas que se adopten pueden tener distinto alcance, desde generales hasta sectoriales, y nuestro nivel de éxito dependerá de su adecuada determinación.

Instrumentos internacionales en IA y lecciones aprendidas

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 informe.

En particular, la Recomendación del Consejo de la OCDE en Inteligencia Artificial[18] 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 - a las

[18] https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0449. Últ. Acceso el 09/02/2024.

que se hará referencia en los capítulos siguientes-, así como un conjunto de principios aplicables a ésta[19].

Esta organización realizó además recomendaciones para el desarrollo de políticas a nivel nacional y cooperación internacional orientadas en especial a pequeñas y medianas empresas (PYMES), a saber:

1. invertir 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);

2. promover el ecosistema digital para IA (promoviendo en particular mecanismos como los fideicomisos de datos para compartir información de forma legal, ética y segura);

3. 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);

4. 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 emprendeurismo, entre otros);

5. 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).

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

Los principios de la OCDE han servido de base para otros desarrollos posteriores, como los once principios rectores para IA Avanzada ratificados por el G7 y conocidos como principios de Hiroshima[20], que a su vez dieron lugar a un código de conducta para desarrolladores.

Solo a modo de referencia[21], 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.

Como se mencionó, recientemente Uruguay adhirió[22] a la Recomendación sobre la Ética de la IA de UNESCO[23], 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. 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

[20] https://www.mofa.go.jp/files/100573466.pdf. Últ. Acceso el 12/02/2024.

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

[22] 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.

[23] https://www.unesco.org/es/artificial-intelligence/recommendation-ethics. Últ. Acceso el 09/02/2024.

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, 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 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 tecnologías[24].

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)[25].

Más recientemente, debe mencionarse por su relevancia la adopción de la Resolución A/RES/78/265 por parte de la Asamblea General de la ONU[26], en la que se insta a todos los estados parte y a otras organizaciones del sector privado, la sociedad civil, entre otros, a desarrollar y apoyar enfoques y marcos normativos y de gobernanza en pos de un uso seguro y fiable de la IA.

Existen otro conjunto de iniciativas que impactan en la forma en que internacionalmente se tratarán los sistemas de IA, y que se mencionarán con más detalle a lo largo del presente informe.

[24] https://www.unesco.org/es/articles/la-unesco-ayudara-mas-de-50-paises-elaborar-una-politica-etica-en-materia-de-ia-este-ano. Últ. Acceso el 09/02/2024.

[25] https://www.unesco.org/es/articles/unesco-apoya-proceso-de-revision-de-la-estrategia-de-etica-de-la-inteligencia-artificial-en-uruguay. Últ. Acceso el 09/02/2024.

[26] ONU – Asamblea General. Resolución aprobada por la Asamblea General el 21 de marzo de 2024. 78/265. “Aprovechar las oportunidades de sistemas seguros y fiables de inteligencia artificial para el desarrollo sostenible”. A/RES/78/265. Disponible en: https://documents.un.org/doc/undoc/gen/n24/087/86/pdf/n2408786.pdf?token=hxXvAKO8RS5xFkIlcb&fe=true. Últ. Acceso:29/4/2024.

Definiciones base para el informe

El objetivo aquí es definir qué se considera un sistema de inteligencia artificial a efectos del análisis y las recomendaciones que plantea el presente documento, así como plantear algunos conceptos fundamentales que contribuyen a comprender las características y funcionamiento de estos sistemas.

Los inicios del desarrollo de inteligencia artificial se remontan a mediados del siglo pasado, pero la forma vertiginosa en que se producen los avances tecnológicos en relación a cómo estos sistemas se construyen y funcionan, hace que la respuesta a la pregunta sobre qué es la inteligencia artificial sea un sostenido desafío.

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.

Como se indicó, a efectos de éste documento se adoptará la definición revisada de la OCDE, que es la siguiente: “sistema basado en una máquina que, para objetivos explícitos o implícitos, infiere, a partir de la entrada que recibe, cómo generar resultados como predicciones, contenidos, recomendaciones o decisiones que pueden influir en entornos físicos o virtuales. Los diferentes sistemas de IA varían en sus niveles de autonomía y adaptabilidad después del despliegue[27]” (Traducción no oficial[28]).

[27] 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.

[28] 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”.

Tal y como ha sido analizado recientemente por el Comité de Inteligencia Artificial (CAI) del Consejo de Europa, esta definición actualizada, busca identificar las 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 físicas[29]. La misma ha constituido la base para las definiciones de sistemas de IA establecida por el Reglamento de Inteligencia Artificial de la Unión Europea[30], y el Draft del Convenio Marco sobre Inteligencia Artificial, Derechos Humanos, Democracia y Estado de Derecho[31] adoptado en el marco del CAI, en el cual Uruguay participa como observador.

Evolución de la definición

La Recomendación de la OCDE sobre IA adoptada en 2019[32] definía los sistemas de inteligencia artificial "como un sistema basado en máquinas que puede, para un conjunto dado de objetivos definidos por el ser humano, realizar predicciones, recomendaciones o decisiones que afectan entornos reales o virtuales. Los

[29] 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.

[30] 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.

[31] 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.

[32] OCDE, C/MIN(2019)3/FINAL disponible en https://one.oecd.org/document/C/MIN(2019)3/FINAL/en/pdf . Últ. Acceso: 26/4/2024.

sistemas de IA están diseñados para operar con diferentes niveles de autonomía" (traducción no oficial[33]).

Conforme el organismo, las modificaciones introducidas en 2023 a efectos de reflejar las características y funcionamiento actuales de los sistemas de inteligencia artificial apuntan a[34]:

- Clarificar los objetivos de un sistema de IA, que pueden ser explícitos o implícitos.
- Reflejar que la entrada que recibe el sistema puede ser proporcionada por seres humanos o máquinas.
- Especificar que la Recomendación se aplica a sistemas de IA generativa.
- Sustituir el término "real" por "físico" para referir a los entornos.
- Reflejar el hecho de que algunos sistemas de IA pueden continuar evolucionando después de su diseño e implementación.

Al respecto, el memorándum explicativo indica que[35]:

- Si bien en la fijación y el desarrollo de objetivos de un sistema de IA siempre es posible remontarse a un ser humano que origina el proceso de desarrollo del sistema de IA, algunos tipos de sistemas pueden desarrollar subobjetivos implícitos, y en ocasiones, establecer objetivos para otros sistemas.
- Si bien la supervisión humana puede producirse en cualquier fase del ciclo de vida del sistema de IA, algunos sistemas de IA pueden generar resultados

[33] Texto original en inglés: "AI system: An AI system is a machine-based system that can, for a given set of human-defined objectives, make predictions, recommendations, or decisions influencing real or virtual environments. AI systems are designed to operate with varying levels of autonomy"

[34] Ver Información de antecedentes (Background information) en: https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0449#backgroundInformation . Últ. Acceso:16/4/2024.

[35] OCDE (2024), "Memorando explicativo sobre la definición actualizada de un sistema de IA de la OCDE", OECD Artificial Intelligence Papers , n.º 8, OECD Publishing, París. Disponible en: https://doi.org/10.1787/623da898-en . Últ. Acceso:16/4/2024.

sin que éstos se describan explícitamente en el objetivo del sistema de IA y sin instrucciones específicas de los seres humanos.

- Algunos sistemas pueden desarrollar la capacidad de realizar nuevas formas de inferencia no previstas inicialmente al ser programados, esto es, de modificar su comportamiento a través de la interacción directa con entradas y datos, antes o después de su despliegue.

- La referencia a “inferir” debe entenderse como “generar salidas” a partir de entradas. En tanto el concepto de salida(s) refiere a los resultados generados por un sistema de IA que varían en función de las distintas capacidades y funcionalidades que desempeñan.

En definitiva, las definiciones tomadas de la OCDE que se considerarán son:

Sistema de IA: un sistema de IA es un sistema basado en una máquina que, para objetivos explícitos o implícitos, infiere, a partir de la entrada que recibe, cómo generar resultados como predicciones, contenidos, recomendaciones o decisiones que pueden influir en entornos físicos o virtuales. Los diferentes sistemas de IA varían en sus niveles de autonomía y adaptabilidad después del despliegue.

Ciclo de vida del sistema de IA: 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 un sistema de IA puede ocurrir en cualquier momento durante la fase de operación y monitoreo.

Conocimiento de IA: El conocimiento de IA se refiere a las habilidades y recursos, como datos, códigos, algoritmos, modelos, investigaciones, conocimientos técnicos, programas de capacitación, gobernanza, procesos y mejores prácticas, necesarios para comprender y participar en el ciclo de vida del sistema de IA.

Actores de IA: Los actores de IA son aquellos que desempeñan un papel activo en el ciclo de vida del sistema de IA, incluidas las organizaciones e individuos que implementan u operan IA.

A continuación, se abordan otros conceptos fundamentales que contribuyen a comprender las características y funcionamiento de los sistemas de IA.

Machine learning

El aprendizaje automático o Machine learning (ML) es un campo de la Inteligencia Artificial.

En palabras de la Organización de las Naciones Unidas para la Educación, la Ciencia y la Cultura (UNESCO) “es un conjunto de técnicas que permite a las máquinas aprender automáticamente utilizando patrones y deducciones en lugar de instrucciones directas de una persona. Las técnicas de ML con frecuencia instruyen a las máquinas para que alcancen un resultado al proporcionar numerosas instancias de resultados correctos. Sin embargo, también pueden especificar un conjunto de pautas y dejar que la máquina las descubra por sí misma en los datos”[36].

El modelo se entrena a partir de datos de entrada que pueden ser etiquetados (aprendizaje automático supervisado) o no etiquetados (aprendizaje automático no supervisado). Un tercer tipo es el denominado aprendizaje por refuerzo, que implica una mejora continua del modelo basado en la retroalimentación[37].

La eficacia de los modelos de aprendizaje automático, depende, entre otros factores, del volumen y calidad de los datos de entrenamiento.

[36] 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.

[37] UNESCO (2021). Inteligencia artificial y educación. Guía para las personas a cargo de formular políticas, P.9. Disponible en: https://unesdoc.unesco.org/ark:/48223/pf0000379376 . Últ. Acceso:16/4/2024.

Redes neuronales artificiales

Una red neuronal artificial (RNA) se inspira en la estructura de las redes neuronales del cerebro humano.

Siguiendo la descripción de la UNESCO, las redes neuronales artificiales "son un tipo de técnica de aprendizaje automático que permite a los computadores aprender a realizar tareas mediante el análisis de ejemplos de entrenamiento"[38]. Una RNA está diseñada con nodos de procesamiento interconectados, que suelen estar organizados en capas. Cada nodo recibe datos de los nodos de la capa inferior y envía datos a los nodos de la capa superior[39].

Deep Learning

El aprendizaje profundo (Deep Learning) ha sido definido por UNESCO como una técnica de vanguardia del aprendizaje automático que "permite que la máquina reconozca por sí misma conceptos complejos tales como rostros, cuerpos humanos o imágenes de gatos, espulgando millones de imágenes extraídas de Internet, sin que esas imágenes sean previamente etiquetadas por los humanos. Nacido de la combinación de los algoritmos de aprendizaje automático con las redes neuronales formales y con el uso de los macrodatos, el Deep learning revolucionó la inteligencia artificial"[40].

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

[38] 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.

[39] 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.

[40] UNESCO. Léxico de la Inteligencia Artificial. Disponible en: https://www.unesco.org/es/articles/lexico-de-la-inteligencia-artificial-0. Últ. Acceso:16/4/2024.

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)”[41].

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 sintéticos derivados. Esto puede incluir imágenes, vídeos, audio, texto y otros contenidos digitales” (traducción no oficial)[42].

Modelos fundacionales o de uso general

Son modelos con amplias capacidades que se adaptan a distintos escenarios.

En el Reglamento de IA de la Unión Europea se definen como un modelo de IA entrenado con un gran volumen de datos utilizando la autosupervisión a gran

[41] 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.

[42] Ver artículo 3, literal p. 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: 22/06/2024.

escala, que presenta un grado considerable de generalidad y es capaz de realizar de manera competente una gran variedad de tareas distintas; puede integrarse en diversos sistemas o aplicaciones posteriores[43].

Entidades que realizaron aportes para la elaboración del informe

Agesic contó para la elaboración del presente informe con los aportes de representantes de distintas unidades ejecutoras y entidades que participaron en los grupos de trabajo asociados a las líneas temáticas que se mencionarán a continuación, incluyendo: Presidencia de la República (Prosecretaría de la Presidencia y Secretaría de Derechos Humanos), Ministerio de Educación y Cultura (Consejo de Derechos de Autor), Ministerio de Economía y Finanzas (Unidad Defensa del Consumidor), Ministerio de Industria, Energía y Minería (Dirección Nacional de Telecomunicaciones y Dirección Nacional de la Propiedad Industrial), Ministerio de Trabajo y Seguridad Social (Inspección General del Trabajo y la Seguridad Social), Unidad Reguladora de Servicios de Comunicaciones, Agencia Nacional de Investigación e Innovación, Programa Uruguay Innovation Hub, Unidad Reguladora y de Control de Datos Personales, e Institución Nacional de Derechos Humanos y Defensoría del Pueblo.

Asimismo, se recibieron aportes en el proceso de consulta realizado, por parte de la Asociación de Escribanos del Uruguay (AEU), el Laboratorio de Datos y Sociedad (DATYSOC), DATA Uruguay, la Cámara Uruguaya de Tecnologías de la Información (CUTI) y la Institución Nacional de Derechos Humanos y Defensoría del Pueblo (INDDHH).

Aun cuando no se recogieron todas las recomendaciones de quienes respondieron a la consulta, se estimó necesario agregar la documentación remitida para ilustrar sobre las distintas perspectivas planteadas, la que obra en Anexo a este informe.

[43] Ver artículo 3. Numeral 63. Disponible en: Disponible en: https://www.europarl.europa.eu/doceo/document/TA-9-2024-0138_ES.pdf. Últ. Acceso: 22/06/2024.

Líneas temáticas consideradas

Aspectos generales

En la elaboración del informe, y considerando los avances y los insumos obtenidos de los procesos de revisión y creación de las Estrategias Nacionales de Datos y de IA respectivamente, se definieron las siguientes líneas temáticas:

- Institucionalidad y gobernanza
- Derechos Humanos
- Trabajo y capacitación
- Propiedad Intelectual
- Responsabilidad civil y relaciones de consumo
- Infraestructura y ciberseguridad
- Medidas de promoción

En las siguientes páginas se reproduce el alcance de las citadas líneas.

Línea Institucionalidad y gobernanza

Consideraciones preliminares

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

Institucionalidad de IA e institucionalidad de datos, al igual que gobernanza de IA y gobernanza de datos se encuentran ineludiblemente ligadas, derivado de la relación de dependencia que la primera posee respecto de los segundos. En esta línea, Agesic se propone plantear la institucionalidad desde la perspectiva de la estructura necesaria para el desarrollo, monitoreo y auditoría de una política pública en IA y datos, desde las competencias requeridas a la interna de las organizaciones públicas, y desde las normas que hoy en día ya regulan la forma en que se gobiernan los datos a nivel nacional.

En lo que tiene que ver con la institucionalidad para la IA, es importante considerar antecedentes internacionales, pero bajo el prisma de la idiosincrasia local, en tanto 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 IA, 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 Agesic, denominado Unidad Reguladora y de Control de Datos Personales (Urcdp), 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 al 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 obstan a 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 IA en Uruguay deberá contemplar sí los antecedentes internacionales y nacionales asociados al tema, pero reiteramos, analizados a la luz de la idiosincrasia local.

Conjuntamente con la institucionalidad de la IA, 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 incluye distintos tipos

de datos -personales y no personales-, su gestión, las entidades 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 cuando estos alimenten o sean generados por sistemas de IA.

Selección de antecedentes internacionales

El actual texto del Convenio de IA del Consejo de Europa (CoE)[44] establece en su artículo 1° que las partes deben adoptar y mantener medidas legislativas, administrativas u otras apropiadas 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 Convenio plantea, con matices, la aplicabilidad de sus disposiciones para el ámbito público y privado.

En materia de innovación, el 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. Cabe recordar que el artículo 75 de la Ley N° 20.212 dispuso la posibilidad de 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 Convenio es un principio central; que las personas conozcan efectivamente que están interactuando con un sistema de IA, y los mecanismos de supervisión son parte integrante de esa transparencia.

En lo que respecta al Reglamento Europeo en IA[45], su 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.

[44] https://www.coe.int/en/web/artificial-intelligence/the-framework-convention-on-artificial-intelligence. Últ. Acceso: 13/06/2024.

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

El capítulo 2 del Título VI del Reglamento 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.

El Reglamento Europeo de IA o Ley de IA de la UE forma parte de un conjunto de regulaciones que refieren a la gobernanza de los datos y que buscan –en el marco de la Estrategia europea de Datos[46]- crear un mercado único en que los datos fluyan libremente entre distintos sectores de la sociedad. Este ecosistema se encuentra integrado por la Digital Services Act, la Digital Governance Act, la Digital Markets Act, la Data Act, la e-Privacy Regulation y el GDPR (Reglamento Europeo de Protección de Datos).

En los Estados Unidos, encontramos la Orden Ejecutiva en el desarrollo y uso seguro, fiable y confiable de sistemas de Inteligencia Artificial[47]. Pone énfasis en 8 principios que deben ser cumplidos por las entidades del Gobierno Federal para alcanzar los objetivos buscados y establece un conjunto de acciones que deben ser adoptadas por distintas agencias del gobierno federal en sus respectivos ámbitos de competencia, vinculadas a IA. No se prevé 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.

No puede soslayarse la influencia de la República Popular China en la materia, que adicionalmente a normas preexistentes en ciberseguridad y protección de datos personales, ha promovido medidas para la regulación de la IA en general, y la IA generativa en particular. Se prevén así medidas específicas sobre transparencia en el uso de sistemas de IA, salvaguardas ante determinados usos, aprobación

[46] Más información de esta estrategia está disponible en: https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/europe-fit-digital-age/european-data-strategy_en. Últ. Acceso: 21/06/2024.

[47] 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.

gubernamental para usos incluidos en listados, prevención de la discriminación, ejercicio de derechos por parte de usuarios, y responsabilidades punibles con sanciones de multas[48].

Reino Unido por su parte, publicó un documento con una aproximación pro-innovación a la regulación de IA[49], que surge luego de una consulta pública realizada por un plazo de 1 año. Adicionalmente, Reino Unido creó una Oficina para la Inteligencia Artificial que es parte del Departamento de Ciencia, Innovación y Tecnología, y una 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. Previamente y hasta junio de 2023 había contado con un Consejo de IA integrado por expertos de múltiples sectores, 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. 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.

[48] Una síntesis de qué esperar de la normativa china puede encontrarse en el Observatorio Parlamentario, Programa Asia Pacífico de la Biblioteca Nacional de Chile, disponible en https://www.bcn.cl/observatorio/asiapacifico/noticias/andamiaje-institucional-inteligencia-artificial-china. Últ. Acceso: 21/06/2024. Adicionalmente, puede encontrarse una traducción al inglés de la propuesta legislativa en la web del “Center for Security and Emerging Technology - Georgetown University's Walsh School of Foreign Service” https://cset.georgetown.edu/publication/china-ai-law-draft/. Últ. Acceso: 21/06/202.

[49] 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.

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.

Diagnóstico en materia de Institucionalidad y gobernanza 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. En el marco de esas competencias se le atribuye a la Agencia la posibilidad de crear grupos de trabajo y otras instancias con distintos actores que colaboren en la implementación de las estrategias.

En función de dicho artículo, recientemente Agesic creó el **Comité Estratégico del Sector Público para la Inteligencia Artificial y Datos,** integrado por representantes de dicha Agencia, del Ministerio de Industria, Energía y Minería, el Ministerio de Educación y Cultura, el Ministerio de Trabajo y Seguridad Social, el Ministerio de Economía y Finanzas, el Instituto Nacional de Estadística, el Instituto Nacional de Derechos Humanos y Defensoría del Pueblo, la Agencia Nacional de Investigación e Innovación, y de la Unidad Reguladora y de Control de Datos Personales.

Adicionalmente, el inciso final del artículo 74 prevé un cometido que excede el vinculado a la estrategia, y refiere al desarrollo de sistemas de inteligencia artificial, para lo que Agesic podrá establecer criterios y definir mecanismos de fiscalización de su cumplimiento. Dicho inciso en concreto establece: “AGESIC 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”.

Consecuente con esta disposición, se establece que esa competencia es sin perjuicio, en primer lugar, de las competencias de la Urcdp, quien puede determinar 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.

En el aspecto de institucionalidad, corresponde mencionar dentro de este diagnóstico, las reflexiones emergentes del proceso de consulta. La INDDHH, propone por su parte, que, atento a atribuciones asignadas a Agesic y a la Urcdp de fijación de criterios generales y fiscalización, su ámbito de actuación debería situarse fuera del Poder Ejecutivo, sugiriéndose específicamente atribuirle la forma jurídica de servicio descentralizado.

Al respecto, es opinión de esta Agencia que, si bien la propuesta es entendible y atendible, la institucionalidad existente permitiría llevar adelante una adecuada gobernanza de la IA, por lo menos en la actualidad. Sin perjuicio de ello, se adjunta la propuesta completa de la INDDHH por anexo, para su consideración por el Poder Legislativo.

La CUTI en sus aportes manifiesta que la institucionalidad existente en Uruguay sería adecuada para tratar los desafíos planteados, sin perjuicio de la necesidad de contar con grupos asesores con participación de múltiples actores y un rol relevante en la definición de políticas.

Para que la gobernanza de IA y la adopción de dicha tecnología sea de forma confiable y responsable, también deben considerarse medidas para una adecuada gobernanza y gestión de datos. Los datos son uno de los insumos principales de dicha tecnología y su principal resultado. A su vez, para que los datos sean confiables y puedan ser utilizados es importante asegurarse que exista una gestión adecuada de éstos, definiendo y adoptando normativas, políticas y lineamientos, para lo cual resulta relevante considerar estándares nacionales, regionales e internacionales en la materia.

Si bien nuestro país no cuenta con una gobernanza de datos establecida en el sector público en forma completa, existen determinados avances que colaboran en su construcción.

Existen determinadas competencias de Agesic en este campo, como las normas de intercambio de información e interoperabilidad, gobierno abierto y datos abiertos, que fueron compiladas en el decreto N° 184/015, de 14 de julio de 2015. Asimismo, las unidades desconcentradas de la citada Agencia, la Urcdp y la Unidad de Acceso a la Información Pública (Uaip) tienen competencia a nivel nacional en lo que respecta a la gestión de la información personal y de la información pública, respectivamente.

Los aportes a la consulta realizada se orientaron hacia la sugerencia de mecanismos específicos para la protección de los datos (como el análisis de los fideicomisos de datos propuestos por la INDDHH), la adopción de mecanismos para resolver conflictos entre la promoción de la innovación en el desarrollo de servicios públicos y el impacto de un eventual fracaso en ese ámbito (CUTI) y la generación de estándares que permitan evaluar soluciones uruguayas y “exportarlas” (CUTI).

Relacionado con la forma en que se utilizan sistemas de IA, la AEU menciona la importancia de considerar sectores o usos específicos, puntualmente en el ámbito judicial (proponiendo sistemas de “caja blanca” basados en técnicas para realizar predicciones, clasificaciones y detecciones inteligentes), del scoring (enfatizando en la imposibilidad de uso de datos que no formen parte de aquellos empleados para la finalidad determinada y la necesidad de explicabilidad) y en el contractual y notarial (donde desaconsejan el uso de datos sintéticos).

Línea Derechos Humanos

Consideraciones preliminares

El objetivo de esta línea es plantear cuales son los riesgos que no pueden soslayarse en el desarrollo de una política pública en materia de IA, y pueden requerir –de entenderlo necesario- medidas especiales, por su impacto en los derechos de las personas.

Adicionalmente, el objetivo es identificar medidas para aprovechar los sistemas de IA en beneficio de las personas y de sus derechos, identificando en particular medidas 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 IA realizadas por organismos internacionales y la regulación vigente o en proceso de elaboración a nivel regional e internacional.

Los impactos de la IA 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 Humanos[50] 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,

[50] 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.

desarrollo, implementación y uso de los modelos, instrumentos y servicios resultantes".

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.

En nuestro país y relacionado con la política de Derechos Humanos, debe mencionarse especialmente el Plan Nacional de Derechos Humanos 2023-2027, donde se incluye 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 arriba mencionado, al 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 de la IA en los objetivos definidos.

Selección de antecedentes internacionales

En la ya mencionada "Recomendación sobre la ética de la inteligencia artificial" 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.

Asimismo, dicha recomendación considera 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 de su ciclo de vida. 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 la denominada Evaluación de Impacto Ético.

La Evaluación de Impacto Ético 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".

Como se mencionó precedentemente, la reciente resolución de la Asamblea General de la ONU[51] para la promoción de sistemas de IA seguros y fiables que

[51] Puede obtenerse más información en: https://news.un.org/es/story/2024/03/1528511#:~:text=La%20Asamblea%20General%20de%20la%20ONU%20adopt%C3%B

permitan alcanzar los Objetivos de Desarrollo Sostenible (ODS), contiene en particular recomendaciones de medidas a ser adoptadas por los Estados Miembros.

También en el marco de la ONU merece un destaque particular el documento de diciembre de 2023 “Interim Report: Governing AI for Humanity”[52], que contiene entre otros una categorización de riesgos desde la perspectiva de la vulnerabilidad existente o potencial 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 ODS.

Siguiendo con antecedentes internacionales, la regulación comunitaria de la Unión Europea, aprobada por los países miembros el 13 de marzo de 2024 establece algunos aspectos de relevancia destacados por la propia organización[53]:

1) Reglas para distintos tipos de Riesgos:

    a. Riesgos inaceptables, prohibidos por constituir una amenaza para las personas: manipulación cognitiva del comportamiento de grupos de personas vulnerables, “scoring” social, identificación y categorización biométrica de las personas, 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

3%20por,que%20beneficien%20tambi%C3%A9n%20al%20desarrollo%20sostenible%20para%20todos. Últ. Acceso: 25/03/2024.

[52] 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.

[53] 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.

específicas que deben ser registrados en una base de datos de la UE (Gestión y operación de infraestructura crítica, Capacitación vocacional y educación, trabajo, gestión de trabajadores y acceso a empleo, acceso y goce de servicios privados esenciales y servicios públicos y beneficios, cumplimiento de la ley, migración, asilo y gestión de control de fronteras, 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 saber:

    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. Ello a través de la generación de condiciones que estimulen la prueba de modelos de IA previo a su puesta en producción.

En el caso del Reino Unido, el proyecto regulatorio presentado y puesto a consulta pública en el correr del año pasado tuvo por objeto alcanzar una aproximación pro-innovación y pro-seguridad.

Dicho proyecto distingue 3 categorías de riesgos: 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.

La distinción en riesgos se encuentra también presente en proyectos que se están discutiendo a nivel sudamericano, como el proyecto N° 2338[54] de la República Federativa de Brasil, en el que distinguen sistemas de riesgo alto y excesivo, con la posibilidad de imponer estrictas medidas para su desarrollo y puesta en marcha. El gobierno chileno por su parte, remitió el 7 de mayo de 2024 al Parlamento un proyecto de ley[55] en el que también distingue los sistemas de IA de riesgo inaceptable, aquellos de alto riesgo, y agrega sistemas de riesgo limitado.

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 gubernamentales[56]. Dentro de las medidas previstas en la Orden Ejecutiva se encuentran la generación de estándares en seguridad, la protección de la privacidad de los estadounidenses, avanzar en derechos civiles y equidad, proteger a los consumidores, pacientes y estudiantes, dar apoyo a los trabajadores, promover la innovación y la competencia, avanzar en el liderazgo de Estados Unidos en el extranjero, y asegurar el uso gubernamental responsable y efectivo de la IA (en el anexo de normativa internacional se presentan las medidas con un mayor grado de detalle).

[54] https://legis.senado.leg.br/sdleg-getter/documento?dm=9347622&ts=1718367327465&disposition=inline. Últ. Acceso: 13/06/2024.

[55] https://www.camara.cl/verDoc.aspx?prmID=17048&prmTIPO=INICIATIVA. Últ. Acceso: 14/06/2024.

[56] 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.

Diagnóstico en materia de IA y Derechos Humanos

El diagnóstico en esta línea se centra en 5 aspectos centrales, vinculados a los puntos mencionados por el Alto Comisionado de las Naciones Unidas para los Derechos Humanos, y detallados arriba.

1. ¿Es necesario reforzar la aplicación de las normas y principios de derechos humanos preexistentes a través de instrumentos normativos que expliciten y especifiquen su aplicación en el ámbito de la IA 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. ¿Puede la autorregulación constituirse en un remedio efectivo para dirigir las acciones de entidades públicas y privadas en el desarrollo de IA?
3. ¿Es suficiente el enfoque de riesgos?, y como corolario, ¿existen sistemas de IA que por su impacto en los derechos de las personas deban ser prohibidos o limitados, o que requieran la imposición de medidas especiales?
4. ¿Cuáles son las garantías de transparencia y explicabilidad que deben establecerse en el marco del desarrollo de sistemas de IA centrados en las personas?
5. ¿Cuáles son los criterios orientadores para la definición de una política pública asociada al desarrollo de la IA en nuestro país que permita además 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 son de plena aplicación, en la medida en que estos principios fueron previstos 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 puntualmente en relación con la política de IA.

Como se mencionó, los principios incluidos en el artículo 74 se encuentran alineados a los consagrados en el primer Convenio Internacional en la materia elaborado por el CoE. 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 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 ya presente en la regulación de la protección de datos personales, la que además puede ser aplicable a los sistemas de IA cuando se utilicen o generen este tipo de datos.

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 prevé la realización de estas 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.

A modo de ejemplo, el artículo 6° literal c del decreto mencionado 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. Es cierto que existen ciertas circunstancias en que el ámbito de aplicación de esta ley puede no alcanzar algunas situaciones, tal y como señala la sociedad civil en la respuesta a la consulta y como se verá luego.

En lo que respecta a la autorregulación, existen múltiples ejemplos. En particular en materia de datos, las normas en protección de datos personales pueden servir para ejemplificar cómo funcionan estos mecanismos (ver por ejemplo los códigos de conducta previstos en el artículo 36 de la Ley N° 18.331).

La adopción de esquemas de co-regulación que establezcan normativamente determinadas líneas rojas y mecanismos de supervisión parecen un camino más conveniente. Estas definiciones pueden observarse en el trabajo de MANTELERO[57], 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 además de la aproximación co-regulatoria, las propuestas planteadas por estas organizaciones se decantan hacia una aproximación basada en riesgos más que en una basada en principios.

En cuanto a la eventual imposición de medidas especiales, también ello se vincula con el análisis de los impactos en los derechos de las personas, con otras medidas para una más efectiva supervisión del funcionamiento de los sistemas. La creación de registros de algoritmos, la solicitud de una autorización especial previa o incluso la obligación de realizar pruebas en entornos controlados, pueden ser instrumentos útiles para determinados tipos de sistemas y ante determinado tipo especial de riesgos.

En lo que hace relación con el principio de transparencia y explicabilidad, el Grupo de Expertos de Alto Nivel para la Inteligencia Artificial de la Comisión Europea (AI HLEG), en sus “Directrices Éticas para una IA Fiable” [58] señala que la explicabilidad –elemento central de la transparencia junto a la trazabilidad y la comunicación- es la

[57] 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.

[58] https://digital-strategy.ec.europa.eu/es/library/ethics-guidelines-trustworthy-ai. Últ. Acceso: 14/06/2024.

habilidad para explicar tanto los procesos técnicos de un sistema de IA como las decisiones humanas vinculadas. En nuestro derecho, la explicabilidad posee consagración normativa expresa en dos disposiciones de la Ley N° 18.331: los artículos 13 y 16.

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".

Sin perjuicio de lo indicado, resulta necesario considerar efectivamente soluciones más amplias para sistemas de IA que no realicen tratamientos de datos personales, o en casos de destinatarios que deban estar en conocimiento de su interacción con dichos sistemas aun cuando no sean sus propios datos los utilizados por éstos.

En materia de empleo de sistemas de IA en la Administración Pública, corresponde mencionar la Ley N° 18.381, de 17 de octubre de 2008, que tiene por objeto

promover la transparencia de la función administrativa de todo organismo público, sea o no estatal, y garantizar el derecho fundamental de las personas al acceso a la información pública (artículo 1°). Su decreto reglamentario N° 232/010, de 2 de agosto de 2010 establece en su artículo 6° el principio de la máxima publicidad, de forma que los sujetos obligados proporcionen la información de la forma más amplia posible, y su artículo 38 incluye dentro de la información que obligatoriamente deben difundir los sujetos obligados por la ley en sus sitios web, “cualquier otra información que pudiere ser de utilidad o relevante para el conocimiento y evaluación de las funciones y políticas públicas que son responsabilidad del sujeto obligado”.

De esta forma, la obligación de transparentar, pero sobretodo explicar las decisiones adoptadas por las entidades públicas cuando emplean sistemas de IA encuentra su fundamento no en una sino en dos leyes fundacionales del entorno digital.

En lo que refiere a eventuales criterios orientadores para la política pública en la materia, éstos podrían asociarse al cumplimiento de principios y a la provisión de herramientas prácticas que permitan el desarrollo innovador, el control del ajuste a las normas en derechos humanos, y mecanismos de supervisión.

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.

Podemos afirmar que la mayoría de las inquietudes recibidas de las entidades que participaron en la consulta realizada se centraron en esta línea temática. Así, por ejemplo, CUTI manifiesta que si bien el marco legal e institucional actual sería adecuado para el manejo de los riesgos potenciales derivados del uso de IA -atento además a las actualizaciones realizadas a la ley de protección de datos personales-, sería necesario un comité o grupo específico para evaluar el impacto en los

derechos humanos, y un abordaje cauteloso de la clasificación de riesgos, de forma de no impactar en la innovación y la inversión en IA.

El diagnóstico emanado de las instituciones de la sociedad civil vinculado a la suficiencia o no de las normas plantea que las disposiciones de la ley de protección de datos personales no resultan suficientes por dirigirse, entre otras cosas, exclusivamente a los tratamientos de datos personales, por lo que deberían incluirse disposiciones que especifiquen el concepto de “supervisión humana significativa”, habiliten el ejercicio de derechos colectivos, la publicación de evaluaciones de impacto, los requisitos para la explicabilidad, trazabilidad y auditabilidad de algoritmos, la garantía de interacción humana y presencial con la administración pública, y las relaciones entre derechos de autor, secreto comercial y auditabilidad de sistemas de IA (propuestas de DATYSOC).

En el caso de DATA, se resalta la importancia del derecho previsto en el artículo 16 de la ley de protección de datos personales, pero se aclara que es necesario que se apliquen esos estándares a la administración pública a través de modificaciones a la ley N° 18.381. Ponen además énfasis en la discusión sobre sistemas de alto riesgo y el establecimiento de garantías básicas, y la necesidad de otorgar apoyos al trabajo de la INDDHH.

En el caso de la AEU, en esta línea se plantea la consideración de si es necesaria una normativa general o sectorial, y evalúa como conveniente el enfoque de riesgos, teniendo en cuenta además la asignación y distribución de responsabilidades por daños. Todo ello con centro en el ser humano y contemplando la obligatoriedad de que las empresas expliciten dónde y cómo utilizan IA, y considerando además el deber de prevenir y asegurar que no se reflejen actitudes discriminatorias y evitar riesgos. Asimismo, plantea el establecimiento de evaluaciones de impacto en los derechos humanos de los desarrollos de IA y el fortalecimiento del rol del consentimiento informado y del principio de finalidad previstos en la Ley N° 18.331.

Surge de las respuestas a las consultas recibidas de la sociedad civil la necesidad de detenerse en el análisis del uso de la IA en el ámbito de la vigilancia por parte de las fuerzas de seguridad, lo que se considerará en otro capítulo.

Línea Propiedad Intelectual

Consideraciones preliminares

Se señala por la Organización Mundial de la Propiedad Intelectual (OMPI)[59] 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). Los secretos comerciales se incluirán como parte de la discusión.

Las conexiones entre la Propiedad Intelectual y la innovación son innegables[60], así como los impactos de la Inteligencia Artificial sobre ésta[61]. El Plan Nacional de Inteligencia Artificial de la República Argentina[62] 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[63] 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;

[59] "¿Qué es la Propiedad Intelectual?" disponible en: https://www.wipo.int/publications/es/details.jsp?id=4528. Últ. Acceso: 25/03/2024.

[60] "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.

[61] "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.

[62] https://oecd-opsi.org/wp-content/uploads/2021/02/Argentina-National-AI-Strategy.pdf Últ. Acceso: 26/03/2024.

[63] https://www.wipo.int/edocs/pubdocs/es/wipo-pub-rn2023-11-es-ai-inventions.pdf. Últ. Acceso: 13/06/2024.

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 en forma previa a establecer modificaciones a la normativa.

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 por IA. MANTEGNA[64] en este punto propone distintas alternativas, con el fin de regular las creaciones asistidas por IA y las generadas por IA, que van en línea con las alternativas propuestas por OMPI.

Teniendo en cuenta lo indicado por la citada autora, el alcance de esta línea se relaciona con 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.

[64] MANTEGNA, Micaela. “ARTEficial: Creatividad, Inteligencia Artificial y Derechos de Autor”. Ed. CDYT, 2022. Págs. 299 y sigs..

Por su parte, y por su impacto, resulta necesario evaluar la cuestión de la propiedad intelectual en los desarrollos aplicados por el Estado al utilizar la IA para la provisión de sus servicios y el cumplimiento de sus cometidos.

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, vinculado al impacto de la IA[65]. En dicho proyecto, se plantean en pocos artículos, algunas disposiciones significativas:

- 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;

- 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;

- 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;

- 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.

En el caso de la legislación de Reino Unido, el artículo 9 (3) de la Ley de 1988 de Derechos de Autor, Diseños y Patentes[66] en materia de autoría, establece que cuando la obra literaria, dramática, musical o artística fue generada por

[65] https://www.assemblee-nationale.fr/dyn/16/textes/l16b1630_proposition-loi. Últ. Acceso: 26/03/2024.

[66] https://www.legislation.gov.uk/ukpga/1988/48/contents. Últ. Acceso: 27/03/2024.

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-.

La citada Resolución la Asamblea General de la ONU A/RES/78/265[67], pone foco en la Propiedad Intelectual al establecer: “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”.

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.

Diagnóstico en materia de IA y Propiedad Intelectual

Como primer punto, debe mencionarse 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

[67] https://documents.un.org/doc/undoc/gen/n24/087/86/pdf/n2408786.pdf?token=q7sbXbo0iQB4sT9YhT&fe=true. Últ. Acceso: 14/06/2024.

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 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 ots[68], 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, aun cuando pueda resultar prudente preguntarse si es posible atribuir la titularidad de los derechos al sistema de IA –a través de una especie de personalidad electrónica-, a una persona física o jurídica en particular –desarrollador, usuario u otros- a un conjunto de personas, o entender que ésta debe ser del dominio público, no parecen estar dadas las condiciones para dar una respuesta en este momento.

El empleo de datos de entrenamiento en los modelos de IA es otro punto a dilucidar, con el fin 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 de estos sistemas, o si se requieren excepciones especiales –como puede encontrarse en el proyecto de ley de IA de Brasil[69]-.

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

[68] 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 Ecnomómica. N° 77/2024. Disponible en: https://www.wipo.int/publications/en/details.jsp?id=4715. Últ. Acceso: 26/03/2024.

[69] https://www25.senado.leg.br/web/atividade/materias/-/materia/157233. Ver en particular el artículo 42. Últ. Acceso: 27/03/2024.

En lo que respecta al secreto comercial, existen distintas normas vinculadas al tema[70] -como artículo 39 del Acuerdo sobre los Aspectos de Propiedad Intelectual relacionados con el Comercio (ADPIC)-.

En materia de datos personales los alcances de la información que deben divulgar las empresas y organizaciones en determinados tipos tratamiento automatizados de datos personales se encuentran contemplados en los artículos 13 y 16 de la Ley N° 18.331.

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 IA.

En el marco de la discusión sobre el alcance de esta línea, la DNPI planteó algunos aspectos que corresponde mencionar. Así, se señaló que el sistema de propiedad intelectual implica un mecanismo de incentivos para capturar valor, permitiendo a los creadores negociar y evitar el aprovechamiento indebido de sus creaciones. Se indica en particular que no es posible, en esta instancia, trasladar ese fundamento a las creaciones de la IA.

Dicha Dirección, además, sustenta que, en nuestro país, por seguir la tradición europea continental, el derecho del autor se ve como una extensión de los derechos de la personalidad, consagrando derechos morales inalienables e irrenunciables a favor del autor; por su parte respecto a la originalidad, ésta se entiende como una expresión de la personalidad del autor. En el caso de las patentes, los derechos inalienables refieren al reconocimiento como inventor, atento a lo dispuesto por el artículo 2° de la Ley N° 17.164, de 2 de setiembre de 1999.

Así, y siguiendo a la normativa vigente, para otorgar derechos exclusivos sobre la invención al inventor, éste debe proporcionar una descripción clara, detallada y

[70] 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.

completa del invento; con la intervención de algoritmos u otros mecanismos de IA la cuestión está en esa posibilidad de brindar efectivamente una descripción completa de la forma en que dichos algoritmos llegan a un resultado u otro, o generar un efecto “black box”.

También se plantearon consideraciones en materia de Propiedad Intelectual en las respuestas a la consulta realizada por DATYSOC, que mencionó la omisión de la legislación vigente en el uso de obras con fines de análisis computacional (incluyendo la restricción de la condición de que los usos citados no compitan con la normal explotación de las obras y no dañen injustificadamente los intereses de los autores, para lo que proponen además una redacción), además de la necesidad de regular las relaciones entre derechos de autor, secreto comercial y auditabilidad de los sistemas (que en el aspecto puntual de la propiedad intelectual implicaría excepciones habilitantes del ingreso, copia y análisis de sistemas para auditarlos a solicitud de un Juez o cuando la ley así lo disponga), y establecer prohibiciones vinculadas a usos competitivos, o que perjudiquen al autor o titular de los derechos de las obras en forma injustificada.

En el caso de DATA, se alinea con la necesidad de dar mayor apoyo en la toma de decisiones de adquisición de software o soluciones basadas en IA por la Administración Pública, señalando la posibilidad de realizar adaptaciones a la Ley N° 19.179, de 27 de diciembre de 2014, y su decreto reglamentario N° 44/015, de 30 de enero de 2015. Ello, además de considerar la posibilidad de crear un mecanismo de intervención para que Agesic pueda determinar el riesgo y asesorar a entidades públicas sobre la realización de evaluaciones de impacto previas a las adquisiciones de soluciones basadas en IA para algunos sectores.

Línea Infraestructura y Ciberseguridad

Consideraciones preliminares

El desarrollo de IA depende de varios factores. Uno de ellos es la adecuada infraestructura, para lo que el Estado asume un rol central.

El Ministerio de Inteligencia Artificial de los Emiratos Árabes Unidos publicó en noviembre de 2020 un reporte[71] 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 tres: 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 OCDE publicó en febrero de 2023 su reporte N° 350[72] 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: 1) evaluar la revisión de las capacidades computacionales especialmente para IA en actores del sector público y privado, considerando el uso de servicios de nube en 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

[71] https://ai.gov.ae/infrastructure_report/. Últ. Acceso: 28/03/2024.

[72] 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.

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, y en ese sentido, corresponde considerar la existencia y suficiencia o no de normas asociadas a:

1) infraestructura para la gestión y el intercambio de datos
2) el almacenamiento de información
3) ciberseguridad
4) redes de telecomunicaciones

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, cuando afirma que muchos países han desarrollado estrategias nacionales de IA sin haber analizado en forma completa si tienen la infraestructura computacional y software para IA suficiente a fin de alcanzar sus objetivos.

La iniciativa de **Infraestructura Pública Digital** promovida desde el PNUD[73], mencionada anteriormente, 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.

[73] https://www.undp.org/digital/digital-public-infrastructure, Últ. Acceso: 02/05/2024.

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 pro-innovación.

Diagnóstico 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 privadas[74].

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, dos normas podrían ser de trascendencia en este punto: a) el artículo 74 de la Ley N° 19.149, de 24 de octubre de 2013, 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

[74] 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.

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 al almacenamiento de información, 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 decreto[75], pero debería considerarse la posibilidad de una actualización, en línea con los criterios definidos por la Agencia[76].

En cuanto a la infraestructura habilitante del intercambio de información, Agesic tiene a disposición la Plataforma de Interoperabilidad, creada 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 definido en ésta. Sí puede

[75] "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 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.

[76] "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-estado#:~:text=Con%20el%20fin%20de%20guiar%20a%20las%20entidades,este%20documento%20principios%20generales%20a%20tener%20en%20cuenta. Últ. Acceso: 30/03/2024.

señalarse qué, aunado a una regulación profusa y preexistente en la materia, existió una actualización reciente por los artículos 78 y siguientes de la Ley N° 20.212.

En el marco de las discusiones respecto a la elaboración del informe, desde DINATEL se remitieron propuestas vinculadas al alcance y diagnóstico realizado en esta línea temática.

Así, se planteó considerar el estado de la normativa actual en el ámbito de la infraestructura para la gestión y el intercambio de datos, el almacenamiento de información, las obligaciones en materia de ciberseguridad, las redes de telecomunicaciones (robustez y calidad de servicio), la identificación de infraestructura crítica, los acuerdos internacionales en materia de intercambio de datos y la asociada a responsabilidades civiles, además de la temática de la infraestructura de nube y la actualización de la regulación actual de datos en la nube.

Se señaló por DINATEL que el desarrollo de la IA en este punto debe incorporar las necesidades de infraestructura por fuera del sector telecomunicaciones, una visión de impacto social y una regulación no restrictiva o leyes de promoción para la instalación en el país y uso de data centers públicos y privados para fines públicos. Ello además de otros aportes que se adjuntan en el anexo del presente documento.

Línea trabajo y capacitación en IA

Consideraciones preliminares

Los impactos de la IA 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.

El presente informe, en esta línea puntual, procuró identificar medidas para 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 el reporte elaborado por la OCDE titulado “Perspectivas de empleo de la OCDE 2023: La inteligencia artificial y el mercado laboral”[77] se indica que el impacto de la IA generará cambios en las necesidades de habilidades, de las que existe además una falta actualmente, por lo que las políticas públicas desempeñarán un papel importante para incentivar la capacitación por los empleadores, como parte además, de la educación formal.

Ello es compartido por la UNESCO en la Recomendación sobre la ética de la Inteligencia Artificial, que dentro del ámbito de actuación N° 10 establece 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 reconversión laboral, entre otros. Se incluyen otras medidas vinculadas a la investigación, la competitividad de los mercados y protección de consumidores, la provisión de financiamiento cuando sea necesario, etcétera.

[77] 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.

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 Extremadura[78]. En su artículo primero establece como finalidad principal y con 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 IA del gobierno de los Estados Unidos, 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.

Diagnóstico en materia de trabajo y capacitación para la IA

Existen distintas disposiciones a nivel nacional que prevén 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, más allá que la capacitación a trabajadores en el ámbito digital se encuentra presente en programas como los llevados adelante por el Instituto Nacional de Empleo y Formación Profesional (INEFOP), o por la Escuela Nacional de Administración Pública (ENAP) en el caso de trabajadores del sector público.

[78] https://www.boe.es/buscar/doc.php?id=BOE-A-2023-8795. Últ. Acceso: 31/03/2024.

Por lo expresado, 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.

Línea responsabilidad civil y derechos del consumidor

Consideraciones preliminares

La IA 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 CORES[79], 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 SANTOS[80] 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 su evolución.

[79] 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.

[80] JOSÉ DOS SANTOS, Sonia "Inteligencia Artificial y Responsabilidad Civil" en "Inteligencia Artificial y Derecho" 1ª. Ed. Ed. Hammurabi. 2020. Pág. 179 y sigs.

Dentro del concepto de responsabilidad civil, la distinción más común es la realizada entre la contractual –derivada del incumplimiento de un contrato entre dos o más partes- o extracontractual –derivada del perjuicio ocasionado a alguien, sin existir dicho vínculo contractual-. El régimen de responsabilidad civil, se encuentra regulado en Uruguay primariamente 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 encuentran desde el punto de vista subjetivo las figuras de proveedor y consumidor.

ARAMENDIA[81] 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.

La autora plantea tres 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, 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.

[81] 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.

Selección de antecedentes internacionales

Resulta en este punto relevante considerar la propuesta de Directiva sobre Responsabilidad de la IA de la Unión Europea[82], que complementa el Reglamento recientemente aprobado.

Señala CASALS[83] 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 Europea[84] 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".[85]

---

[82] https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=CELEX%3A52022PC0496. Últ. Acceso: 30/03/2024.

[83] 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.

[84] https://ec.europa.eu/commission/presscorner/detail/es/ip_22_5807. Últ. Acceso: 30/03/2024.

[85] 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=H4sIAAAAAAAEAMtMSbF1CTEAAmNDCwsjI7Wy1KLizPw8WyMDIwNDQyMDkEBmWqVLfnJIZUGqbVpiTnEqANKvjtI1AAAAWKE. Últ. Acceso: 30/03/2024.

Un proyecto de ley presentado en la República Argentina[86] 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.

Diagnóstico en materia de responsabilidad civil y derechos del consumidor

El primer punto del diagnóstico es que 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 aplicarse por analogía en estos casos –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 de IA- 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

[86] 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 BORDOLI[87], 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.

[87] 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.

Línea de medidas de promoción para la IA

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 ventajas.

Puede considerarse al respecto el reporte interino del Órgano Asesor en Inteligencia Artificial de la ONU de diciembre de 2023[88], 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.

La pertinencia y alcance de eventuales medidas de promoción de IA debe tener 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 éstos.

[88] https://www.un.org/sites/un2.un.org/files/ai_advisory_body_interim_report.pdf. Últ. Acceso: 04/04/2024.

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 Unidos[89] 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 Europea[90] 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 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.

[89] 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.

[90] https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=celex:52021PC0206. Últ. Acceso: 04/04/2024.

En Brasil, el proyecto de ley N° 2338/2023[91] 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 IA.

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.

Diagnóstico preliminar en materia de medidas de promoción en IA

Actualmente existen algunas 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, existen 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.

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

Otras líneas temáticas relevadas en función de los aportes recibidos

El uso de sistemas de IA con fines de vigilancia

Dentro de las inquietudes y recomendaciones planteadas desde la sociedad civil al momento de responder al documento de consulta puesto a disposición por esta Agencia, se plantean cuestiones asociadas al uso de sistemas de IA con fines de vigilancia por parte de las fuerzas de seguridad.

La Ley N° 19.696, de 29 de octubre de 2018, reglamentada por decreto N° 157/022, de 23 de mayo de 2022, establece y regula el Sistema Nacional de Inteligencia del Estado (SNIE), imponiendo a los órganos que lo integran el cumplimiento de un conjunto de principios con el objetivo del respeto a la Constitución, y a los principios del régimen democrático republicano de gobierno y el respeto a los derechos humanos.

En ese marco, el artículo 20 de la Ley dispone que la búsqueda de información mediante procedimientos especiales que puedan afectar la libertad y privacidad de los ciudadanos deberá ser autorizada por el Poder Judicial. En materia de controles, cabe destacar el artículo 25 que prevé la creación en el marco de la Asamblea General, de una comisión parlamentaria bicameral con el cometido de controlar y supervisar la actuación del sistema.

El decreto N° 157/022 aprueba la Política Nacional de Inteligencia, especificando un conjunto de acciones y medidas, pero sin perjuicio de referencias genéricas al cumplimiento de los derechos humanos, no se realiza previsión alguna con relación a la aplicación de la IA en las actividades de vigilancia de las personas.

La sociedad civil, en el marco de la respuesta a la consulta realizada, plantea sugerencias como la de imponer una moratoria en la adquisición de software de vigilancia hasta que no exista una base legal que regule adecuadamente el ecosistema de vigilancia policial, o la posibilidad de exigir la auditabilidad y explicabilidad algorítmica, la trazabilidad, protocolos de control de acceso y la descripción de responsabilidades detalladas sobre quienes usan estos sistemas de vigilancia.

Por su parte, la sociedad civil también plantea el establecimiento de líneas rojas en cuanto a qué usos están estrictamente prohibidos a la policía y qué usos requieren orden judicial, la prohibición del uso de vigilancia biométrica en tiempo real y sin orden judicial en espacios públicos y una regulación específica de la admisibilidad, valoración y diligenciamiento de los matches biométricos como métodos de investigación y como prueba digital, entre otros.

Finalmente, las recomendaciones de la sociedad civil incluyen el entrenamiento adecuado de los funcionarios policiales, jueces y fiscales -mediante una certificación obligatoria- y en una regulación del uso de la IA con fines de vigilancia por parte del Ministerio del Interior, con carácter urgente.

Esta Agencia comparte la preocupación por un adecuado empleo de los sistemas de IA en el marco de las actividades de las fuerzas de seguridad, pero también quiere enfatizar que es necesario establecer un diálogo multisectorial, a fin de contemplar un adecuado equilibrio entre las necesidades asociadas a la seguridad interna y la protección de derechos fundamentales de las personas.

Inserción y cooperación internacional

Otro de los aspectos que no fueron parte de las líneas iniciales, pero que tiene una enorme relevancia, es la inserción internacional del país. Como con otros temas en la agenda de nuestros países, la IA plantea retos globales que nos motiva a buscar soluciones globales.

Por otra parte, en tanto el desarrollo de sistemas de IA aplicados por la región son “importados” de otras partes del mundo, debemos hacer un esfuerzo adicional por generar mecanismos de cooperación regionales que contemplen nuestras propias necesidades.

Como parte de la Agenda Común[92] presentada por el Secretario General de la ONU en 2021, dicha organización lanzó el año pasado la iniciativa “Global Digital

[92] https://www.un.org/en/content/common-agenda report/assets/pdf/Common_Agenda_Report_English.pdf. Últ. Acceso: 22/06/2024.

Compact – an Open, Free and Secure Digital Future for All"[93] -actualmente en proceso de consulta y que se espera sea acordada en la Cumbre del Futuro a realizarse este año- la que dentro de su objetivo 5 incluye la mejora de la gobernanza internacional de tecnologías emergentes, incluyendo la IA, para el beneficio de la humanidad. Se propone en el documento una gobernanza internacional ágil, multidisciplinaria y multiactor, y algunas iniciativas concretas como establecer un Panel Científico Internacional en IA y Tecnologías Emergentes y un Grupo de Contacto Internacional en Gobernanza de IA.

Resulta interesante de este documento, que también plantea la promoción de la cooperación Norte-Sur y Sur-Sur en materia de desarrollo de conjuntos de datos, capacidad computacional, soluciones locales, casos de uso y ecosistemas empresariales en países en desarrollo.

A nivel internacional ya se ha mencionado el Convenio Marco de IA promovido por el Consejo de Europa, que se constituye en el primer tratado internacional en la materia, con una visión de principios y también de riesgos. Al haber participado nuestro país como observador en el proceso de elaboración, tiene la posibilidad de convertirse en miembro del Convenio, lo que deberá ser valorado con el asesoramiento del Ministerio de Relaciones Exteriores. Desde ya se adelanta que esta Agencia comparte las disposiciones del Convenio y apoya la adhesión.

Finalmente, a nivel regional deben destacarse especialmente los esfuerzos de UNESCO y CAF por incorporar la voz regional en la discusión sobre el futuro de la IA. De la Primera Cumbre Ministerial y de Altas Autoridades sobre la Ética de la IA de América Latina y el Caribe organizada por éstas con el apoyo del gobierno de Chile, emanó la ya mencionada Declaración de Santiago[94], en la que se aprobó el establecimiento de un Grupo de Trabajo para la constitución de un Consejo Intergubernamental de IA para América Latina y el Caribe, en el marco de la Recomendación sobre la Ética de la IA de la UNESCO, con el propósito de fortalecer las capacidades regionales en la materia.

[93] https://www.un.org/techenvoy/global-digital-compact. Últ. Acceso: 22/06/2024.

[94] https://minciencia.gob.cl/uploads/filer_public/40/2a/402a35a0-1222-4dab-b090-5c81bbf34237/declaracion_de_santiago.pdf. Últ. Acceso: 22/06/2024.

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

En el marco del proceso de construcción del presente informe se realizaron varias reuniones con las entidades mencionadas en el presente documento, de las que pueden resumirse los siguientes aportes:

Línea Institucionalidad y gobernanza

- 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

- 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

- 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

- 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

- 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

- 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:
    - Normas para gestión e intercambio de datos
    - Capacidad de almacenamiento, capacidad de cómputos
    - Ciberseguridad

- Capacidad de conectividad e infraestructura: escalabilidad, flexibilidad y adaptabilidad a los cambios

Línea Medidas de promoción

- 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.

Recomendaciones

Conceptos previos

En los capítulos anteriores se presentó una visión del proceso y el marco aplicado en la elaboración del informe cometido a esta Agencia de conformidad con el precitado artículo 74 de la Ley N° 20.212.

Las recomendaciones que se presentan son el resultado del análisis institucional realizado a partir del diagnóstico que fue desarrollado previamente sobre los desafíos identificados para cada línea temática, en función de:

1. las orientaciones resultantes del artículo 74 de la Ley N° 20.212;
2. el marco jurídico nacional, incluyendo las normas del derecho internacional aplicables y las obligaciones jurídicas resultantes de respetar, proteger, garantizar y promover los derechos humanos en el entorno digital y fuera de éste;
3. los principios y recomendaciones emergentes de los antecedentes internacionales de soft law;
4. la revisión de los antecedentes regulatorios generados por otros países;
5. los aportes recibidos de entidades públicas, de la sociedad civil y del sector privado, en el proceso de trabajo implementado para este informe, y en el de construcción de las Estrategias lideradas por esta Agencia;
6. las orientaciones establecidas en la política digital del país emergentes del Plan de Gobierno Digital 2025[95], la Agenda Uruguay Digital 2025[96] y la Estrategia de IA para el Gobierno Digital[97].

[95] https://www.gub.uy/agencia-gobierno-electronico-sociedad-informacion-conocimiento/politicas-y-gestion/plan-gobierno-digital-2025. Últ. Acceso: 20/06/2024.

[96] https://www.gub.uy/uruguay-digital/comunicacion/publicaciones/agenda-uruguay-digital-2025-actualizacion-medio-termino. Últ. Acceso: 20/06/2024.

[97] https://www.gub.uy/agencia-gobierno-electronico-sociedad-informacion-conocimiento/comunicacion/publicaciones/estrategia-inteligencia-artificial. Últ. Acceso: 20/06/2024.

Dada la transversalidad de los sistemas de IA y sus impactos positivos y negativos actuales y potenciales en todos los sectores de la sociedad, estas recomendaciones no deberían ser interpretadas como una lista taxativa.

Éstas reflejan el resultado del análisis institucional alcanzado a la fecha de presentación de este informe sobre aspectos generales y no sectoriales, y en un contexto pautado por el vertiginoso desarrollo de las tecnologías -lo cual determina la necesidad de un análisis sostenido de las potencialidades y riesgos implicados-, la existencia de procesos en curso a nivel regional e internacional, la existencia de un proceso en curso de revisión de la Estrategia de IA y la construcción de las Estrategias Nacionales de Datos y de Ciberseguridad.

Todo ello hace previsible que en el futuro estos elementos puedan tener un impacto en los desafíos públicos a los que refieren estas recomendaciones, que necesiten ser atendidos durante el proceso de trabajo que, eventualmente, inicie el Poder Legislativo.

Por otra parte, los análisis realizados parten del conocimiento y experiencia de esta Agencia en cuestiones de transformación y política digital y de los aportes realizados por otras entidades públicas en ámbitos específicos, pero en varias de las temáticas analizadas resulta necesario generar un debate profundo con estas últimas y otros actores, antes de adoptar cualquier tipo de medida.

Recomendaciones generales.

El creciente número de instrumentos internacionales que se han venido gestando en los últimos años, reflejan un escenario en el que cada vez existe mayor consenso sobre la necesidad de regular las actividades dentro del ciclo de vida de los sistemas de IA, con el fin de garantizar que estas sean plenamente consistentes con los derechos humanos, la democracia y el Estado de Derecho, y al mismo tiempo, potenciar las oportunidades que brindan estas tecnologías para la humanidad y asegurar su acceso equitativo entre los países y al interior de éstos.

Como se expuso en este informe, estos instrumentos incluyen, entre otros: la Recomendación de la OCDE sobre IA y sus principios adoptados en 2019 que fueron actualizados en 2024; la Recomendación sobre la Ética de la Inteligencia Artificial adoptada en 2021 por la UNESCO; los principios de IA y el "Código de conducta internacional para organizaciones que desarrollan sistemas avanzados de IA" desarrollado por el G7 en 2023 en el marco del Proceso de IA de Hiroshima; el Reglamento de IA de la Unión Europea, aprobado en marzo de 2024; el Convenio Marco sobre Inteligencia Artificial adoptado por el Consejo de Europa, adoptado en mayo de 2024; y la reciente Resolución "Sistemas de inteligencia artificial seguros y confiables para el desarrollo sostenible", adoptada por la Asamblea General de la Organización de las Naciones Unidas en marzo de 2024.

A nivel interamericano, pueden citarse a modo de ejemplo, entre otros: la Declaración de Santiago para promover una inteligencia artificial ética en América Latina y el Caribe emergente en 2023 de la Cumbre Ministerial y de Altas Autoridades de América Latina y el Caribe, y la Carta regional sobre Inteligencia artificial en la administración, adoptada en el ámbito del Centro Latinoamericano de Administración para el Desarrollo (CLAD) en 2023. Uruguay ha estado atento a estos esfuerzos, y en varios casos ha participado de su gestación o bien ha adherido a los mismos.

De estos antecedentes surge el llamado claro a los Estados a respetar y actuar proactivamente para proteger y promover los derechos humanos, durante todo el ciclo de vida de la IA, adoptando para ello marcos regulatorios adecuados y efectivos, bajo un enfoque equilibrado que integre los riesgos y oportunidades que brinda la IA y promueva la innovación responsable y segura.

Se reconoce en los antecedentes presentados, que la gobernanza de la IA es un campo en evolución, que requiere avanzar en la construcción de marcos comunes, y al mismo tiempo contemplar el margen de cada Estado para establecer los enfoques e instrumentos regulatorios a nivel nacional en función de los contextos y prioridades nacionales, de forma consistente con su marco normativo y las obligaciones emergentes del derecho internacional aplicable.

En función todo lo anterior, esta Agencia considera pertinente, en primer término, respaldar la importancia de que nuestro país sostenga un enfoque proactivo para la

regulación de los sistemas de IA a través de distintos instrumentos de política pública:

1. Actualizando, bajo un enfoque de múltiples partes interesadas, su Estrategia de Inteligencia Artificial, para responder al nuevo contexto generado particularmente -y no sólo- a partir de la expansión de los modelos más avanzados como la IA Generativa; y con el objetivo de ampliar el alcance al sector privado, tal como fue dispuesto por el artículo 74 de la Ley 20.212. Dicho proceso se encuentra en curso y se espera su finalización en el segundo semestre de este año.
2. Revisando, en lo pertinente, la normativa vigente, con el objeto de:
    i) Reforzar el diseño institucional para la gobernanza de la IA en el país, incluyendo mecanismos para la participación y colaboración de las múltiples partes interesadas;
    ii) Garantizar que las actividades durante todo el ciclo de vida de los sistemas de IA sean plenamente consistentes con los derechos humanos, la democracia y el Estado de Derecho, a través de marcos que permitan identificar, prevenir, evaluar y mitigar los riesgos e impactos negativos sobre tales derechos.
    iii) Impulsar el aprovechamiento equitativo de las oportunidades y beneficios de la IA en beneficio de la sociedad y el desarrollo sostenible del país en sus diferentes dimensiones (social, cultural, ambiental y económica) promoviendo la investigación y la innovación segura y en función del interés público;
    iv) Garantizar el desarrollo y uso, ético, respetuoso de los derechos humanos, responsable y seguro de los sistemas de IA en el sector público;
    v) Fortalecer la soberanía digital y la soberanía de IA del país con visión de futuro.
3. Desarrollando desde el sector público, entre otros posibles instrumentos, protocolos consensuados, guías y recomendaciones técnicas para los sectores y ámbitos que resulten críticos para la sociedad y los intereses nacionales, y promoviendo, en lo pertinente, la adopción de instrumentos tales como pautas, códigos y otros mecanismos de autorregulación

alineados con las orientaciones nacionales; e implementando las políticas y medidas que se definan en el marco de la Estrategia Nacional de Ciudadanía Digital, la Estrategia Nacional de Datos, la Estrategia Nacional de IA y la Estrategia Nacional de Ciberseguridad.

En segundo término, tomando en cuenta las inquietudes y aportes recibidos de la sociedad civil y del sector privado durante el proceso de trabajo desarrollado para la elaboración de este informe, esta Agencia quisiera subrayar también como recomendación general, la importancia de que las medidas de regulación que se adopten:

1. sean precedidas y se sustenten en un proceso de discusión pública basado en el enfoque de múltiples partes interesadas;
2. tomen en cuenta tanto el impacto del déficit de regulación, como el impacto de la sobrerregulación;
3. sean analizadas interdisciplinariamente involucrando distintos conocimientos expertos.

Uruguay ha tenido una extensa y sostenida trayectoria en ámbitos internacionales como la Alianza para el Gobierno Abierto (OGP por sus siglas en inglés), a través de la cual ha impulsado e implementando diversas iniciativas para integrar los principios del gobierno abierto a su política digital, a la vez que ha definido los pilares del gobierno abierto como parte de los objetivos de su política digital.

En tal sentido y en consonancia también con otros enfoques internacionales como la Recomendación de la UNESCO sobre Ética de la IA, se impulsa que el país siga recorriendo y profundizando el camino de la creación participativa y transparente de sus políticas digitales a través de políticas de gobierno abierto y parlamento abierto.

Entre las sugerencias y aportes recibidos por esta Agencia durante el proceso de elaboración del informe constan las siguientes medidas específicas propuestas, que se ponen en conocimiento del Poder Legislativo:

- Creación de un foro para detectar prioridades y formular recomendaciones por parte de diferentes actores sociales.
- Realización de una audiencia pública ante el Poder Legislativo en la que participen empresas, academia y sociedad civil especializada.

- Generación de grupos asesores con participación de todos los actores, que funcionen de forma regular.

Finalmente, en tercer lugar, esta Agencia quisiera destacar como recomendación general la importancia de que en caso de generarse nuevos instrumentos regulatorios, estos contemplen un proceso de revisión y actualización periódicas, en función de los retos que vayan emergiendo.

Recomendaciones específicas

Se realiza una síntesis de recomendaciones en base a las orientaciones definidas y líneas temáticas abarcadas.

Institucionalidad y gobernanza de IA

Como se mencionó más arriba, éste es un aspecto central en muchos de los instrumentos internacionales, y existen varias fórmulas aplicadas en distintas jurisdicciones que procuran de una forma u otra, establecer una institucionalidad específica para la IA, ya sea apoyándose en institucionalidades preexistentes, o generando nuevas. Asimismo, la definición de la institucionalidad de la IA en el país impacta en los mecanismos de gobernanza de datos –los cuales deben ser establecidos- y por ende en el propio desarrollo de la IA.

El rol de Agesic en la institucionalidad de la IA

En lo que refiere al rol de Agesic, se propone evaluar la posibilidad de que las actuales capacidades de la Agencia sean potenciadas, instituyendo una nueva estructura interna que contemple la línea de Inteligencia Artificial y Datos, incluyendo los roles definidos en el inciso final del artículo 74 de la Ley N° 20.212.

De esta forma, se clarificaría la actual expansión de competencias de la Agencia más allá del diseño e implementación de la Estrategia Nacional de IA. Se estarían además aprovechando las potencialidades de Agesic, desde que actualmente son de su competencia aspectos de la gestión de los datos a la interna de las entidades públicas.

Podría resultar apropiado –aunque no estrictamente necesario- establecer una disposición normativa de rango legal en el que se le atribuyan a la Agencia competencias adicionales a las ya existentes –indicadas en el artículo 74 in fine y en el artículo 75 de la Ley N° 20.212-, incluyendo su rol en la coordinación con otras entidades a nivel nacional y la representación del país a nivel internacional en este tema. Más allá de lo dicho, debe recordarse que el liderazgo en materia de transformación y política digital de la Agencia resulta de varias disposiciones preexistentes que ya han sido reseñadas.

Sin perjuicio del liderazgo de Agesic en la materia, se observa que es necesaria la participación de otros actores dentro y fuera del sector público, de forma de colaborar en el diseño e implementación de políticas públicas integrales. Agesic cuenta desde sus inicios con un conjunto de Consejos Asesores y lidera distintos comités estratégicos.

En materia de estrategia de adopción de una política de inteligencia artificial y datos, se propone la institucionalización normativa del actual Comité Estratégico del Sector Público para la Inteligencia Artificial y Datos, que coordine con la Agencia no sólo el desarrollo de la Estrategia Nacional de IA y Datos sino también la planificación de los planes de acción que permitan su implementación.

Dentro de los roles fundamentales del Comité estaría la colaboración con Agesic en la elaboración de políticas generales en la materia, más allá de la actuación con otras entidades públicas competentes al elaborar políticas sectoriales. Serían en este modelo las entidades públicas sectoriales quienes deberán llevar adelante los procesos de elaboración de normativa y recomendaciones sectoriales, monitoreo y fiscalización del cumplimiento, alertando a Agesic y al Comité en caso de desviaciones.

Otro aspecto a considerar y que puede motivar una diferente integración del Comité es la definición de otros temas que surjan del proceso participativo de creación de las Estrategias Nacionales de IA y de Datos y que orienten la política pública en estos temas.

En función de lo establecido en el artículo 74 in fine de la Ley N° 20.212, los procesos de fiscalización sectoriales que correspondan a entidades públicas de contralor, contarán con la colaboración de Agesic –y eventualmente del Comité-, cuando se empleen sistemas de IA.

Más allá de integraciones puntuales, esta Agencia entiende que existen entidades que deben ser parte de esta institucionalidad (como por ejemplo la ANII, el MIEM, la URCDP, la INDDHH), de forma de cumplir con las orientaciones dadas por el Poder Legislativo en cuanto al desarrollo de una IA basado en la ética, que promueva la innovación y respete los derechos humanos.

Institucionalidad de la IA a la interna de las organizaciones

Se sugieren dos líneas de acción con respecto a la interna de las entidades públicas: i. una línea de capacitación y fortalecimiento en materia de IA y Datos, y, ii. una línea de fortalecimiento estructural para dotar a cada institución de capacidades que permitan la gestión, el monitoreo y el contralor de las políticas que se implementen, así como para llevar a cabo planes estratégicos y operativos alineados con dichas políticas.

Existen a la fecha un conjunto de figuras que obligatoriamente deben instituirse por las entidades públicas y que tienen relación con la gobernanza de los datos: la figura del delegado de protección de datos personales –instituida por el artículo 40 de la Ley N° 19.670, de 15 de octubre de 2019-, la figura del responsable de transparencia –instituida por los artículos 41 y 57 del decreto N° 232/010, de 2 de agosto de 2010, reglamentario de la Ley N° 18.381, de 17 de octubre de 2008- y la figura del responsable de seguridad de la información –instituida legalmente por el artículo 78 literal B de la Ley N° 20.212, de 6 de noviembre de 2023-.

La particularidad de las figuras del delegado de protección de datos y del responsable de seguridad de la información es que no sólo se extienden a entidades públicas sino también a algunas entidades privadas:

- en el caso de la primera de las figuras indicadas, se extiende a aquellas entidades privadas que tratan datos sensibles como negocio principal –siendo la definición de datos sensibles taxativa y dispuesta por el artículo 4° literal E de la Ley N° 18.331, de 11 de agosto de 2008- y las que traten grandes volúmenes de datos –definidos como datos de más de 35.000 personas por el artículo 10 literal c del decreto N° 64/020, de 17 de febrero de 2020-;
- en el caso de la segunda, refiere a entidades privadas vinculadas a servicios o sectores críticos del país –lo que depende de la definición dada por la reglamentación que a la fecha aún no ha sido dictada-.

A ello debe agregarse la necesidad de contar con referentes que implementen las políticas de datos abiertos en las entidades públicas, vinculadas al cumplimiento de lo dispuesto en el artículo 82 de la Ley N° 19.355, de 12 de diciembre de 2015.

Esta Agencia entiende que es posible la reconversión de las funciones de las figuras ya existentes, en especial la del delegado de protección de datos, mediante instancias de capacitación en IA y gobernanza de datos. Sí parece conveniente crear a la interna de las organizaciones públicas un Comité Interno de Datos que incluya la figura del delegado de protección de datos, el responsable de seguridad de la información, el responsable de transparencia y el referente de datos abiertos.

Perspectiva multisectorial y multidisciplinaria

Se ha mencionado en reiteradas oportunidades a lo largo de este informe, la necesidad de que la definición de las políticas tenga una perspectiva de múltiples actores que incluya a las entidades públicas, las privadas, la academia y la sociedad civil, teniendo en cuenta, además, los distintos sectores productivos. Asimismo, se ha planteado que los organismos cuenten con roles estratégicos en materia de IA y Datos que sean habilitadores para el desarrollo de las políticas en la materia y potencien las oportunidades que ambas temáticas brindan.

Para ello se propone basarse en institucionalidades ya existentes en Agesic, modificando las competencias del Consejo Asesor Honorario de la Sociedad de la Información, e incorporando eventualmente nuevos actores, en un esquema similar al existente actualmente en materia de Ciberseguridad. Adicionalmente, deberá contemplarse la multidisciplinariedad.

Existen actualmente en Agesic dos ámbitos vinculados a la IA que resulta conveniente mantener y fortalecer: 1) la Comunidad de IA en la Administración Pública[98], integrada por referentes técnicos de distintas entidades públicas; 2) el Observatorio de uso de IA en el Estado[99], creado como parte de un compromiso

[98] https://www.gub.uy/agencia-gobierno-electronico-sociedad-informacion-conocimiento/comunicacion/noticias/comunidad-inteligencia-artificial-administracion-publica. Últ. Acceso: 29/03/2023.

[99] https://www.gub.uy/agencia-gobierno-electronico-sociedad-informacion-conocimiento/comunicacion/publicaciones/observatorio-uso-inteligencia-artificial-estado. Últ. Acceso: 29/03/2024.

asumido en el 5° Plan de Acción de Gobierno Abierto. Ambos espacios habilitan la participación de distintos actores del ecosistema, con fines complementarios y de gran valor para el desarrollo de la IA, destacándose la participación de la sociedad civil y de técnicos especializados en la materia.

Gobernanza de datos

Finalmente, y en lo que respecta a la gobernanza de datos, debería seguirse avanzando en las obligaciones de las entidades públicas para la publicación de datos en forma segura –a través de la plataforma prevista por la reglamentación- y respetuosa de la protección de datos personales, avanzando más allá de la obligación establecida en el artículo 5° de la Ley N° 18.381, de 17 de octubre de 2008.

Debemos por otra parte seguir avanzando hacia un modelo de gobernanza de datos que de sostenibilidad a la política que se defina en la materia.

Asimismo, es importante continuar fomentando la obligatoriedad del intercambio de información –dentro del marco vigente- entre entidades públicas (artículo 157 y siguientes de la Ley N°18719), con el fin de promover la reutilización de datos, y avanzar en establecer los responsables sobre los datos maestros de Gobierno.

El uso de datos de entidades privadas puede marcar también un diferencial en la materia, para lo cual podrían promoverse medidas de incentivo en caso de que se decidan compartir datos –no necesariamente personales, pero sí útiles para la definición de políticas públicas-. Estas medidas de incentivo no están presentes en la normativa vigente, pero podrían incluir exoneraciones tributarias y mejoras en la provisión de servicios, adicionalmente a aspectos estrictamente reputacionales.

A nivel internacional el Reglamento (EU) 2023/2854 (Data Act)[100], establece determinados derechos a los usuarios de dispositivos para acceder y compartir sus datos, obligaciones de empresas privadas para compartir información en caso de que le sea requerido por entidades públicas y de cumplir requisitos mínimos que

[100] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32023R2854&qid=1704709568425. Últ. Acceso: 21/06/2024.

aseguren la interoperabilidad –en línea con la estrategia de estandarización para un mercado único, resiliente, verde y digital-, entre otros.

La regulación mencionada es además uno de los pilares de la estrategia europea de datos y de su política de transformación digital, y se complementa con el Reglamento (EU) 2022/868 (Data Governance Act)[101], que sienta las bases para los procesos de intercambio de datos y prevé conceptos interesantes como el de "altruismo de datos", que permite compartir información para objetivos de interés general, con las salvaguardas apropiadas.

En los aspectos de uso de datos a nivel de mercado deberá incluirse la perspectiva de la Unidad de Defensa del Consumidor y de la Comisión de Promoción y Defensa de la Competencia, ambas del Ministerio de Economía y Finanzas.

Respecto a datos personales y entrenamiento de sistemas, parece necesario discutir la actual regulación en materia de bases legítimas de tratamiento de datos personales. Así, el artículo 9° de la Ley N° 18.331, de 11 de agosto de 2008, omite la inclusión de bases de tratamiento que sí existen a nivel internacional, y las existentes pueden generar algunas dificultades interpretativas a la hora ser aplicadas para entrenar sistemas de IA. Si bien esta circunstancia no necesariamente impide el uso de los datos, la falta de una base de legitimación como el interés legítimo, agrega complejidad al tema y lleva a considerar si es posible la utilización de otras bases para estos fines.

Otros instrumentos como el sugerido por la INDDHH de fideicomisos de datos han comenzado a formar parte de la discusión. No obstante, el delicado equilibrio en el tratamiento de datos personales previsto en la Ley N° 18.331 motiva que esta discusión sea liderada por la Urcdp.

[101] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32022R0868, Últ. Acceso: 21/06/2024.

Resumen de recomendaciones asociadas a la institucionalidad y gobernanza	
Recomendaciones orientadas a eventuales modificaciones o actualizaciones normativas	- Crear Comités Internos de Datos en las entidades públicas, incluyendo a responsables de transparencia, delegados de protección de datos, responsables de información, y referentes de datos abiertos. - Promover el uso de datos abiertos e interoperables, considerando incluir nuevas obligaciones para las entidades públicas asociadas a la publicación de datos en formato abierto, estableciendo plazos y condiciones para dicha publicación
Otras iniciativas recomendadas	- Especificar las atribuciones a Agesic vinculadas al liderazgo en materia de IA y Datos - Crear una nueva institucionalidad dentro de Agesic a cargo de la política de IA y Datos. - Institucionalizar el Comité Estratégico del Sector Público para IA y Datos. - Reformular el Consejo Asesor Honorario de Sociedad de la Información para incorporar nuevos actores y funciones. - Definir un modelo de gobernanza de datos de gobierno. - Fortalecer la capacitación de las entidades públicas y dotarlas de las capacidades necesarias para asegurar que puedan llevar a cabo la implementación de políticas, estrategias y planes operativos en materia de IA y datos

	- Brindar capacitación en datos e IA a delegados de protección de datos y otras figuras relacionadas con la gestión de datos en las entidades públicas. - Promover incentivos para que entidades privadas compartan datos, respetando las normas en materia de protección de datos personales y propiedad intelectual, y a través de mecanismos seguros. - Promover la creación de bases de datos públicas que contengan información que contemple el idioma y la idiosincrasia local, y puedan servir como datos de entrenamiento para sistemas de IA. - Habilitar el empleo de la plataforma de interoperabilidad prevista en el decreto N° 178/013, de 11 de junio de 2013, por parte de entidades privadas.

Ética, Derechos Humanos y Democracia

El punto de partida para la protección de los derechos humanos

Uruguay mantiene un vínculo estrecho con el Sistema Interamericano y el Sistema Universal de protección de los derechos humanos, ha ratificado los tratados de derechos humanos emergentes de estos sistemas y participa activamente de sus instancias. Las recomendaciones que se formulan en este apartado parten de considerar el elenco de obligaciones (respetar, proteger y garantizar) que derivan para los Estados de la protección internacional de los derechos humanos.

En esta misma línea, la reciente Resolución sobre IA de la Asamblea General de Naciones Unidas, destaca “que se deben respetar, proteger y promover los derechos humanos y las libertades fundamentales durante todo el ciclo de vida de los sistemas de inteligencia artificial” y “exhorta a todos los Estados Miembros y, en su caso, a

otros interesados, a que se abstengan o dejen de usar sistemas de inteligencia artificial que sean imposibles de operar en consonancia con el derecho internacional o que supongan riesgos indebidos para el disfrute de los derechos humanos, en especial de quienes se encuentran en situaciones vulnerables, y reafirma que los derechos de las personas también deben estar protegidos en Internet, también durante el ciclo de vida de los sistemas de inteligencia artificial"[102].

La protección jurídica de los derechos humanos en nuestro país se afianza en la Constitución de la República, las normas del derecho internacional de los derechos humanos que han sido ratificadas, y un amplio y diverso conjunto de leyes que especifican la protección y regulan el ejercicio de ciertos derechos. No obstante, la protección jurídica de los derechos humanos en este campo se vería fortalecida con el desarrollo de normas que especifique la protección en este ámbito, en algunos casos.

Medidas especiales orientadas a la protección de los derechos humanos

En función de lo expuesto en el apartado anterior, y partiendo de lo que ya se ha avanzado a través de la Ley Nº 20.212, la primera recomendación apunta a ampliar la especificación de principios orientados a la Estrategia de IA que hace el artículo 74 de la citada norma, indicándolos como principios rectores de las políticas de IA y sus distintos instrumentos regulatorios.

Ahora bien, dichos principios pueden complementarse con medidas que los doten de contenido sustantivo y permitan llevarlos a la práctica, tomando como base los artículos 6° a 12° de la Ley N° 18.331, que no sólo enumeran el alcance de los principios, sino que también determinan ciertas acciones que deben ser llevadas adelante en la práctica por los responsables y encargados de tratamiento de datos personales.

Complementariamente, y a partir de la orientación que se desprende del propio artículo 74 de la Ley Nº 20.212, deben abordarse los actuales y potenciales riesgos e impactos adversos sobre los derechos humanos implicados en el ciclo de vida de

[102] https://documents.un.org/doc/undoc/gen/n24/087/86/pdf/n2408786.pdf?token=ZTiBbJsISYXoE5uIOW&fe=true

los sistemas de IA, en el sector público y privado, a través de la regulación y otras medidas.

En función de la necesidad de abordar los mencionados riesgos e impactos, se sugiere valorar adoptar un enfoque basado en el riesgo con el fin de:

1. Analizar y definir las aplicaciones de los sistemas de IA que resultan inaceptables como sociedad por su impacto sobre los derechos de las personas, evaluando las prohibiciones o moratorias que resulten adecuadas y consistentes con la obligación de proteger los derechos humanos; y,

2. Identificar y definir aquellas aplicaciones de la IA que representan un riesgo alto para los derechos de las personas en función del contexto y el uso previsto, la gravedad y probabilidad de los posibles impactos, con el fin de definir las medidas específicas que resulten aplicables.

A efectos de abordar los riesgos se han venido desarrollando distintos modelos y enfoque a nivel comparado. Por ejemplo:

- El Reglamento de IA de la Unión Europea establece un conjunto de aplicaciones prohibidas (Título II del Reglamento) entre las que se cuentan la manipulación cognitiva del comportamiento de personas que afecte la autonomía y capacidad de elegir libremente, los sistemas de categorización biométrica basados en datos biométricos, y los usos de sistemas de IA para la identificación biométrica remota en tiempo real de personas físicas en espacios de acceso público con fines de aplicación de la ley, estableciendo excepciones.

- La Orden Ejecutiva adoptada en 2023 por el Gobierno de Estados Unidos ordena a las entidades gubernamentales de acuerdo con sus respectivas competencias la adopción de diferentes medidas que apuntan a contar con directrices y estándares para el desarrollo e implementación responsable de la IA según su área de actividad y dispone un conjunto de obligaciones orientadas a brindar información a distintas agencias nacionales por parte de las empresas que desarrollen determinados modelos de IA.

- Asimismo, el artículo 16 del Convenio Marco adoptado en marzo por el Consejo de Europa, establece que cada Parte evaluará la necesidad de una moratoria o prohibición u otras medidas apropiadas con respecto a determinados usos de los sistemas de IA cuando considere que dichos usos son incompatibles con el respeto de los derechos humanos, el funcionamiento de la democracia o el Estado de Derecho.

Así, se sugiere valorar, para determinados tipos de riesgos que requieran de medidas especiales:

1. Establecer en forma obligatoria y ex ante una evaluación de impacto en los derechos humanos;

2. Establecer el deber de inscripción del sistema en un Registro estatal de acceso público a cargo de la entidad que lidere la política de IA en el país;

3. El sometimiento de los sistemas a un proceso de autorización o certificación previa según la finalidad o el tipo de sistema de que se trate;

4. Prever mecanismos de auditoría periódica de los sistemas y eventual remisión de resultados a la entidad a cargo de su revisión;

5. Complementar las normas que garantizan la transparencia y explicabilidad de los sistemas de IA que se utilizan para tomar decisiones o para apoyar la toma de decisiones, y la supervisión humana relacionada con el funcionamiento y resultados de dichos sistemas.

Por otra parte, tal y como ha subrayado el informe preliminar del Órgano Asesor de Alto Nivel sobre IA de la ONU, la IA encierra importantes oportunidades para la humanidad y la realización de los derechos de las personas a través del potencial implicado para mejorar la prestación de servicios públicos, facilitar el acceso al conocimiento, a la educación, la atención sanitaria, el desarrollo productivo, la agricultura, etc.

En consecuencia, junto con abordar los riesgos se recomienda considerar la promoción del desarrollo de sistemas de IA que tengan por finalidad el bien común

a través de la determinación de fines que se entiendan cumplen con dicho propósito, definiendo además apoyos y medidas de promoción, entre otros.

Implementación de derechos

Desde la perspectiva de las personas, se sugiere considerar la implementación a través de disposiciones legales, de determinados derechos como:

1. El derecho a saber que se está interactuando con un sistema de IA;
2. El derecho a obtener información básica del funcionamiento del sistema y los resultados esperados, a través de una persona física en caso de ser necesario y;
3. Eventualmente, el derecho de recurrir cuando se adopte una decisión en base a ese sistema, complementando el derecho de impugnación de valoraciones personales y el derecho de información previstos en la Ley Nº 18.331 de protección de datos personales.

Igualdad y no discriminación

La actual Estrategia Nacional de Ciudadanía Digital[103] señala que los "impactos que pueden surgir en el contexto de desarrollo de tecnologías disruptivas como la inteligencia artificial (IA) van más allá de lo individual, abarcando efectos colectivos y sociales. Es decir, se puede hablar de impactos sistémicos de muchas de estas tecnologías digitales. Por ejemplo, los vinculados a sus efectos en el futuro de los trabajos y la democracia como elementos claves".

En el trabajo de investigación "Construyendo ciudadanía en entornos digitales. Perspectivas transversales de abordaje[104]", siguiendo el documento de CEPAL "Ciudadanía digital en América Latina. Revisión conceptual de iniciativas", se

[103] https://www.gub.uy/agencia-gobierno-electronico-sociedad-informacion-conocimiento/comunicacion/publicaciones/estrategia-nacional-ciudadania-digital-para-sociedad-informacion. Últ. Acceso: 20/06/2024.

[104] https://www.gub.uy/agencia-gobierno-electronico-sociedad-informacion-conocimiento/comunicacion/publicaciones/construyendo-ciudadania-entornos-digitales-perspectivas-transversales-3. Últ. Acceso: 20/04/2024.

plantea que el concepto de brecha digital hoy en día se asocia a brechas en los usos y beneficios de las tecnologías digitales (derivados de diferencias en el nivel socioeconómico, la edad, el género, el capital cultural y las habilidades digitales).

Se afirma en dicho trabajo la necesidad de incorporar una perspectiva de inclusión o igualdad digital, y de desarrollar las habilidades necesarias para superar las limitaciones de acceso y capacidades, así como para comprender las reglas del juego y reflexionar sobre nuestros propios comportamientos.

Las medidas que se adopten en función de las recomendaciones de este documentos deberían integrar un enfoque que tenga en cuenta especialmente la mayor vulnerabilidad que enfrentan diversos grupos de la sociedad, adoptando marcos y políticas para abordar los sesgos que puedan profundizar las desigualdades, y proteger a las personas frente a todas las formas de discriminación y velar para que los resultados discriminatorios no se trasladen a los sistemas de IA, y en su caso se detecten y se corrijan.

Enfrentar los retos para las democracias

A nivel global resulta cada vez mayor la preocupación por los impactos de la desinformación y la protección de la integridad de los procesos democráticos y la capacidad de las personas de formar su opinión libremente.

En este sentido, por ejemplo, al analizar los impactos y riesgos implicados en la Inteligencia Artificial, el informe provisional del Órgano Asesor de Alto Nivel en IA de la ONU[105] analiza que algunos riesgos de la IA se originan en las limitaciones técnicas de estos sistemas como en el caso de los sesgos dañinos o las llamadas alucinaciones en la IA generativa, en tanto otros, son producto del uso humano, como las deep fakes, las que “pueden plantear grave riesgo para la confianza social y el debate democrático”.

La Resolución AG/RES. 3004 (LIII-O/23) sobre “Fortalecimiento de la Democracia”[106] aprobada en la cuarta sesión plenaria de 23 de junio de 2023 de la

[105] https://www.un.org/sites/un2.un.org/files/ai_advisory_body_interim_report.pdf. Últ. Acceso: 20/06/2024.

[106] https://scm.oas.org/doc_public/SPANISH/HIST_23/AG08884S03.docx. Últ. Acceso: 20/06/2024.

Organización de Estado Americanos (OEA) resolvió encargar a la Secretaría General el desarrollo de una agenda interamericana respecto a tecnologías emergentes, particularmente en lo relativo al uso ético de políticas de IA, algoritmos y gobernanza de datos, ello en el marco de un conjunto de medidas destinadas precisamente al fortalecimiento democrático.

La preocupación internacional frente a los desafíos mencionados quedó reflejada en la última actualización de los Principios sobre IA de la OCDE realizada en 2024 en la que uno de los objetivos fue precisamente reflejar la creciente importancia de abordar estos fenómenos en el contexto de la IA generativa. En este sentido los principios plantean "abordar la desinformación amplificada por la IA, respetando al mismo tiempo la libertad de expresión y otros derechos y libertades protegidos por el derecho internacional aplicable"[107].

Mientras continúan los esfuerzos globales por comprender este fenómeno y su abordaje, es necesario pensar medidas no sólo limitativas –necesarias sin duda- sino también de alfabetización digital e informacional, generando habilidades instrumentales y fundamentales para la interacción crítica de las personas en el entorno digital.

Como parte de estas medidas, pueden promoverse mecanismos para identificar la manipulación de información y los contenidos generados por IA, y las políticas para robustecer las habilidades digitales de las personas –en este último caso apoyadas en nuestro país en la Estrategia Nacional de Ciudadanía Digital -.

Mecanismos y recursos accesibles, adecuados y efectivos

Existen en nuestro ordenamiento jurídico distintas entidades públicas con competencias en materia de derechos humanos fuera del ámbito del sistema de justicia, como la Institución Nacional de Derechos Humanos y Defensoría del Pueblo, la Unidad Reguladora y de Control de Datos Personales, y la Unidad de Acceso a la Información Pública, entre otras.

[107] https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0449#mainText. Últ. Acceso: 20/06/2024.

Con el fin de garantizar que las eventuales vulneraciones de los derechos humanos resultantes de uso de la IA se atiendan mediante mecanismos y recursos accesibles, adecuados y efectivos, se sugiere realizar un análisis de los mecanismos actuales con el fin de identificar si existe la necesidad de fortalecer las competencias específicas de los organismos existentes o de crear nuevos mecanismos que sean necesarios, así como la articulación de sus competencias.

Regulación del desarrollo, uso y adquisición de IA en el sector público

La Carta Iberoamericana de Inteligencia Artificial en la Administración Pública adoptada en 2023 en el ámbito del CLAD, tiene "como objetivo principal promover un modelo compartido de desarrollo de la Inteligencia Artificial desde y en las administraciones públicas del ámbito iberoamericano[108]". Como base para este marco común, el capítulo 3 plantea un conjunto de principios generales de la IA en la Administración Pública: autonomía humana; transparencia, trazabilidad y explicabilidad; rendición de cuentas, responsabilidad y auditabilidad; seguridad y robustez técnica; fiabilidad, precisión y reproductibilidad; confianza, proporcionalidad y prevención del daño; privacidad y protección de los datos personales; calidad e integridad de los datos; equidad, inclusión y no-discriminación; centralidad de las personas, valor público y responsabilidad social; y sostenibilidad y protección ambiental.

Al identificar las dimensiones clave para la adopción de la IA en la Administración Pública, la Carta plantea como componente de las estrategias nacionales que: "las legislaciones nacionales deberían atender cuestiones que logren que los sistemas algorítmicos sean seguros, transparentes, trazables, no discriminatorios y sostenibles ambientalmente. También se debería adaptar la normativa de protección de los datos personales, así como del uso y reutilización de los datos públicos en general. Adicionalmente, se debe garantizar que los sistemas de Inteligencia Artificial sean supervisados por humanos, en lugar de ser completamente autónomos, minimizando los potenciales daños y eliminando situaciones de riesgo extremo. Junto a ello se deben establecer mecanismos robustos de ciberseguridad para mantener la integridad de los datos y la

[108] https://clad.org/wp-content/uploads/2023/10/Borrador-CIIA-V1-ES-08-2023.pdf. Últ. Acceso: 20/05/2024.

inviolabilidad de las infraestructuras tecnológicas. Finalmente, habría que garantizar que los algoritmos públicos sean transparentes y no privativos o sometidos a patentes, promoviendo infraestructuras tecnológicas basadas en arquitecturas abiertas".

Se trata de principios compartidos con la Estrategia de IA actualmente en proceso de revisión, en la que se subraya además que "toda solución tecnológica que utilice IA debe respetar los Derechos Humanos, las libertades individuales y la diversidad".

En función del camino que Uruguay ya ha venido recorriendo en el marco de su política digital nacional centrada en las personas por definición, se recomienda continuar fortaleciendo los instrumentos regulatorios referentes al ámbito público, integrando aquellos componentes de la nueva Estrategia de IA que se adopte en 2024 relativos al uso y desarrollo de estas tecnologías específicamente en dicho ámbito.

En tal sentido, una medida puntual a considerar es la realización de evaluaciones de impacto en los derechos humanos como requisito para la adquisición, desarrollo y/o uso de los sistemas de IA por parte de las entidades públicas en áreas en que se determine que pueda existir un riesgo alto para los derechos de las personas; En función de lo ya expresado, y en particular, se recomienda analizar como parte del paquete de medidas a evaluar, la regulación del desarrollo, adquisición y aplicación de sistemas de vigilancia con fines de seguridad pública.

Adicionalmente, y atento a que se encuentra en curso la elaboración de las estrategias de Datos y Ciberseguridad, también será relevante considerar los lineamientos que allí se definan para identificar los elementos que requieran una regulación legal que complemente los marcos generales pre-existentes.

Capacitación y educación para la IA

Como se mencionó oportunamente al considerar la línea temática de trabajo y capacitación para IA, en este informe se identifican medidas concretas orientadas específicamente a la formación de las personas y al fortalecimiento de sus habilidades.

Otros aspectos vinculados al impacto de la IA en el mundo del trabajo requerirán desarrollos más abarcativos y una discusión abierta con la participación del Estado, empleadores, trabajadores y sindicatos, de forma de obtener acuerdos que potencien los beneficios de la aplicación de esta tecnología y mitiguen efectos adversos.

No obstante, desde la óptica de este informe, pueden realizarse las siguientes recomendaciones, sugiriéndose:

1. la promoción de programas de capacitación a través de entidades de la enseñanza técnica, terciaria y universitaria en temas de IA y gestión de datos, en colaboración con cámaras empresariales, sindicatos, y otras agrupaciones;

2. establecer apoyos específicos o beneficios particulares para las empresas que realicen cursos orientados a la IA para sus trabajadores y cuerpos gerenciales, en sectores predefinidos;

3. evaluar la obligación de que los empleadores capaciten a los trabajadores que deban aplicar o que puedan verse afectados por sistemas de IA, previo a su instrumentación, en sectores predefinidos.

Resumen de recomendaciones en ética, derechos humanos y democracia	
Recomendaciones orientadas a eventuales modificaciones o actualizaciones normativas	- Explicitar los principios enumerados en el artículo 74 de la Ley 20.2012 como principios rectores de la política nacional de IA y para su implementación. - Definir riesgos que resulten inaceptables como sociedad; e identificar los usos que representen un alto riesgo y requieran medidas

	especiales, definiendo también dichas medidas. - Evaluar la adopción de medidas orientadas a combatir la desinformación y proteger la integridad de los procesos democráticos y la capacidad de las personas de formar su opinión libremente. - Analizar el fortalecimiento de los mecanismos existentes o la creación de nuevos mecanismos para resolver vulneraciones de los derechos humanos resultantes de sistemas de IA. - Regular derechos instrumentales en pro de la transparencia, la explicabilidad y la impugnabilidad.
Otras iniciativas recomendadas	- Establecer normas específicas con respecto al desarrollo, uso y adquisición de la IA en el Sector público. - Evaluar los instrumentos regionales e internacionales de cooperación en la materia. - Analizar la adopción de medidas con el fin de continuar abordando las brechas digitales y fortalecer el desarrollo de ciudadanía digital.

	- Promover iniciativas de uso de IA para el bien de la sociedad. - Promover la capacitación especialmente de trabajadores en colaboración con cámaras empresariales, sindicatos, y otras agrupaciones, y establecer apoyos específicos o beneficios particulares para las empresas que realicen cursos orientados a la IA, en sectores predefinidos. - Evaluar la obligación de que los empleadores capaciten a los trabajadores que deban aplicar o que puedan verse afectados por sistemas de IA, previo a su instrumentación, en sectores predefinidos.

Innovación responsable

Seguridad jurídica en los aspectos de la responsabilidad civil y la Propiedad Intelectual

De los análisis realizados surge la necesidad de revisar el régimen nacional de responsabilidad civil, en tanto no parece razonable acudir a interpretaciones o integraciones de normas que no se compadecen con la realidad actual, para dar así mayores certezas a desarrolladores, usuarios y otros actores del sistema.

Se sugiere considerar las siguientes alternativas: i. determinar con entidades competentes sugerencias de contenidos mínimos en contratos que se suscriban entre quienes ponen a disposición sistemas y quienes los emplean. En ese sentido, podrán considerarse como antecedentes las normas en materia de responsabilidad proactiva de la protección de datos personales; ii. establecer una comisión de

análisis que específicamente se centre en una eventual reforma del régimen de responsabilidad civil en la materia.

La seguridad jurídica se asocia además a un adecuado sistema de atribución de derechos en caso de creaciones en las cuales se encuentre implicado, en alguna forma, un sistema de IA.

Esta Agencia sugiere:

1. Incluir en el caso de obras generadas por IA sin intervención humana directa, una indicación de esta circunstancia en la propia obra, y en algunos casos la referencia al sistema empleado para la creación de la obra. Podrían plantearse excepciones vinculadas al uso doméstico, o para otros fines;

2. Iniciar un proceso de consulta acerca de cómo se considerarán las obras generadas exclusivamente por IA. No existe actualmente una consolidación de la opinión de que dichas obras puedan atribuirse a estos sistemas por lo que la consulta debería realizarse con todos los actores involucrados; teniendo en cuenta no sólo aspectos asociados a la atribución de la titularidad sino también de las compensaciones económicas que correspondan;

3. Considerar una definición acerca del sistema a aplicar para las obras asistidas por IA, como por ejemplo atribuyéndolo a quien dirige el proceso creativo de la obra finalizada[109];

4. Reafirmar que los alcances para el tratamiento de los datos empleados por estos sistemas para la generación de nuevas obras, dependerá de la normativa vigente -artículo 35 de la Ley N° 9.376, y el artículo 9° bis de la Ley N° 18.331-.

En otros aspectos vinculados con la propiedad intelectual, se sugiere considerar que:

[109] Pueden verse distintas alternativas al respecto en MANTEGNA. Op. Cit. Pág. 309.

1. En lo que respecta a la inscripción registral, continuar con el proceso ya iniciado por la Ley N° 20.212, y evaluar la posibilidad de que exista comunicación entre este registro, otros registros, y la publicación de software público indicada en el artículo 7° del decreto N° 44/015 en el caso de las entidades públicas;

2. Ampliar el alcance del artículo 2° de la Ley N° 19.179, a los programas de ordenador (programas fuente o programas objeto), compilaciones de datos o de otros materiales, en cualquier forma, que por razones de la selección o disposición de sus contenidos constituyan creaciones de carácter intelectual, y la expresión de ideas, informaciones y algoritmos, formulada en secuencias originales ordenadas de forma apropiada para ser usada por un dispositivo de procesamiento de información o de control automático.

Infraestructura y ciberseguridad

En este informe ya se ha planteado la necesidad de contar con una adecuada infraestructura para el desarrollo de la IA, y el rol relevante del Estado para alcanzar ese objetivo.

Siguiendo el informe de la OCDE relevado al analizar esta línea, parece necesario adoptar un conjunto de medidas asociadas a la revisión de las capacidades computacionales en los sectores público y privado, considerar el número, capacidad y disponibilidad de centros de datos existentes, definir estándares en materia de gestión de datos, analizar las capacidades de procesamiento y necesidades de hardware en el país, determinar la demanda potencial de procesamiento para IA, distinguir las necesidades de procesamiento para IA, proveer capacitación y entrenamiento, mapear y analizar las cadenas de suministro.

Se considera necesario generar o actualizar instrumentos normativos que faciliten la adquisición, operación y mantenimiento de estas infraestructuras de forma de impulsar una gestión de la capacidad que se adecue rápidamente al avance exponencial que muestra esta tecnología en particular.

A los efectos de este informe, cuyo objetivo es brindar recomendaciones al Poder Legislativo, los análisis realizados deben además encontrarse orientados a la determinación de si las disposiciones normativas vigentes están alineadas a las necesidades en la materia.

Desde esa perspectiva, esta Agencia quiere resaltar que existe una legislación y reglamentación profusa en aspectos tales como el intercambio de datos, la ciberseguridad, el tratamiento de información –personal y no personal-, las redes de telecomunicaciones, las adquisiciones en el ámbito público, entre otras. Puede reconocerse sí, la dificultad que plantea la dispersión normativa existente, por lo que podría resultar relevante la organización de las normas mencionadas a través de un texto ordenado o instrumentos similares.

La ciberseguridad en particular ha sido objeto de regulación desde la creación de Agesic, y recientemente ha sido resaltada su relevancia con la sistematización de distintas disposiciones y la actualización de las competencias de la Agencia y de las obligaciones de entidades públicas en general y algunas privadas en particular, en varios artículos de la Ley N° 20.212.

Los resultados del proceso de construcción de la Estrategia Nacional de Ciberseguridad, y los objetivos estratégicos que resulten de ese proceso –como ya fue mencionado en reiteradas oportunidades en el presente informe- serán un insumo central para la determinación de nuevas medidas que colaboren a un ecosistema seguro para el desarrollo de la IA y de otras tecnologías.

En materia de infraestructura, y considerando los aportes recibidos a lo largo del proceso de elaboración de este informe, Agesic propone promover un diálogo con otros actores en este aspecto, para lo que se sugiere como alternativas:

1. Agregar como cometido específico del Consejo Asesor de Informática Pública el de colaborar en la definición de recomendaciones;

2. Articular acciones con el Comité de Gobernanza de Procesos y Soluciones Transversales creado por decreto N° 431/022, de 27 de diciembre de 2022,

3. Definir junto con la Agencia Reguladora de Compras Estatales (ARCE) requisitos específicos para contrataciones asociadas al desarrollo de sistemas de IA.

En particular en aspectos de sustento normativo para el intercambio de datos en forma segura, resulta recomendable habilitar el uso de la Plataforma de Interoperabilidad creada por el decreto N° 178/013 para el consumo de servicios por parte de entidades privadas y evaluar la modificación del decreto N° 92/014, para clarificar normativamente los supuestos asociados al uso de servicios de proveedores de nube.

Una perspectiva integral de la infraestructura y los procesos para la transformación digital

Es necesario trabajar en una perspectiva integral, repensando la forma en que se plantea el uso de la infraestructura y los procesos del Estado, facilitando el despliegue de tecnología como la IA.

En tal sentido, se debería apuntar a promover el aprovechamiento de la IA como una oportunidad para la mejora de los servicios públicos, la eficiencia del Estado y la toma de decisiones basadas en datos.

Propuestas como la Infraestructura Pública Digital (DPI por sus siglas en inglés) permiten un enfoque integral con el fin de llevar adelante procesos de transformación digital más eficientes. Recientemente se lanzó la iniciativa denominada “Salvaguardias de la DPI”. Esta iniciativa tiene por objetivo compartir lecciones aprendidas, creando un marco para minimizar riesgos a nivel técnico, normativo y organizativo, y en definitiva un entorno para una implementación segura, inclusiva, práctica y adaptable de la DPI[110].

En esta perspectiva, la mejora en la infraestructura del Estado, que soporta tecnología como la IA, debe redundar en un beneficio para la innovación y la

[110] Puede accederse al reporte provisional de la iniciativa en: https://safedpi.gitbook.io/safeguards/working-group-documents/reports. Últ. Acceso: 22/06/2024.

investigación en el sector público y en el sector privado, contribuyendo al desarrollo económico y social del país.

En esta lógica debería tenderse a que los componentes de la infraestructura, cuando corresponda, puedan ser aprovechados por actores del ecosistema innovador, científico y emprendedor, considerando especialmente las distintas características de dichos actores.

Impactos medioambientales de la infraestructura

Sin perjuicio de que el aspecto medioambiental no fue parte de las líneas temáticas centrales del presente informe, resulta ineludible realizar alguna referencia a los impactos que el desarrollo acelerado de la tecnología en general y de la IA en particular posee para el medio ambiente.

El uso de la IA puede generar grandes beneficios para mitigar los impactos del cambio climático, y en los hechos, distintas iniciativas incluso a nivel nacional promueven desarrollos que ataquen este problema[111].

Sin embargo, existen aspectos de impacto negativo vinculados a la extracción de materiales para la creación de componentes de hardware, el uso del agua, el consumo de energía, entre otros, lo que hace necesario traer a las autoridades y actores relevantes a esta discusión.

La recomendación sobre la ética de la IA de UNESCO señala claramente la necesidad de que todos quienes participen en el ciclo de vida de los sistemas de IA respeten las normas y prácticas nacionales e internacionales vinculadas a la precaución, concebidas para la protección y restauración del medio ambiente y los ecosistemas, y para el desarrollo sostenible.

CLAD incluye dentro de los principios de su carta el de sostenibilidad y protección ambiental, defendiendo el uso de tecnologías ambientalmente sostenibles y energéticamente no contaminantes, fundadas en la aplicación de materiales y

[111] Ver a modo de ejemplo: https://www.anii.org.uy/apoyos/innovacion/309/fondo-de-investigacion-e-innovacion-en-cambio-climatico/. Últ. Acceso: 20/06/2024.

dispositivos reutilizables y fuentes de energía renovables, todo en línea con los ODS.

Atento a lo señalado, la perspectiva ambiental debe encontrarse presente en toda iniciativa asociada al desarrollo de infraestructura para la IA.

Medidas de promoción

Las medidas de promoción son múltiples y deberían enfocarse no en la promoción de la tecnología, sino en objetivos a alcanzarse a través de ésta. Se mencionaron en el análisis realizado algunas medidas que se desprenden de normas vigentes, y las entidades a cargo de llevarlas adelante.

En enero de este año, la Comisión Europea lanzó un paquete de medidas de apoyo a startups europeas y pequeñas y medianas empresas para el desarrollo de IA segura. Dentro del paquete mencionado se encuentra la instalación de fábricas de IA con supercomputadoras accesibles para PYMES, apoyo en el uso de modelos de IA para propósitos generales, la creación de una oficina de IA dentro de la Comisión, apoyo financiero a través de distintos programas y el desarrollo de espacios de datos, entre otros.

Del proceso de construcción de las estrategias lideradas por esta Agencia, surge en forma reiterada la necesidad de que el desarrollo de infraestructura contemple instrumentos como beneficios arancelarios, exoneraciones impositivas e incentivos para la importación de componentes y exportación de servicios desde nuestro país, entre otros.

Algunas medidas de promoción, como incentivos, exoneraciones, y otros beneficios que hoy ya existen en normas vigentes pueden orientarse o reorientarse al fomento de actividades que, gracias a la IA, puedan redundar en un beneficio para la economía, la sociedad, y, en definitiva, las personas.

En materia de apoyo a la IA en el Sector Público, ya en el 2021 el Banco Mundial[112] sugería la instalación de un hub central de innovación para IA en el gobierno,

[112] https://documents1.worldbank.org/curated/en/746721616045333426/pdf/Artificial-Intelligence-in-the-Public-Sector-Summary-Note.pdf. Últ. Acceso: 21/06/2024.

similar al programa de UIH con el que actualmente cuenta nuestro país. En dicho documento, el Banco Mundial señala que las inversiones deben dirigirse hacia el capital humano y la infraestructura digital, priorizando la investigación, el emprendedurismo, las tecnologías digitales fundacionales y las habilidades digitales.

Los objetivos que se tracen al respecto están vinculados entre otros y a criterio de esta Agencia, a los objetivos ya definidos en la Agenda Digital Uruguay 2025 y a los que resulten del proceso de construcción de las estrategias nacionales de Datos y Ciberseguridad, y de la actualización de la Estrategia Nacional de Inteligencia Artificial.

Más allá de las alternativas de apoyos financieros sostenidos en normas vigentes, existen otro tipo de medidas que promueven el uso responsable de la IA, entre las que encontramos los sandboxes regulatorios y los espacios de datos, instrumentos que posibilitan la experimentación segura, un marco de responsabilidad acotado, y la colaboración de múltiples partes (sector público, privado, academia y sociedad civil).

Por su parte, debe continuarse el camino de la cooperación internacional en la materia, así como la suscripción de acuerdos que habiliten un mejor posicionamiento del país en cuanto a innovación e investigación segura en IA, como ocurre con la suscripción del reciente Tratado de Cooperación en materia de Patentes.

Resumen de recomendaciones en materia de fomento a la innovación en IA	
Recomendaciones orientadas a eventuales modificaciones o actualizaciones normativas	- Impulsar la extensión del cometido previsto en el artículo 74 de la Ley N° 19.149, de 24 de octubre de 2013 a toda la Administración.

	- Ampliar el alcance del artículo 2° de la Ley N° 19.179, de 27 de diciembre de 2013.
Otras iniciativas recomendadas	- Establecer una comisión interdisciplinaria de análisis para una eventual reforma del régimen de responsabilidad civil en la materia. - Analizar junto con los organismos competentes propuestas de contenidos mínimos de alcance de la responsabilidad en los contratos que se suscriban entre desarrolladores, usuarios y otros actores de sistemas de IA. - En materia de Propiedad Intelectual, promover una discusión sobre las alternativas para la generación de obras por IA sin intervención humana directa y para las obras asistidas por IA. - Continuar con el proceso de inscripción iniciado por la Ley N° 20.212, de 6 de noviembre de 2023, y evaluar la comunicación entre este registro, otros registros, y la publicación de software público. - Evaluar incluir como cometido específico del Consejo Asesor de Informática Pública el de colaborar con Agesic en la definición de las recomendaciones necesarias para el desarrollo adecuado de la infraestructura para IA a nivel país.

	- Considerar la elaboración de un análisis vinculado a la infraestructura actual e integral en la materia, que considere especialmente medidas de la inversión pública y de promoción de la inversión privada. - Evaluar la definición de una nueva política de uso de nube sobre la determinada en el decreto N° 92/014, de 7 de abril de 2014. - Establecer la colaboración entre entidades a cargo de la promoción de iniciativas en materia de infraestructura de IA, incluyendo en especial la perspectiva medioambiental. - Consolidar las herramientas necesarias para llevar adelante las acciones que se definan en la Estrategia Nacional de Ciberseguridad. - Finalizar la propuesta de reglamentación de los entornos controlados de prueba y otras medidas de promoción de la innovación, y realizar su implementación. - Evaluar junto al MEF, el MIEM, la ANII y otras entidades públicas competentes la determinación de las medidas de apoyo necesarias.

Anexo 1: Antecedentes nacionales

Mapeo de la normativa nacional

Para la elaboración del presente informe, se tuvo en cuenta la existencia de un conjunto de disposiciones de rango legal y reglamentario, que pretendió enfocarse estrictamente a aspectos vinculados a las líneas temáticas definidas y su vínculo con la IA.

A continuación, se presenta una tabla con las disposiciones identificadas, distinguidas según la línea temática asociada y una breve descripción de cada una de ellas.

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	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.

20 de octubre de 2022.	

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. Reglamentados por decretos N° 414/009, de 31 de agosto de 2009, y 64/020, de 17 de febrero de 2020.	Datos Personales	Se establecen las formas de tratamiento de los datos personales en el sector público y privado, asociados a un conjunto de principios.
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,	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

de 27 de diciembre de 2010		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.
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	Interoperabilidad e intercambio	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.
Decreto N° 357/016, de 7 de noviembre de 2016	Datos Abiertos y Gobierno Abierto	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.

Aplicación de principios en IA

Normas	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. El artículo en su inciso segundo establece que “(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”.
Artículo 5° Ley N° 18.331, de 11 de agosto de 2008.	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, 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.
Ley N° 19.179, de 27 de diciembre de 2013. Reglamentado por decreto N° 44/015,	Regula el formato para el procesamiento y almacenamiento de información digital en determinadas entidades públicas y privadas.

de 30 de enero de 2015.	

Infraestructura y Ciberseguridad

Normas aplicables	Resumen de contenido
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.	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.
Ley N° 18.331, de 11 de agosto de 2008. Reglamentada por decretos N° 414/009, de 31 de agosto de 2009 y	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 2020, en particular recomienda la adopción de determinadas medidas de seguridad en sus artículos 3° y

64/020, de 17 de febrero de 2020.	4°, sugiriendo expresamente la adopción del Marco de Ciberseguridad de Agesic.
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.	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.
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.	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.
Decreto 92/014, de 7 de abril de 2014	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.
Ley N° 19.924, de 18 de diciembre de 2020, artículos 372	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

a 375 que 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.	para el Desarrollo de la Ciencia y el Conocimiento, que 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.
Ley N° 20.075, de 20 de octubre de 2022 artículo 461, reglamentado por decreto N° 216/023, de 17 de julio de 2023	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 Uruguay Innovation Hub, 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.
Ley N° 20.212, de 6 de noviembre de 2023, artículos 78 a 84.	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

	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. Reglamentada por decreto N° 308/021, de 10 de setiembre de 2021.	Se establecen políticas de empleo para favorecer la actividad laboral remunerada de jóvenes, mayores de edad 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 aplicables	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.
Artículo 461 de la Ley N° 20.075, de 20 de octubre de 2022	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.
Decreto N° 216/023, de 17 de julio de 2023	Se crea el Programa Uruguay Innovation Hub para promover el ecosistema emprendedor e innovador.
Ley N° 20.121, de 23 de agosto de 2023. Reglamentada por decreto N° 360/023, de 14 de noviembre de 2023.	Ley vinculada al fomento para la radicación en Uruguay, de técnicos y profesionales del sector de las tecnologías de la información

Artículo 75 Ley N° 20.212, de 6 de noviembre de 2023	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.

Anexo 2: Antecedentes internacionales

Principios y recomendaciones internacionales

La atención sobre los sistemas de inteligencia artificial se ha vuelto omnipresente en la agenda de los organismos y foros internacionales, abarcando las más diversas temáticas y áreas: desde cómo la Inteligencia Artificial puede ayudar a alcanzar los Objetivos del Desarrollo Sostenible, hasta los debates en torno a su aplicación en el ámbito militar.

En medio de esta diversidad, sin embargo, es posible identificar un punto de partida en común en varios de los esfuerzos internacionales concretados o en curso orientados a la gobernanza de la inteligencia artificial: y es el énfasis en la necesidad de construir una gobernanza orientada a potenciar las oportunidades y beneficios implicados en la inteligencia artificial para la humanidad asegurando el acceso equitativo a estos beneficios, y a abordar al mismo tiempo, los desafíos y riesgos derivados de estas tecnologías.

Para ello, como se desprende de los antecedentes que se reseñan a continuación, buena parte de los esfuerzos en curso enfatizan la necesidad de adoptar un enfoque que: coloque a las personas en el centro; proteja los derechos humanos, la democracia y el Estado de Derecho; se asiente en el derecho internacional y el derecho internacional de los derechos humanos; promueva que los sistemas de inteligencia artificial sean seguros y fiables y se desarrollen y utilicen de manera ética; y promuevan la innovación para aprovechar el potencial de la IA en beneficio de la humanidad y el desarrollo sostenible.

El objetivo de este anexo del Informe es presentar una síntesis de los principios rectores y recomendaciones que buscan orientar las acciones de los Estados en la formulación de su legislación, políticas u otros instrumentos relacionados con la IA emergentes del ámbito internacional, en función de la revisión de antecedentes internacionales realizada en el marco de la preparación del presente informe. Estos principios y recomendaciones deben entenderse como un complemento a las obligaciones internacionales de derechos humanos derivadas para los Estados del derecho internacional vigente.

La selección de los antecedentes reseñados se realizó en función de su relevancia internacional y de su impacto en Uruguay, se presentan en cada subsección en orden cronológico.

Naciones Unidas

En el ámbito de la Organización de las Naciones Unidas existe en curso un proceso orientado a la gobernanza internacional de la Inteligencia Artificial impulsado por el Secretario General, a la vez que se encuentra en negociación el Pacto Digital Global que incluiría un capítulo específico sobre Inteligencia Artificial. Se proyecta que el Pacto sea adoptado en el marco de la Cumbre del Futuro que tendrá lugar en setiembre próximo. Los procesos en curso tienen, como antecedente, entre otros, los hitos en el ámbito de la Organización de las Naciones Unidas que se indican a continuación en esta sección.

Recomendación de la UNESCO sobre la ética de IA (2021)

La Recomendación sobre la ética de la inteligencia artificial fue adoptada en noviembre de 2021 por la Conferencia General de la Organización de las Naciones Unidas para la Educación, la Ciencia y la Cultura (UNESCO)[113]. Tiene el propósito de orientar a los Estados en la formulación de sus leyes y políticas relativas a la inteligencia artificial. Para ello, la Recomendación impulsa un conjunto de valores[114], principios y acciones de política.

El texto analizan “las repercusiones positivas y negativas profundas y dinámicas de la inteligencia artificial” en las sociedades, el ambiente y en la vida humana y plantea que “el hecho de tener en cuenta los riesgos y las preocupaciones éticas no debería obstaculizar la innovación y el desarrollo”, sino por el contrario, estimular

[113] UNESCO. Recomendación sobre la ética de la inteligencia artificial, Adoptada el 23 de noviembre de 2021. Disponible en: https://unesdoc.unesco.org/ark:/48223/pf0000381137_spa . Últ. Acceso:29/4/2024.

[114] Los valores indicados son: Respeto, protección y promoción de los derechos humanos, las libertades fundamentales y la dignidad humana. Prosperidad del medio ambiente y los ecosistemas. Garantizar la diversidad y la inclusión. Vivir en sociedades pacíficas, justas e interconectadas.

una investigación y una innovación realizadas de manera ética y basada en los derechos humanos[115].

En 2023 Uruguay adhirió a la Recomendación de la UNESCO, reforzando así el compromiso del país hacia su implementación el marco de la nueva Estrategia de Inteligencia Artificial y la primera Estrategia Nacional de Datos[116]. Por lo expuesto y dada su importancia como marco de referencia para la elaboración del presente Informe, a continuación, se presenta una síntesis de los 10 principios rectores que promueve la Recomendación.

Principios de la UNESCO[117]

Principio	Alcance
Proporcionalidad e inocuidad.	La Recomendación plantea que se debería garantizar la aplicación de procedimientos de evaluación de riesgos y medidas para impedir daños a los seres humanos, el ambiente y los ecosistemas. Asimismo, se debería garantizar que los procesos relacionados con el ciclo de vida de los sistemas de IA estén ceñidos a propósitos u objetivos legítimos. La Recomendación sostiene que los sistemas de IA no deberían utilizarse con fines de calificación social o vigilancia masiva.
Seguridad y protección.	La Recomendación indica que los riesgos de seguridad y protección deberían identificarse,

[115] Ibíd. Preámbulo.

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

[117] En base a los párrafos 25 a 47 de la Recomendación sobre la Ética de la IA de la UNESCO.

	prevenirse y eliminarse a lo largo del ciclo de vida de la IA.
Equidad y no discriminación	La Recomendación destaca que se debería adoptar un enfoque inclusivo para asegurar que los beneficios de las tecnologías de IA estén disponibles y sean accesibles para todas las personas, teniendo en cuenta las necesidades específicas de los distintos grupos. Asimismo sostiene que se deberían abordar las brechas digitales en los países y entre ellos y los sesgados a lo largo del ciclo de vida de los sistemas de IA.
Sostenibilidad	La Recomendación subraya la necesidad de evaluar los impactos de las tecnologías de la IA en la sostenibilidad, esto es, la evaluación continua de los efectos humanos, sociales, culturales, económicos y ambientales implicados en esta tecnología.
Derecho a la intimidad y protección de datos.	La Recomendación plantea que la privacidad debe ser respetada, protegida y promovida a lo largo del ciclo de vida de los sistemas de IA. Sostiene que los sistemas algorítmicos requieren evaluaciones adecuadas del impacto en la privacidad, y señala que deberían establecerse marcos de protección de datos y mecanismos de gobernanza de datos adecuados, y de acuerdo con el enfoque de múltiples partes interesadas.
Supervisión y decisión humanas	La Recomendación sostiene que los Estados Miembros deberían velar para que, en cualquier etapa del ciclo de vida de los sistemas de IA, siempre

	sea posible atribuir la responsabilidad ética y jurídica a personas físicas o entidades jurídicas existentes.
Transparencia y explicabilidad	La Recomendación afirma que las personas deberían ser plenamente informadas cuando una decisión se basa en algoritmos de IA o se toma a partir de sus resultados y en particular cuando impacta en sus derechos, y plantea que deberían existir mecanismos adecuados para revisar y enmendar la decisión. Sostiene que los actores de IA deberían informar a los usuarios de manera adecuada y oportuna cuando un producto o servicio se brinda directamente o con ayuda de un sistema de IA. La Recomendación define que la explicabilidad, supone hacer inteligibles los resultados de los sistemas de IA y facilitar información sobre ellos. También se refiere a la inteligibilidad de la entrada, salida y funcionamiento de cada componente algorítmico y la forma en que contribuye a los resultados de los sistemas (trazabilidad).
Responsabilidad y rendición de cuentas	La Recomendación plantea que los actores de la IA y los Estados Miembros deberían respetar, proteger y promover los derechos humanos, fomentar la protección del medio ambiente y los ecosistemas, asumiendo su responsabilidad ética y jurídica respectiva. Para ello, deberían elaborarse mecanismos adecuados de supervisión, evaluación del impacto, auditoría y diligencia debida, incluso en lo que se refiere a la protección de los denunciantes de

	irregularidades, para garantizar la rendición de cuentas respecto de los sistemas de IA y de su impacto a lo largo de su ciclo de vida.
Sensibilización y educación.	La Recomendación enfatiza que la sensibilización y la comprensión pública respecto de las tecnologías de la IA, su funcionamiento e impacto deberían promoverse mediante una educación abierta y accesible, la participación cívica, las competencias digitales y la capacitación en materia de ética de la IA, la alfabetización mediática e informacional.
Gobernanza y colaboración adaptativas y de múltiples partes interesadas.	La Recomendación plantea que a efectos de asegurar un enfoque inclusivo en la gobernanza de la IA es necesario garantizar la participación de las diferentes partes interesadas (los gobiernos, las organizaciones intergubernamentales, la academia, la sociedad civil, el sector privado, las instituciones de derechos humanos, entre otras).

A efectos de la implementación de estos principios, la Recomendación de la UNESCO promueve un conjunto de acciones específicas a implementar por los Estados y otros actores. En función del objeto de este informe, se destacan las siguientes:

- Velar por que los mecanismos de gobernanza de la IA sean inclusivos, transparentes, multidisciplinarios y cuenten con múltiples partes interesadas.
- Asegurar que la legislación en materia de sistemas de IA se ajuste a las obligaciones de los Estados Miembros en materia de derechos humanos

y promueva los derechos humanos y las libertades fundamentales a lo largo del ciclo de vida de estos sistemas.

- Elaborar o adaptar, según proceda, marcos reguladores para alcanzar la rendición de cuentas y la responsabilidad por el contenido y los resultados de los sistemas de IA en las diferentes etapas de su ciclo de vida. Estos marcos deberían tener en cuenta que: la responsabilidad y la rendición de cuentas deben recaer siempre en última instancia en personas físicas o jurídicas y que no se debe otorgar personalidad jurídica a los propios sistemas de IA e incorporar el principio de la supervisión humana.
- Contar con marcos para proteger los datos personales y garantizar una supervisión eficaz e independiente en el marco de un mecanismo de gobernanza de datos.
- Establecer requisitos claros de transparencia y explicabilidad de los sistemas de IA para ayudar a garantizar la fiabilidad de dichos sistemas durante todo su ciclo de vida. Esos requisitos deberían abarcar la concepción y la aplicación de mecanismos de evaluación del impacto que tengan en cuenta la naturaleza del ámbito de aplicación, la utilización prevista, los destinatarios y la viabilidad de cada sistema de IA en particular.
- Asegurar el cumplimiento de las leyes, políticas y prácticas ambientales por parte de todos los actores de la IA.
- Asignar fondos específicos del presupuesto público a la financiación de planes con perspectiva de género, velar por que las políticas digitales nacionales incluyan un plan de acción en materia de género y elaborar políticas pertinentes.
- Promover programas generales de sensibilización sobre los avances de la IA, en particular sobre los datos y las oportunidades que ofrecen y los retos que plantean las tecnologías de la IA, el impacto de los sistemas de IA en los derechos humanos, incluidos los derechos de los niños, y sus repercusiones. Estos programas deberían ser accesibles tanto a los grupos técnicos como a los no técnicos.

- Promover la investigación y alentar a las empresas del sector privado a que faciliten el acceso de la comunidad científica a sus datos para la investigación.
- Garantizar que los actores de la IA respeten y promuevan la libertad de expresión y el acceso a la información en lo que respecta a la generación, moderación y conservación automáticas de contenidos, a través de marcos adecuados, incluso reglamentarios, que propicien la transparencia, velen por que los usuarios tengan acceso a puntos de vista diversos y prever procesos de notificación rápida a los usuarios sobre los motivos de la eliminación u otro tratamiento de los contenidos, así como mecanismos de recurso que permitan a los usuarios solicitar reparación.
- Evaluar y abordar el impacto de los sistemas de IA en los mercados de trabajo y sus consecuencias en las necesidades educativas de cada país.
- Impulsar y apoyar los esfuerzos de otros actores para adecuar los programas y estrategias de capacitación a las futuras implicaciones del trabajo y a las necesidades de la industria, incluidas las pequeñas y medianas empresas y poner en marcha programas de perfeccionamiento y reconversión profesional, y explorar programas de protección social para aquellos que no puedan reconvertirse.
- Adoptar las medidas adecuadas para garantizar la competitividad de los mercados y la protección de los consumidores, considerando posibles medidas y mecanismos en los planos nacional, regional e internacional, a fin de impedir los abusos de posición dominante en el mercado, incluidos los monopolios, en relación con los sistemas de IA durante su ciclo de vida.

Principios y recomendaciones preliminares del Órgano Asesor de Alto Nivel sobre Inteligencia Artificial (2023).

Este antecedente se desprende del Informe provisional: Gobernar la IA para la humanidad (Interim Report: Governing AI for Humanity) elaborado por el Órgano Asesor sobre Inteligencia Artificial de las Naciones Unidas, publicado en diciembre

de 2023[118]. El órgano fue creado ese mismo año a instancias del Secretario General, con el fin de tratar los riesgos, las oportunidades y la gobernanza internacional de la IA y está integrado por personas expertas independientes[119].

El informe del órgano asesor describe un conjunto de oportunidades y riesgos implicados en los sistemas de IA y analiza que el déficit de gobernanza global conlleva a que los beneficios y riesgos se encuentren desigualmente repartidos en el mundo. Destaca la necesidad de identificar y abordar los riesgos de la IA, incluida la creación de consenso sobre qué riesgos son inaceptables y cómo pueden prevenirse o anticiparse.

Las recomendaciones del Órgano Asesor enfatizan la necesidad de una gobernanza global internacional de la IA basada en cinco principios rectores que se resumen a continuación.

Principios para la gobernanza internacional de la IA promovidos por el Órgano Asesor sobre IA de la ONU

Principio	Alcance
La IA debe gobernarse de forma inclusiva, por y para el beneficio de todos.	El informe plantea que la IA debe ser gobernada de forma tal que todas las personas y todos los países sin perjuicio de su nivel de desarrollo puedan beneficiarse de la misma.
La IA debe regirse por el interés público.	El informe sostiene que se necesitan normas vinculantes aplicadas consistentemente por los

[118] https://www.un.org/sites/un2.un.org/files/un_ai_advisory_body_governing_ai_for_humanity_interim_report.pdf. Últ. Acceso:29/4/2024.

[119] La lista completa de integrantes se encuentra disponible en el siguiente enlace: https://www.un.org/en/ai-advisory-body/members Últ. Acceso:29/4/2024.

	Estados miembros para garantizar que prevalezcan los intereses públicos.
La gobernanza de la IA debe construirse de manera conjunta con la gobernanza de los datos y la promoción de los datos comunes.	El informe plantea la necesidad de considerar cómo se recopilan, almacenan y comparten los datos, para asegurar que los datos se compartan y utilicen de una manera que beneficie a la sociedad en su conjunto.
La gobernanza de la inteligencia artificial debe ser universal, en red y estar arraigada en una colaboración adaptativa entre múltiples partes interesadas.	El informe destaca que cualquier esfuerzo de gobernanza de la inteligencia artificial debe priorizar el respaldo universal de diferentes Estados Miembros y partes interesadas y la participación inclusiva del Sur Global contemplando los distintos contextos culturales.
La gobernanza de la IA debe basarse en las normas y compromisos internacionales.	El informe promueve que la gobernanza de la IA debe basarse 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.

Se ha anunciado que el informe final del Órgano Asesor sería presentado a mediados de 2024, y que el mismo sería un insumo fundamental para la definición de los compromisos y acciones específicas en materia de Inteligencia Artificial que los Estados Miembros asumirán en el marco del Pacto Digital Global en setiembre

de 2024. Uruguay ha participado de las instancias de consulta promovidas por el Órgano Asesor sobre IA y participa de la negociación en curso del Pacto Digital Global.

Resolución A/RES/78/265 de la Asamblea General de la ONU (2024)

La resolución de la Asamblea General de las Naciones Unidas 78/265, "Aprovechar las oportunidades de sistemas seguros y fiables de inteligencia artificial para el desarrollo sostenible"[120], fue adoptada el 21 de marzo de este año tras haber sido copatrocinada por más de 120 Estados, entre estos, Uruguay.

La Resolución alcanza a los "sistemas de inteligencia artificial en el ámbito no militar, cuyo ciclo de vida incluye las etapas de prediseño, diseño, desarrollo, evaluación, puesta a prueba, despliegue, utilización, venta, adquisición, explotación y retirada de servicio".

El texto define las características que distinguen los sistemas seguros y fiables de IA en los siguientes términos: "(…) están centrados en las personas, son fiables, se pueden explicar, son éticos e inclusivos, respetan plenamente la promoción y la protección de los derechos humanos y el derecho internacional, mantienen la privacidad, están orientados al desarrollo sostenible y son responsables"[121].

La Resolución afirma que[122] "se deben respetar, proteger y promover los derechos humanos y las libertades fundamentales durante todo el ciclo de vida de los sistemas de inteligencia artificial", y "exhorta a todos los Estados Miembros y, en su caso, a otros interesados, a que se abstengan o dejen de usar sistemas de inteligencia artificial que sean imposibles de operar en consonancia con el derecho internacional o que supongan riesgos indebidos para el disfrute de los derechos humanos".

[120] ONU - Asamblea General. Resolución aprobada por la Asamblea General el 21 de marzo de 2024. 78/265. Aprovechar las oportunidades de sistemas seguros y fiables de inteligencia artificial para el desarrollo sostenible. A/RES/78/265. Disponible en: https://documents.un.org/doc/undoc/gen/n24/087/86/pdf/n2408786.pdf?token=hxXvAKO8RS5xFkIlcb&fe=true. Últ. Acceso:29/4/2024.

[121] Ibíd. Considerandos.

[122] Ibíd. Punto 5.

La resolución de la ONU alienta a los Estados Miembros a promover sistemas seguros y fiables de inteligencia artificial a través de distintos medios, entre otros:

- Promoviendo la elaboración y la aplicación de enfoques y marcos regulatorios y de gobernanza nacionales, en consonancia con sus respectivas políticas y prioridades, y con las obligaciones que les incumben en virtud del derecho internacional, a fin de apoyar la innovación y la inversión responsables e inclusivas en inteligencia artificial, promoviendo al mismo tiempo sistemas seguros y fiables de IA [123].

- Fomentando el desarrollo, la aplicación y la divulgación de mecanismos de seguimiento y gestión de riesgos, mecanismos para la protección de los datos, incluida la protección de los datos personales y políticas de privacidad, y evaluaciones de impacto según proceda, durante todo el ciclo de vida de los sistemas de inteligencia artificial[124].

- Alentando el desarrollo y la implantación de herramientas técnicas, normas o prácticas eficaces, accesibles, adaptables e interoperables a nivel internacional, incluidos mecanismos de autenticación del contenido y del origen fiables, como las marcas de agua o el etiquetado, en los casos en que sea técnicamente posible o apropiado, que permitan a los usuarios identificar los casos en que se ha manipulado la información, distinguir o determinar el origen del contenido digital auténtico y del generado por inteligencia artificial o manipulado, y aumentando la alfabetización mediática e informacional[125].

- Facilitando la elaboración y la aplicación de marcos, prácticas y normas eficaces e interoperables a nivel internacional para el entrenamiento y la puesta a prueba de los sistemas de inteligencia artificial a fin de mejorar la formulación de políticas y de ayudar a proteger a las personas frente a todas las formas de discriminación, sesgo, uso indebido u otros daños, y de evitar reforzar o perpetuar las aplicaciones y los resultados discriminatorios o

[123]Ibíd. Punto 6. Literal a)

[124] Ibíd. Punto 6. Literal e)

[125] Ibíd. Punto 6. Literal g).

sesgados durante todo el ciclo de vida de los sistemas de inteligencia artificial [126].

- 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 [127].

- Promoviendo la transparencia, la previsibilidad, la fiabilidad y la facilidad de comprensión a lo largo de todo el ciclo de vida de los sistemas de inteligencia artificial que se utilizan para tomar decisiones o para apoyar la toma de decisiones que afectan a los usuarios finales, entre otras cosas, proporcionando información y explicaciones, y promoviendo la supervisión humana, por ejemplo, mediante el examen de las decisiones automatizadas y los procesos conexos o, en los casos en que resulte apropiado y pertinente, mediante la previsión de alternativas de toma de decisiones por personas o medios de reparación y de rendición de cuentas eficaces para quienes se vean afectados negativamente por las decisiones automáticas de los sistemas de inteligencia artificial [128].

- Fortaleciendo la inversión en la elaboración y la aplicación de salvaguardias eficaces, incluidas evaluaciones de riesgos y del impacto, a lo largo de todo el ciclo de vida de los sistemas de inteligencia artificial para proteger el goce pleno y efectivo de los derechos humanos y las libertades fundamentales y mitigar el posible impacto en él [129].

[126] Ibíd. Punto 6. Literal h).

[127] Ibíd. Punto 6. Literal i).

[128] Ibíd. Punto 6. Literal k).

[129] Ibíd. Punto 6. Literal l).

Otros procesos intergubernamentales

En el ámbito de la Organización para la Cooperación y el Desarrollo Económicos (OCDE), así como en el Consejo de Europa, el G7 y el G20, en los últimos años han tenido lugar diversos procesos orientados a impulsar un marco común para la gobernanza de la IA. En esta sección se presenta una síntesis de los principios y orientaciones de política emergentes de estos esfuerzos.

Recomendación de la OCDE sobre Inteligencia Artificial (2019)

La Recomendación del Consejo de la OCDE sobre IA[130] fue adoptada originalmente por el Consejo de la Organización para la Cooperación y el Desarrollo Económico (OCDE) en mayo de 2019. Para dar respuesta a los avances en las tecnologías de Inteligencia Artificial y particularmente en el campo de la IA generativa, desde entonces fue enmendada en dos oportunidades: en 2023 y recientemente en 2024.

Los principios buscan facilitar la interoperabilidad de las políticas globales y abogan por una IA que sea innovadora y confiable, y que proteja los derechos humanos y valores democráticos. En 2024 Uruguay solicitó formalmente la adhesión a los Principios de la OCDE, estando actualmente el proceso en trámite.

Principios de la OCDE sobre Inteligencia Artificial

Principio	Alcance
Crecimiento inclusivo, desarrollo sostenible y bienestar	La Recomendación plantea que las partes interesadas[131] deben participar de manera proactiva en una gestión responsable de la IA en beneficio de las personas y el planeta, favoreciendo el crecimiento

[130] OCDE. Recomendación del Consejo sobre Inteligencia Artificial. **OCDE/LEGAL/0449.** https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0449 Últ. Acceso, 13/05/2024.

[131] La Recomendación define partes interesadas indicando que “abarcan todas las organizaciones e individuos involucrados o afectados por los sistemas de IA, directa o indirectamente”.

	inclusivo, el bienestar, el desarrollo sostenible y la sostenibilidad medioambiental.
Respeto del Estado de Derecho, los derechos humanos y los valores democráticos, incluidas la equidad y la privacidad.	La Recomendación sostiene que los actores de la IA[132] deben respetar el Estado de derecho, los derechos humanos y los valores democráticos durante todo el ciclo de vida del sistema de IA, para lo cual deben aplicar mecanismos y salvaguardas para hacer frente a los riesgos derivados de los usos fuera de la finalidad prevista, el uso indebido intencionado o el uso indebido no intencionado, de una manera adecuada al contexto. Esto también incluye abordar la desinformación amplificada por la IA, respetando al mismo tiempo la libertad de expresión y otros derechos y libertades protegidos por el derecho internacional aplicable.
Transparencia y explicabilidad	La Recomendación subraya que los actores de la IA deben comprometerse con la transparencia y la divulgación responsable de los sistemas de IA, para lo cual deben proporcionar información significativa, adecuada al contexto y coherente con el estado de la técnica. Tal información debe permitir una comprensión general de los sistemas de IA, incluidas sus capacidades y limitaciones, conocer cuando se está interactuando con los sistemas de IA, y cuando sea factible y útil, información sencilla y fácil de entender sobre las fuentes de datos/entradas, factores,

[132] La Recomendación define que “los actores de IA son aquellos que desempeñan un papel activo en el ciclo de vida del sistema de IA, incluidas las organizaciones e individuos que implementan u operan IA”.

	procesos y/o lógica que permita comprender el resultado y, de ser el caso, cuestionar su resultado para aquellos afectados negativamente por el resultado.
Robustez, seguridad y protección	La Recomendación plantea que los sistemas de IA deben ser sólidos, seguros y protegidos a lo largo de todo su ciclo de vida, de forma tal que en cualquier condición de uso no planteen riesgos irrazonables para la seguridad. Cuando sea técnicamente factible, para reforzar la integridad de la información y al mismo tiempo garantizar el respeto a la libertad de expresión.
Responsabilidad	La Recomendación plantea que los actores de la IA deben ser responsables del correcto funcionamiento de los sistemas de IA y del respeto de los principios anteriores. Con este fin deben garantizar la trazabilidad, incluso en relación con los conjuntos de datos, los procesos y las decisiones tomadas durante el ciclo de vida del sistema de IA y aplicar un enfoque sistemático de gestión de riesgos a cada fase del ciclo de vida del sistema de IA de forma continua y adoptar una conducta empresarial responsable para abordar los riesgos relacionados con los sistemas de IA.

Principios de Inteligencia Artificial del G20 (2019)

En 2019 a través de una resolución el Grupo de los Veinte (G20) explicitó su apoyo a los Principios de OCDE y tomó nota de sus recomendaciones[133]. La resolución reproduce los referidos principios ya comentados en el apartado anterior.

Principios rectores internacionales para las organizaciones que desarrollan sistemas avanzados de IA, Principios de Hiroshima (2023)

Los principios de la OCDE también han servido de base para otros desarrollos, como los Principios rectores internacionales para las organizaciones que desarrollan sistemas de IA avanzada, adoptados por el G7, denominados Principios de Hiroshima[134]. Su adopción se produjo en 2023 el marco del Proceso de Hiroshima[135] y buscan abordar los recientes avances de los sistemas más avanzados de IA incluyendo la IA generativa, ofreciendo orientación para las organizaciones que desarrollan y utilizan los sistemas de IA más avanzados. El concepto de organizaciones en el contexto de los Principios incluye, entre otras, entidades del mundo académico, la sociedad civil, el sector privado y el sector público.

Los Principios de Hiroshima dieron lugar a un código de conducta para desarrolladores.

[133] https://www.mofa.go.jp/policy/economy/g20_summit/osaka19/pdf/documents/en/annex_08.pdf Ùlt. Acceso 2/5/2024.

[134] G7 Leaders' Statement on the Hiroshima AI Process. 30 de octubre de 2023. Disponible en: https://digital-strategy.ec.europa.eu/es/library/hiroshima-process-international-guiding-principles-advanced-ai-system. Ùlt, Acceso, 02/05/2024.

[135] El 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. 4. Cooperación basada en proyectos en apoyo del desarrollo de herramientas y mejores prácticas de IA responsables (Cfr (https://digital-strategy.ec.europa.eu/en/library/g7-leaders-statement-hiroshima-ai-process),

Principios de Hiroshima

Principio	Alcance
Identificación, evaluación y mitigación de riesgos en todo el ciclo de vida de la IA.	Se plantea adoptar las medidas adecuadas durante todo el desarrollo de los sistemas avanzados de IA, incluso antes y durante su despliegue, para identificar, evaluar y mitigar los riesgos existentes a lo largo del ciclo de vida de la IA.
Identificación y mitigación de las vulnerabilidades y, en su caso, de los incidentes y usos indebidos.	Se plantea monitorear vulnerabilidades, incidentes, riesgos emergentes y uso indebido después de la implementación, y tomar las medidas adecuadas para abordarlos. Los mecanismos para informar sobre vulnerabilidades, cuando corresponda, deben ser accesibles a un conjunto diverso de partes interesadas.
Transparencia.	Se plantea informar públicamente a través de información clara y precisa sobre las capacidades, limitaciones y ámbitos de uso apropiado e inapropiado de los sistemas avanzados de IA, para a contribuir a garantizar una transparencia suficiente y aumentar la rendición de cuentas.
Intercambio de información.	Se plantea trabajar por un intercambio responsable de información y de notificación de incidentes entre las organizaciones que desarrollan sistemas avanzados, incluyendo a la industria, los gobiernos, la sociedad civil y la academia.

Políticas de gestión de riesgos y gobernanza de la IA.	Se plantea desarrollar, implementar y divulgar políticas de gobernanza y gestión de riesgos de inteligencia artificial, fundadas en un enfoque basado en el riesgo, incluidas políticas de privacidad y medidas de mitigación. Esto debería incluir procesos de rendición de cuentas y gobernanza para evaluar y mitigar los riesgos, cuando sea factible, durante todo el ciclo de vida de la IA.
Seguridad	Se plantea invertir y aplicar controles de seguridad sólidos, incluida la seguridad física, ciberseguridad y protección frente a amenazas internas en todo el ciclo de vida de la IA.
Mecanismos de autentificación de contenidos	Se plantea desarrollar e implementar mecanismos confiables de autenticación y procedencia de contenido, cuando sea técnicamente factible, como marcas de agua u otras técnicas para permitir a los usuarios identificar contenido generado por IA.
Investigación para mitigar los riesgos sociales y de seguridad e inversión en medidas de mitigación efectivas.	Se plantea realizar, colaborar e invertir en investigaciones que respalden el avance de la seguridad y la confianza de la IA, y abordar riesgos clave, así como invertir en el desarrollo de herramientas de mitigación adecuadas.
Desarrollar sistemas avanzados de IA centrados en el ser humano y los desafíos globales y el apoyo al logro de los ODS.	Se plantea priorizar el desarrollo de sistemas avanzados de IA para abordar los mayores desafíos del mundo, en particular, entre otros, la crisis climática, la salud global y la educación. Apoyar el progreso en los Objetivos de Desarrollo Sostenible de las Naciones Unidas. Las organizaciones deben priorizar la gestión responsable de una IA confiable y

	centrada en el ser humano y también apoyar iniciativas de alfabetización digital.
Desarrollo y adopción de estándares y normas técnicas internacionales relativas a la IA.	Se plantea contribuir al desarrollo y, cuando corresponda, el uso de estándares técnicos y mejores prácticas internacionales, incluidas las marcas de agua, y trabajar con organizaciones de desarrollo de estándares.
Implementación de medidas para la protección de los datos personales y la propiedad intelectual	Se plantea implementar medidas apropiadas de entrada de datos y protecciones para datos personales y propiedad intelectual. Gestionar la calidad de los datos, incluidos los datos de entrenamiento y la recopilación de datos, para mitigar los sesgos. Apoyar la transparencia adecuada de los conjuntos de datos de entrenamiento y el cumplimiento de los marcos legales aplicables.

Convenio Marco del Consejo de Europa (2024)

El Convenio Marco sobre Inteligencia Artificial, Derechos Humanos, Democracia y Estado de Derecho [136] fue adoptado formalmente por el Comité de Ministros del Consejo de Europa (COE) en mayo de 2024 y se abrirá a la firma de los Estados Miembros y no miembros del Consejo en setiembre próximo. El texto del Convenio fue negociado en el ámbito del Comité sobre Inteligencia Artificial del COE en un proceso que se extendió entre 2021 y marzo de 2024. En octubre de 2023 Uruguay se integró al Comité en calidad de observador, condición que le habilita a los Estados no miembros la posibilidad de adherir al tratado.

[136] Disponible en: https://rm.coe.int/-1493-10-1b-committee-on-artificial-intelligence-cai-b-draft-framework/1680aee411

En el caso de este antecedente, se trata de un instrumento de naturaleza jurídica vinculante para los Estados que lo suscriban y ratifiquen.

El Convenio Marco tiene por objetivo garantizar que las actividades dentro del ciclo de vida de los sistemas de inteligencia artificial cumplan y sean consistentes con las obligaciones, estándares y compromisos internacionales de derechos humanos de los Estados, y sean plenamente consistentes con la democracia y el Estado de Derecho.

El tratado obliga a todas las partes a abordar los riesgos derivados de las actividades relacionadas con el ciclo de vida de IA tanto del sector público como del sector privado, estableciendo matices en cuanto al alcance de las obligaciones de los Estados con respecto al sector privado en el contexto del Convenio.

El Informe Explicativo que acompaña Tratado, sostiene que el mismo garantiza que las obligaciones aplicables existentes de cada Parte en materia de derechos humanos, democracia y Estado de Derecho también se apliquen a las actividades dentro del ciclo de vida de la inteligencia artificial. En este sentido, el Convenio Marco está alineado con el sistema y los mecanismos de protección de derechos humanos aplicables de cada Parte, incluidas sus obligaciones de derecho internacional y otros compromisos internacionales y su derecho interno aplicable.

Como tal, ninguna disposición de este Convenio Marco tiene como objetivo crear nuevos derechos humanos u obligaciones de derechos humanos o socavar el alcance y contenido de las protecciones aplicables existentes, sino más bien, al establecer varias obligaciones jurídicamente vinculantes contenidas en sus Capítulos II a VI, facilitar la implementación efectiva de las obligaciones de derechos humanos aplicables de cada Parte en el contexto de los nuevos desafíos planteados por la inteligencia artificial[137].

Con respecto al sector privado, el Informe explica que el tratado obliga a todas las Partes a abordar los riesgos e impactos para los derechos humanos, la democracia y el estado de derecho en el sector privado, y aclara que, al abordar los riesgos no

[137] COE – CAI. Explanatory Report. Párr. 13 (traducción no oficial). Disponible en: https://www.coe.int/en/web/artificial-intelligence/cai. Ùlt. Acceso. 2/5/2024.

es simplemente reconocer esos riesgos, sino que requiere la adopción o el mantenimiento de medidas legislativas, administrativas o de otro tipo apropiadas para dar efecto a esta disposición, así como la cooperación entre las Partes según lo dispuesto en las disposiciones sobre el mecanismo de seguimiento y la cooperación internacional. Aclara, sin embargo, que la obligación no requiere necesariamente legislación adicional, y las Partes pueden hacer uso de otras medidas apropiadas, incluidas medidas administrativas y voluntarias. Entonces, si bien la obligación es vinculante y todas las Partes deben cumplirla, la naturaleza de las medidas adoptadas por las Partes podría variar[138].

Se exceptúa del alcance del Convenio las actividades dentro del ciclo de vida de los sistemas de inteligencia artificial relacionadas con la protección de sus intereses de seguridad nacional. El Informe Explicativo, precisa que esta excepción se aplica sólo si y en la medida en que las actividades se relacionen con la protección de los intereses de seguridad nacional, de forma tal que todas las actividades regulares de aplicación de la ley para la prevención, detección, investigación y enjuiciamiento de delitos, incluidas las amenazas a la seguridad pública, también permanecen dentro del alcance del Convenio Marco siempre y cuando los intereses de seguridad nacional de las Partes no estén en juego.

El Convenio Marco consta de 36 artículos y 8 capítulos.

El capítulo II establece las obligaciones generales de los Estados Parte de: adoptar o mantener medidas para garantizar que las actividades dentro del ciclo de vida de los sistemas de inteligencia artificial sean consistentes con las obligaciones de proteger los derechos humanos, según lo consagrado en el derecho internacional aplicable y en su derecho interno (artículo 4) y de adoptar o mantener medidas que busquen garantizar la integridad, independencia y eficacia de las instituciones y los procesos democráticos (artículo 5). En tanto el capítulo III estipula los principios comunes que orientarán la implementación del Convenio.

Como fue indicado, se exige a las Partes apliquen los marcos nacionales e internacionales existentes al contexto de las actividades dentro del ciclo de vida de

[138] Ibíd. Párr. 29.

los sistemas de inteligencia artificial, adoptando o manteniendo de manera consistente con tales marcos, medidas para garantizar la disponibilidad de recursos accesibles y efectivos para las violaciones de los derechos humanos resultantes de las actividades dentro del ciclo de vida de los sistemas de inteligencia artificial (artículo 14).

Asimismo, el Convenio plantea que los Estados Partes deberán adoptar o mantener medidas ex ante y, según corresponda, de forma iterativa a lo largo del ciclo de vida del sistema de inteligencia artificial, para la identificación, evaluación, prevención y mitigación de los riesgos, considerando los impactos reales y potenciales en los derechos humanos, la democracia y el estado de derecho. Se indica que tales medidas deberán ser graduales y diferenciadas adecuadas al contexto y uso.

Al respecto el Informe Explicativo precisa que esta disposición otorga flexibilidad a las Partes en los enfoques y metodologías para llevar adelante la evaluación. Señala que “en particular, las Partes podrán optar por implementar esta evaluación en diferentes niveles, como a nivel regulatorio, prescribiendo diferentes categorías de clasificación de riesgos y/o a nivel operativo por parte de actores relevantes asignados con responsabilidades para las actividades dentro del ciclo de vida del sistema de inteligencia artificial. Asimismo, cada parte evaluará la necesidad de un moratorio, una prohibición u otras medidas apropiadas con respecto a ciertos usos de los sistemas de inteligencia artificial cuando considere que dichos usos son incompatibles con el respeto de los derechos humanos, el funcionamiento de la democracia o el Estado de Derecho (artículo 15).

Principios enunciados en el Convenio Marco sobre Inteligencia Artificial, Derechos Humanos, Democracia y Estado de Derecho

Principio	Alcance
Dignidad humana y autonomía individual	Adoptar o mantener medidas para respetar la dignidad humana y la autonomía individual

	relacionadas con las actividades dentro del ciclo de vida de los sistemas de inteligencia artificial.
Transparencia y supervisión	Adoptar o mantener medidas para garantizar que existan requisitos adecuados de transparencia y supervisión adaptados a los contextos y riesgos específicos con respecto a las actividades dentro del ciclo de vida de los sistemas de inteligencia artificial, incluso con respecto a la identificación del contenido generado por los sistemas de inteligencia artificial.
Rendición de cuentas y responsabilidad	Adoptar o mantener medidas para garantizar la rendición de cuentas y la responsabilidad por los impactos adversos sobre los derechos humanos, la democracia y el estado de derecho resultantes de actividades dentro del ciclo de vida de los sistemas de inteligencia artificial.
Igualdad y no discriminación	Adoptar o mantener medidas para garantizar que las actividades relacionadas con el ciclo de vida de los sistemas de inteligencia artificial respeten la igualdad, incluida la igualdad de género, y la prohibición de la discriminación y adoptar o mantener medidas destinadas a superar las desigualdades.
Privacidad y protección de datos personales	Adoptar o mantener medias para garantizar la protección de la privacidad de las personas y los datos personales dentro del ciclo de vida de los sistemas de IA, incluso mediante leyes, estándares y marcos nacionales e internacionales, y establecer garantías y salvaguardas efectivas para las personas.

Confiabilidad	Adoptar medidas para promover la confiabilidad de los sistemas de inteligencia artificial, que podrían incluir requisitos relacionados con una calidad y seguridad adecuadas durante todo el ciclo de vida de los sistemas de inteligencia artificial.
Innovación segura	Establecer, cuando resulto apropiado, entornos controlados para desarrollar, experimentar y probar sistemas de IA bajo la supervisión de autoridades competentes para fomentar la innovación, evitando al mismo tiempo impactos adversos sobre los derechos humanos, la democracia y el Estado de Derecho.

Procesos en América Latina y el Caribe

Agenda digital para América Latina y el Caribe, e-LAC (2022)

La Agenda digital para América Latina y el Caribe (e-LAC 2024) fue adoptada en el marco de la Octava Conferencia Ministerial sobre la Sociedad de la Información de América Latina y el Caribe tuvo lugar del 16 al 18 de noviembre de 2022 y fue organizada en conjunto por la Comisión Económica para América Latina y el Caribe (CEPAL) y el Gobierno de Uruguay, ordena un conjunto de prioridades de política y acciones estratégicas a nivel regional en cuatro ejes.

El eje 3 del instrumento aborda la transformación digital productiva y sostenible y establece como uno de los objetivos de la agenda regional el “impulsar el uso efectivo de tecnologías digitales emergentes para promover la productividad, fomentar la innovación y el emprendimiento, previéndose especialmente soluciones de Internet de las cosas, inteligencia artificial y tecnologías amigables con el

medioambiente, con resguardo de los derechos humanos y el uso ético de la tecnología” [139].

En el marco de la implementación de los objetivos de la Agenda se han establecido grupos de trabajo. Los grupos de trabajo son un espacio de cooperación en el marco del eLAC2024, con el objetivo de cumplir una determinada meta bajo la conducción de un país coordinador.

El Grupo de trabajo sobre inteligencia artificial es uno de los grupos establecidos para el período 2023 – 2024 bajo la coordinación del Centro Nacional de Inteligencia Artificial de Chile y la Agencia de Gobierno Electrónico y Sociedad de la Información y del Conocimiento de Uruguay (AGESIC).

Declaración de Santiago (2023)

La Declaración de Santiago para “Para promover una inteligencia artificial ética en América Latina y el Caribe”[140] fue adoptada en octubre de 2023 por loa gobiernos participantes – entre ellos el Gobierno de Uruguay- en el marco del Foro sobre la Ética de la Inteligencia Artificial en América Latina y el Caribe, y de la Cumbre Ministerial y de Altas Autoridades de América Latina y el Caribe, organizada por UNESCO, CAF y el Gobierno de Chile.

La Declaración aprueba la creación de un Grupo de Trabajo para la constitución de un Consejo Intergubernamental de Inteligencia Artificial para América Latina y el Caribe, para fortalecer las capacidades regionales en materia de ética y gobernanza de la IA en el marco de la Recomendación sobre la Ética de la IA de la UNESCO.

A través de este instrumento, los países firmantes acordaron “iniciar un análisis frente a la necesidad de elaborar y adoptar nuevos marcos jurídicos y agendas regulatorias para el diseño, desarrollo y uso responsable de la IA. El análisis

[139] CEPAL (2022). Agenda digital para América Latina y el Caribe, e-LAC 2024, Objetivo 13. Disponible en: https://repositorio.cepal.org/server/api/core/bitstreams/1fae5881-feba-42b4-a0b0-53ba8fa1f679/content. Últ. Acceso, 15/5/2024.

[140] Disponible en: https://minciencia.gob.cl/uploads/filer_public/40/2a/402a35a0-1222-4dab-b090-5c81bbf34237/declaracion_de_santiago.pdf.

debería considerar todos los principios transversales de derechos humanos, en especial los principios de la proporcionalidad e inocuidad, de la seguridad y protección, la equidad y la no discriminación, de la inclusión, de la diversidad de género, de la diversidad cultural, de la accesibilidad, de la sostenibilidad -social, cultural, económica y ambiental-, del derecho a la intimidad y la protección de datos personales, de la supervisión y decisión humana, de la transparencia y la explicabilidad, de la responsabilidad y la rendición de cuentas, de la sensibilización y educación, y de la gobernanza inteligente y colaboración adaptativas y de múltiples partes interesadas"[141]

La Declaración sostiene que es urgente integrar las particularidades de las culturas de América Latina y el Caribe en la creación de tecnologías de IA para la región y plantea que es fundamental incentivar mayores inversiones en la región para aprovechar de forma integral la IA para solucionar sus diversas problemáticas, y promover el uso innovador de esta tecnología, desarrollando los incentivos necesarios para este fin.

Las recientes regulaciones en los Estados Unidos y la Unión Europea

Orden Ejecutiva de 2023 de Estados Unidos

En octubre de 2023, el gobierno de los Estados Unidos emitió una Orden Ejecutiva para el Desarrollo y el uso de la inteligencia artificial de forma segura y fiable[142], en la cual explicita el propósito de impulsar un "enfoque que aborde los riesgos de la IA sin reducir indebidamente sus beneficios"[143].

[141] Cumbre Ministerial y de Altas Autoridades de América Latina y el Caribe (2023). Declaración de Santiago, "Para promover una inteligencia artificial ética en América Latina y el Caribe", punto resolutivo 2. Disponible en: https://minciencia.gob.cl/uploads/filer_public/40/2a/402a35a0-1222-4dab-b090-5c81bbf34237/declaracion_de_santiago.pdf Últ. Acceso. 16/5/2024.

[142] 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.

[143] Artículo 2, literal (a).

La regulación, ordena a diversas entidades federales múltiples medidas para establecer salvaguardas en torno a las tecnologías de inteligencia artificial e impone nuevas normas para determinados desarrolladores de sistemas de IA.
La Orden Ejecutiva plantea ocho principios rectores y prioridades en relación la política de inteligencia artificial que se resumen a continuación:

1. Seguridad y protección: La Orden Ejecutiva promueve que se garanticen evaluaciones sólidas, fiables, repetibles y estandarizadas de los sistemas de IA, así como políticas, instituciones y, en su caso, otros mecanismos para probar, comprender y mitigar los riesgos de estos sistemas antes de ponerlos en uso.
2. Innovación responsable y competencia: La Orden Ejecutiva promueve un conjunto de medidas para atraer el talento al país, inversiones en educación, formación, desarrollo, investigación y capacidad relacionados con la IA, la necesidad de abordar cuestiones de propiedad intelectual (PI) para proteger a los inventores y creadores.
3. Apoyo a los trabajadores: La Orden Ejecutiva analiza que se requiere adaptar la formación y la educación laborales para apoyar una mano de obra diversa y ayudar a facilitar el acceso a las oportunidades que crea la IA, y atender que la IA no despliegue de forma que menoscabe los derechos de los trabajadores.
4. Equidad y protección de derechos civiles: La Orden Ejecutiva plantea que las políticas de Inteligencia Artificial deben ser consistentes con las políticas de promoción de la equidad y con los derechos civiles.
5. Protección al consumidor: La Orden Ejecutiva plantea la protección de los intereses de los consumidores que interactúan con los sistemas de IA, particularmente en áreas críticas, junto con promover el uso responsable de la IA.
6. Privacidad: La Orden Ejecutiva plantea la necesidad de proteger la privacidad a media que la IA sigue avanzando.
7. Gestionar los riesgos del uso de la IA por parte de las entidades federales: La Orden Ejecutiva plantea aumentar la capacidad interna para regular, gobernar y apoyar el uso responsable de la IA para ofrecer mejores resultados.
8. Liderazgo internacional y cooperación: La Orden Ejecutiva plantea que Estados Unidos debe ser líder mundial en IA y pionero en los sistemas y garantías necesarios para desplegar la tecnología de forma responsable, y plantea liderar

los esfuerzos regulatorios orientados a establecer marcos comunes para la garantía y gestión de riesgos, y promoviendo estándares técnicos globales para la IA.

Dentro de las medidas específicas previstas por la Orden Ejecutiva para el logro de los mencionados objetivos se encuentran:

1. Estándares en materia de Seguridad.
    - Requerir a desarrolladores de determinados sistemas que compartan información con el gobierno de Estados Unidos.
    - Desarrollar estándares, herramientas y pruebas para asegurar que los sistemas son seguros y confiables antes de su puesta en producción.
    - Protección contra los riesgos del uso de IA en materiales biológicos peligrosos.
    - Protección 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.
    - Establecer un programa avanzado de ciberseguridad para desarrollar herramientas de IA y colaborar en la detección y resolución de vulnerabilidades en software crítico.
    - Ordenar el desarrollo de un Memorando de Seguridad Nacional para dirigir futuras acciones en IA y seguridad.
2. Protección de la privacidad.
    - Priorizar el apoyo federal para acelerar el desarrollo de tecnologías de preservación de la privacidad.
    - Reforzar la investigación y tecnologías que preserven la privacidad.

- Evaluar la forma en que las agencias recolectan y usan información disponible y reforzar las guías de privacidad para agencias federales.
- 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
   - Proveer guías para arrendadores, programas de beneficios federales y contratistas federales que eviten el uso de algoritmos discriminatorios.
   - Atacar la discriminación algorítmica a través de asistencia técnica, coordinación y mejores prácticas.
   - Asegurar la equidad en el sistema de justicia criminal
4. Proteger a los consumidores, pacientes y estudiantes.
   - Avanzar en el uso responsable de IA en materia de salud
   - Diseñar recursos que apoyen la transformación de la educación a través de herramientas de IA.
5. Apoyo a los trabajadores.
   - Desarrollar principios y buenas prácticas para mitigar los daños y maximizar los beneficios de IA para los trabajadores
   - 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.
   - Catalizar la investigación en IA en los Estados Unidos a través de un piloto de Recurso de Investigación Nacional en IA.

- Promover un ecosistema justo, abierto y competitivo mediante asistencia técnica y recursos para pequeños desarrolladores.
- 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
    - Expandir los compromisos bilaterales, multilaterales, y multiactor para colaborar en IA.
    - Acelerar el desarrollo e implementación de estándares de IA vitales
    - 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.
    - Establecer guías para el uso de IA por oficinas del gobierno.
    - Apoyar a las agencias del gobierno para la adquisición de productos y servicios de IA.
    - Acelerar la rápida contratación de profesionales de IA en el gobierno.

Ley de Inteligencia Artificial de la Unión Europea

El Reglamento Europeo de Inteligencia Artificial [144] fue aprobado por los países de la Unión Europea el 13 de marzo de 2024. De conformidad con lo establecido

[144] **Reglamento de Inteligencia Artificial, 13 de marzo de 2024. Disponible en: https://www.europarl.europa.eu/doceo/document/TA-9-2024-0138_ES.html**

en el artículo 1 su objeto es proteger los derechos fundamentales, la democracia, el Estado de derecho y la sostenibilidad ambiental frente a la IA de alto riesgo al tiempo de impulsar la innovación.

El instrumento de la Unión Europea adopta un enfoque basado en el riesgo en función del cual establece aplicaciones prohibidas y los sistemas de alto riesgo para el cual regula un conjunto de requisitos y obligaciones:

a) **Riesgo inaceptable (Título II).**

Quedan comprendidos en esta clasificación las siguientes aplicaciones prohibidas:

- Manipulación cognitiva del comportamiento de personas que afecte la autonomía y capacidad de elegir libremente o explotar las vulnerabilidades de las personas derivadas de su edad, situación de discapacidad, entre otras. La prohibición no afecta las prácticas legales relacionadas con tratamientos médicos[145].
- Sistemas de categorización biométrica basados en datos biométricos[146].
- Sistemas de IA que permiten a agentes públicos o privados llevar a cabo una puntuación ciudadana de las personas físicas sobre la base de varios puntos de datos relacionados con su comportamiento social en múltiples contextos o de características personales o de su personalidad conocidas, inferidas o predichas durante determinados períodos de tiempo[147].
- Uso de sistemas de IA para la identificación biométrica remota «en tiempo real» de personas físicas en espacios de acceso público con fines de aplicación de la ley (se establece excepciones)[148].

b) **Sistemas de IA de alto riesgo (Título III).**

Se coloca bajo esta clasificación aquellos cuya salida que producen resulte relevante en una acción o decisión con posible riesgo importante para la

[145] Párr. 29.

[146] Párr. 30.

[147] Párr. 31.

[148] Párr. 32 y 33.

salud, la seguridad o los derechos fundamentales de las personas. El reglamento indica la clasificación debe realizarse teniendo en cuenta tanto la gravedad del posible perjuicio como la probabilidad de que éste se produzca. Dispone que la puesta en servicio o la utilización de sistemas de IA de alto riesgo debe supeditarse al cumplimiento de determinados requisitos obligatorios.

Entre otros quedan comprendidos en esta clasificación:

- Varios casos uso de sistemas de identificación biométrica.
- Los sistemas de IA destinados a ser utilizados como componentes de seguridad en la gestión y el funcionamiento de las infraestructuras críticas.
- Los sistemas de IA que se utilizan en la educación o la formación profesional.
- Los sistemas de IA que se utilizan en los ámbitos del empleo, la gestión de los trabajadores, en particular para la contratación y la selección de personal.
- Los sistemas de IA usados para evaluar la calificación crediticia o solvencia de las personas físicas, ya que deciden si dichas personas pueden acceder a recursos financieros o servicios esenciales.
- Los sistemas de IA destinados a ser utilizados con fines de aplicación de la ley
- Los sistemas de IA utilizados en la migración, el asilo y la gestión del control fronterizo.
- Sistemas de IA destinados para la administración de justicia.
- Las implementaciones con IA de productos o componentes de seguridad de productos que ya estén cubiertos por legislación europea (como por ejemplo, dispositivos médicos, ferrocarriles, aviones o maquinaria).

El Reglamento define varias autoridades de supervisión. También dispone una serie de exigencias que los proveedores de sistemas de alto riesgo deben cumplir. Entre éstas, el artículo 9 indica que se establecerá, implantará, documentará y mantendrá un sistema de gestión de riesgos. Asimismo, se

establece que en lo pertinente los proveedores deberán asegurar que las personas físicas sean informadas de que están interactuando con un sistema IA.

Anexo 3: Aportes recibidos en el proceso de consulta

Institución Nacional de Derechos Humanos y Defensoría del Pueblo

Montevideo, 11 de junio de 2024.

Ref. Informe sobre aplicación del artículo 74 de la Ley N° 20.212

i. Antecedentes

De acuerdo a lo establecido en el artículo 74 de la Ley N° 20.212, de 6 de noviembre de 2023, se comete a AGESIC el diseño y desarrollo de una estrategia nacional de datos e inteligencia artificial basada en estándares internacionales, en los ámbitos público y privado. En dicho marco y como parte de dicha estrategia, se ha establecido un plazo de 180 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. A tal fin, la referida norma prevé que AGESIC pueda establecer grupos de trabajo, comités asesores y otros mecanismos de participación que incluyan las perspectivas de actores del sector público, del sector privado, de la academia y de la sociedad civil organizada.

Con fecha 30 de abril de 2024, AGESIC elaboró el documento de Bases para el desarrollo del informe previsto en el art. 74 de la Ley N° 20.212, participándose a diversas entidades públicas, entre ellas la Institución Nacional de Derechos Humanos y Defensoría del Pueblo.

En dicho marco, la INDDHH realizará los siguientes aportes al documento en cuestión, en el marco de sus cometidos y atribuciones institucionales de defensa, promoción y protección de los derechos humanos y, con el objetivo de aportar a la cuestión y dar respuesta a las preguntas planteadas en el informe como elementos de aporte para las entidades participantes.

El presente no implica un análisis de todos los puntos referidos en el extenso informe de que se ha dado cuenta, sino algunas cuestiones que el Consejo Directivo de la INDDHH considera más relevantes referir, sin perjuicio de la trascendencia de todos los aspectos referidos en el documento y de la posibilidad de, en ulteriores instancias, abordar otras cuestiones no referidas en el presente.

ii. Sobre la institucionalidad y gobernanza

Según se consigna en el documento remitido, uno de los primeros aspectos a analizar se relaciona con la institucionalidad y gobernanza de la IA y, en especial, la cuestión a la posición orgánico institucional de la entidad rectora en la materia.

En ese sentido, se cita como ejemplo el caso de la propia AGESIC, creada en virtud de la Ley N° 17.930 como un órgano desconcentrado de la Presidencia de la República y, posteriormente, la Ley N° 18.331, que creo la Unidad Reguladora y de Control de Datos Personales (URCDP) como un desconcentrado de AGESIC, siempre dentro del ámbito de la Presidencia de la República.

Se establecen también ejemplos de derecho comparado, tanto en Latinoamérica como en Europa, verificándose la existencia de entidades autárquicas

(que en nuestro derecho se traducirían en lo que el constituyente consideró como Entes Autónomos o Servicios Descentralizados) y entidades dependientes de Ministerios, funcionando como una suerte de secretarías técnicas, en una suerte de mecanismo asimilable al existente en nuestro país (con la salvedad de que en nuestro caso el vínculo es con la Presidencia). Se refiere finalmente sobre el punto al Reglamento Europeo, al caso norteamericano y la regulación existente actualmente en el Reino Unido.

Respecto al punto y en consideración de las previsiones de la Ley N° 20.212, por la que se compete a AGESIC y la URCDP la fijación de criterios generales sobre la materia (que abarcan incluso la materia de fiscalización), se considera que su ámbito de actuación debería, idealmente, ser situado fuera de la órbita de la Presidencia de la República (dejándose de lado las discusiones doctrinarias en la materia sobre el rol de la Presidencia en clave de nuestra Constitución y la enorme expansión en temáticas y cometidos que ha tenido ese sistema orgánico) y, en general, del propio Poder Ejecutivo, atento a que este último, en los hechos, es el sistema productor y usuario de mayor información y datos en nuestro país.

Tomando en consideración la trascendencia que cada día más tiene el manejo de datos, la información y la IA, el ideal debería ser la existencia de una entidad de control completamente autónomo, como en nuestro país la Constitución reconoce a los tres órganos de control, dotados además de potestad reglamentaria autónoma, como especialmente sucede con el Tribunal de Cuentas y la Corte Electoral.

Siendo ese escenario poco factible, atento a que implica una reforma constitucional, se plantean dos posibles caminos institucionales para la eventual institucionalización.

En primer término, una opción es la ubicación de esta agencia dentro del campo de actuación del Poder Legislativo, como una entidad autónoma e independiente, tal como sucede con la INDDHH, creada a partir de la Ley N° 18.446. El caso del Comisionado Parlamentario para el Sistema Carcelario si bien también pertenece a la órbita del legislativo, posee un rol de rendición directa al parlamento, que no sucede con la INDDHH y que tampoco debería suceder en el caso de una agencia como la indicada en materia de IA. Como fortaleza de este punto sin duda se encuentra el rol representativo que posee el marco de actuación del legislativo y, en especial, la separación clara de la actuación respecto del Poder Ejecutivo, con las particularidades antes señaladas.

La segunda opción factible y con fuertes antecedentes en nuestro derecho, sería la posibilidad de seguir el camino de otras entidades de control tales como URSEC, URSEA y JUTEP, que recientemente (en términos institucionales) se han transformado en lo que en derecho comparado se denomina entidades autárquicas y adoptado -en los tres casos- la forma de servicios descentralizados, aunque eventualmente podrían también adoptar la forma de Entes Autónomos, atento a que no se encuentran limitados por el art. 186 de la Constitución, tal como sucede con el rol de control que posee el BCU.

La forma de Servicio Descentralizado, que, como se indicó, parece ser el camino adoptado para las entidades de control, atento a la especificidad de sus cometidos y la recta aplicación de los principios de especialidad y especialización para los organismos públicos y, en particular, este tipo de entidades, retirándolas de la órbita de actuación jerárquica del Poder Ejecutivo (o la Presidencia de la República) e incluso adoptando una forma de designación jerárquica que excede los mandatos quinquenales de gobierno.

Sin perjuicio, naturalmente el control del sistema seguirá existiendo, atento a las características de la forma de actuación de los servicios descentralizados y los aspectos relativos a la tutela administrativa, estatuto funcional y previsión presupuestal en el marco del art. 220 de la Constitución. Este último extremo sin duda plantea uno de los retos más sustantivos, ya que la asignación presupuestal acorde, como se reconoce en el informe, es capital para la correcta actuación de este tipo de agencias de control.

iii. Otro de los aspectos reseñados en el informe guarda relación con el ejemplo de los fideicomisos de datos. Si bien claramente la figura del fideicomiso -recogido en nuestro país en la Ley N° 17.703- se orienta a la materia de bienes y finanzas (sea se trate de fideicomisos testamentarios, de administración, garantía y financieros), su aplicación al campo de los datos parece claramente innovadora.

Tomando en consideración ejemplos de derecho comparado -en especial la figura del trust del derecho anglosajón- y las bases sustantivas de la figura del fideicomiso, esto es, especialmente, la existencia de fideicomitentes, fiduciario y beneficiarios y, por otra parte, una serie de bienes o derechos fideicomitidos y un mandato, resulta capital que una regulación que viabilice este tipo de instrumentos deberá tener un sustento normativo legal, en aras de proteger los derechos de los titulares de datos y regular los roles de cada una de las partes, en especial el fiduciario, que preferentemente debería ser una entidad estatal (por ejemplo la agencia de control).

De la mano de ello, existen un conjunto importante de aspectos de regulación y control que legalmente deberán estar claramente establecidos, en particular las potestades de actuación de ese fiduciario respecto de los datos que manejen y los eventuales beneficiarios de estos datos recopilados.

En ese marco, la opción del fideicomiso, si bien no resulta descartable, sin duda implica un extenso desarrollo normativo que permita garantizar la seguridad de la información y la debida protección de los derechos de las personas.

iv. (…..)

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

Daniel Carranza
Secretario de Data Uruguay

1. ¿Cuáles son las recomendaciones específicas que podría realizar desde su experiencia para promover las líneas definidas en el presente documento?

Desde Data Uruguay analizamos el documento "Bases para el desarrollo del informe previsto en el art. 74 de la Ley N° 20.212" y destacamos la importancia de una adecuación de la normativa nacional para regular la inteligencia artificial (IA) en Uruguay según los estándares internacionales de derechos humanos más recientes.

Destacamos la importancia del trabajo de Agesic en cuanto al establecimiento de marcos éticos y normas de soft law a través de la Estrategia de IA para el ámbito público, aunque entendemos que esta tarea debe ser complementada con la actualización de la normativa nacional. Los aspectos que requieren una regulación más urgente se relacionan con la toma automatizada de decisiones a través de sistemas de inteligencia artificial, especialmente en la administración pública. Estas situaciones no solamente incluyen la toma de decisiones totalmente automatizadas sino que, también incluyen la interacción persona-máquina y el concepto de supervisión significativa (cuando los operadores actúan siendo conscientes de los sesgos o las limitaciones del sistema).

Con el objetivo de promover las líneas definidas en el presente documento entendemos que, luego de esta consulta, el Parlamento uruguayo debería considerar realizar una apertura de audiencia pública en la que nuestros legisladores puedan interactuar con empresas, academia y sociedad civil especializada, ya que se está legislando en el presente sobre estos temas en base a entendimientos muy superficiales de algunos de los desafíos de normar este tema y sus consecuencias..

Sugerimos un punteo de posibles aspectos a discutir en las instancias de audiencia pública sobre regulación de la IA propuesto, entre ellos:

- La determinación de cuáles son los usos de alto riesgo de vulneración de derechos individuales que ameritarían una regulación específica.
- El establecimiento de garantías básicas tales como: el derecho a la explicabilidad, trazabilidad, transparencia y auditabilidad algorítmica en sistemas con alto riesgo, aunque no traten datos personales o no estén alcanzados por la Ley de Protección de Datos Personales.
- La aplicación obligatoria de instrumentos para la evaluación de riesgos en determinados escenarios críticos que no involucren el uso de datos personales o en dónde las obligaciones de protección de datos personales no apliquen (como en seguridad pública o defensa).
- El etiquetado obligatorio de los contenidos sintéticos.
- La conceptualización del principio de la supervisión humana significativa.

Finalmente, entendemos que, si bien la Institución Nacional de Derechos Humanos y Defensoría del Pueblo es el órgano mandatado para realizar recomendaciones y orientaciones de política pública sobre derechos humanos al Parlamento, los miembros de esta Institución no cuentan con una masa crítica de conocimiento suficiente para poder cumplir con esta función de recomendación sobre IA. Por eso, sería deseable que se sugiera algún tipo de apoyo a la INDDHH para establecer convenios con la academia y la sociedad civil especializada en derechos digitales.

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?

En relación con el análisis desarrollado en torno a los artículo 13 y 16 de la Ley de Protección de Datos Personales en el punto “3.3 Diagnóstico preliminar en materia de IA y Derechos Humanos del documento”, resaltamos la importancia del derecho a impugnar decisiones automatizadas y de obtener información sobre “los criterios de valoración, los procesos aplicados y la solución tecnológica o el programa utilizados”. De cualquier forma, esta normativa resulta insuficiente y es necesario actualizarla para incluir estándares modernos como por ejemplo los estándares

sobre transparencia algorítmica[1] y supervisión humana significativa[2]. Estos mismos estándares podrían incluirse también a través de obligaciones impuestas a la administración pública a través de modificaciones en la Ley de Acceso a la Información Pública.

3. ¿Ha identificado potenciales mejoras o modificaciones a la regulación vigente que puedan colaborar en el desarrollo de la IA en Uruguay?

Reforma de la Ley N° 19.179 de formatos abiertos y software libre y su decreto reglamentario (Decreto N° 44/015)

Siguiendo la misma lógica de actualización de la normativa existente que propone la Agesic en el documento borrador, se sugiere implementar un sistema de apoyo para la toma de decisiones de adquisición de software o soluciones basadas en IA por parte de la administración pública introduciendo modificaciones en la Ley N° 19.179 de formatos abiertos y software libre y en su decreto reglamentario (Decreto N° 44/015). Esta ley es un instrumento que ya existe en nuestro ordenamiento jurídico desde antes del auge de la IA y que podría revisarse para dar prioridad a las soluciones de IA Abierta, evitando las cajas negras y fomentando las garantías de transparencia y explicabilidad. Entendemos que, además de revisar la Ley N° 19.179 y su decreto para impulsar la promoción preferencial de la utilización de modelos de IA Abierta, también debería incluirse un mecanismo de intervención por el que la Agesic determine el riesgo y asesore a los entes públicos para realizar evaluaciones de impacto de forma previa a la adquisición de soluciones basadas en IA, al menos para algunos sectores o usos clave (salud, seguridad pública o educación por ejemplo).

4. ¿Existen otros aspectos que no encuentra considerados y que deban analizarse?

Urgente regulación de la adquisición y uso de software de vigilancia por parte del Ministerio del Interior

Basta con realizar una búsqueda en prensa para constatar que, en los últimos años, el Ministerio del Interior viene adquiriendo de forma sostenida nuevas tecnologías para combatir el crimen. Muchas de estas adquisiciones utilizan potentes sistemas de IA ya sea para detectar disparos

[1] BID (2022), "Auditoría algorítmica para sistemas de toma o soporte de decisiones". Ver: https://publications.iadb.org/publications/spanish/document/Auditoria-algoritmica-para-sistemas-de-toma-o-soporte-de-decisiones.pdf

[2] EU AI Act. Ver: https://www.euaiact.com/key-issue/4

colocando micrófonos en la vía pública como para identificar a las personas basándose en patrones biométricos. Ninguna de estas tecnologías se encuentra debidamente regulada por ley bajo los estándares reclamados por las diferentes Relatorías del sistema internacional de derechos humanos.

El criterio del Comité de Derechos Humanos de la ONU en cuanto a la adopción de medidas de vigilancia es el siguiente: los gobiernos podrán establecer este tipo de medidas sobre sus ciudadanos siempre que 1) estén autorizadas por una ley nacional que sea accesible y precisa, 2) tengan un objetivo legítimo, y 3) que cumplan los criterios de necesidad y proporcionalidad. Hace ya 10 años que la Alta Comisionada de las Naciones Unidas para los Derechos Humanos advirtió que estos requisitos no se están cumpliendo[3], y que los Estados suelen usar sistemas de vigilancia sin leyes nacionales adecuadas, sin garantías procesales y sin suficiente supervisión. La Alta Comisionada señala "la preocupante falta de transparencia gubernamental asociada a las políticas, leyes y prácticas de vigilancia, que dificulta todo intento de evaluar su compatibilidad con el derecho internacional de los derechos humanos y asegurar la rendición de cuentas".

Compartimos la preocupación de La Alta Comisionada y entendemos que el informe que Agesic presente al Parlamento debería recomendar la regulación del uso de la IA con fines de vigilancia por parte del Ministerio del Interior con carácter urgente.

[3] El derecho a la privacidad en la era digital Informe de la Oficina del Alto Comisionado de las Naciones Unidas para los Derechos Humanos" A/HRC/27/37, párr. 48. Ver: https://documents.un.org/doc/undoc/gen/g14/068/74/pdf/g1406874.pdf?token=BBP8Fg822XkzlZAS4c&fe=true

Datysoc
LABORATORIO DE DATOS Y SOCIEDAD

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

Documento elaborado por Patricia Díaz
Co-cordinadora del Laboratorio de Datos y Sociedad | Datysoc

Cuestiones previas

Realizamos algunas sugerencias relacionadas con la estructura del documento:

- Dado que será un documento de una extensión considerable, sugerimos generar un índice con hipervínculos para mejorar su navegabilidad y usabilidad.
- Sugerimos colocar al final de cada línea un punteo con un resumen en el que figuren de forma específica y clara las recomendaciones de regulación.

Autorización: se autoriza al equipo de Agesic a copiar, adaptar y/o incorporar cualquier parte de este documento en la versión final que se presentará al Parlamento, sin necesidad de cita.

1. ¿Cuáles son las recomendaciones específicas que podría realizar desde su experiencia para promover las líneas definidas en el presente documento?

Expresamos que, de forma genérica estamos de acuerdo tanto con el análisis planteado como con los aspectos priorizados y con los lineamientos generales de la propuesta que se presenta en el borrador “Bases para el desarrollo del informe previsto en el art. 74 de la Ley N° 20.212”. Aunque existe un aspecto central que el documento omite abordar de forma explícita y clara, se trata de una pregunta que seguramente varios legisladores tengan en mente: ¿Necesitamos una regulación general de la IA o debemos regular determinados usos de la IA o su uso en determinados sectores?

Entendemos que aún no están dadas las condiciones para una regulación generalista basada en la determinación de diferentes niveles de riesgo, la asignación de obligaciones diferenciadas para cada uno de esos niveles de riesgo y en la creación de nueva institucionalidad especializada para la IA. Hace falta entender mejor el panorama para regular, por eso **proponemos recomendar a los parlamentarios la creación de un foro para promover las líneas definidas en el presente documento, detectar otras prioridades a nivel nacional y formular recomendaciones por parte de diferentes actores sociales para una regulación adecuada y sostenible**.

De forma paralela a esta discusión, **sugerimos centrar los actuales esfuerzos regulatorios en la actualización del cuerpo normativo nacional vigente y en la regulación de los actuales usos de la IA por parte del gobierno que impliquen alto riesgo**.

De esta forma, y sin descartar la posible existencia de otros emergentes, destacamos al uso policial de la IA como un emergente de alto riesgo que amerita urgente regulación y proponemos la creación de una nueva línea: "*Linea uso de IA con fines de vigilancia policial y como prueba en el proceso penal*" (ver pregunta 4).

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?

A continuación presentamos algunos aspectos que no han sido considerados en el documento y que entendemos deberían ser agregados:

Apartado "3. Línea Derechos Humanos"

Proponemos agregar las siguientes consideraciones en el apartado "**3.3 Diagnóstico preliminar en materia de IA y Derechos Humanos** ":

Sobre la Ley 18331 de Protección de Datos Personales (LPDP) y el Decreto 64/020.

Estamos de acuerdo con las apreciaciones del documento borrador en cuanto a que se deberían revisar los Arts. 13 y 16 de la LPDP. Entendemos que estas disposiciones no son suficientes por los siguientes motivos:

1) Derecho a la impugnación de valoraciones personales basadas en tratamiento automatizado de datos (Art. 16) sólo opera en el contexto de datos personales, aunque existe una infinidad de contextos en los que no opera. Un ejemplo ilustrativo: el mecanismo previsto en el Art. 16 no podría utilizarse para impugnar y obtener información de un sistema de IA que analice los datos de contaminación del agua y del aire en el que se entienda que está en riesgo la salud de un conjunto de ciudadanos.
2) El Art. 16 sólo habilita la impugnación de decisiones "**cuyo único fundamento** sea un tratamiento de datos personales". Basta con "colocar un humano en el medio" y decir que el sistema "asesora" pero que el humano toma la decisión para que caiga la aplicación del artículo. Frente a los conocidos "sesgos de automatización"[1] debería considerarse incluir alguna disposición que defina el concepto de "supervisión humana significativa"

[1]Informe "Hacia una supervisión significativa de los sistemas automatizados de toma de decisiones" (2022). Digital Future Society. Disponible en: https://digitalfuturesociety.com/es/report/hacia-una-supervision-significativa-de-los-sistemas-automatizados-de-toma-de-decisiones/

incluyendo aspectos mínimos requeridos como la formación de los actores que operan el sistema entre otros factores.

3) No debemos olvidar que los mecanismos de la LPDP y del Decreto 64/020 no consideran la protección de datos personales como un derecho colectivo, por lo que, en base a estas disposiciones, tampoco podrá exigirse a ninguna institución pública o privada que rinda cuentas sobre parámetros básicos de explicabilidad de sus sistemas automatizados frente a un riesgo potencial sobre los derechos fundamentales.
4) En el Decreto 64/020 los sujetos obligados no tienen obligación de publicar sus evaluaciones de impacto, sólo están obligados a compartirlas con la URCDP si de la evaluación surge un riesgo potencial y significativo (Art. 7).
5) Los Arts. 13 y 16 de la LPDP no especifican cuáles son los requisitos exigidos para que se configure la explicabilidad y no exige trazabilidad ni auditabilidad, por lo que se satisface esta obligación cuando la propia administración presenta explicaciones de forma unilateral.
6) Se necesitan normas que garanticen un mínimo de **transparencia, interpretabilidad y auditabilidad algorítmica** (Stoyanovich, Julia 2020)[2] entendiendo que:
    - **La transparencia algorítmica no es sinónimo de liberar el código fuente**,la publicación del código fuente ayuda, pero a veces es innecesaria y a menudo insuficiente. En algunos casos, la exigencia de liberar el código fuente puede resultar excesiva o lesionar derechos.
    - **La transparencia algorítmica requiere transparencia de datos**, la explicabilidad sólo puede lograrse en contexto de datos, los datos que se usan para el entrenamiento y testing, los datos que se van a usar para la implementación y validación del sistema (datasets de referencia), datos sobre performance y precisión del sistema. La transparencia de datos es necesaria para todos los sistemas automatizados, no solo para sistemas basados en *Machine Learning*.
    - **La transparencia de datos no es sinónimo de hacer públicos todos los datos**, deben liberarse los datos siempre que sea posible; en caso de no ser posible (por cuestiones de protección de datos, confidencialidad, propiedad intelectual, por ejemplo) también se puede: publicar las metodologías de selección o recopilación, acudir a conjunto de datos sintéticos, publicar resúmenes estadísticos o muestra, los datos que se utilizaron para el preprocesamiento, la procedencia de los datos e información sobre su calidad/representatividad y las fuentes conocidas de sesgo relevadas.

[2] Stoyanovich, Julia (2020). TransFAT. Translating fairness, accountability, and transparency into data science practice. Disponible en: https://pdfs.semanticscholar.org/061f/de41f92e6bd408b5722428bdcc8b2a7d0858.pdf

- **La transparencia procesable requiere interpretabilidad o comprensibilidad**, en definitiva, se trata de explicar los supuestos y efectos del sistema (no solo los detalles de operación) y de involucrar al público - técnico y no técnico.

Sobre la Ley 18381 de Acceso a la Información Pública (LAIP).

La LAIP debería incluir una disposición que introduzca el **derecho a ser informado sobre qué decisiones se toman de forma automatizada o con apoyo de un sistema automatizado por parte de la administración pública** y sobre cómo funcionan estos sistemas (tomando en cuenta lo expresado en el apartado anterior en relación a la transparencia, interpretabilidad y auditabilidad algorítmica y la conceptualización de "intervención humana significativa").

También debería incluirse una disposición que garantice el derecho a la interacción humana y presencial con la administración pública.

Apartado "4. Línea propiedad Intelectual"

Proponemos agregar las siguientes consideraciones en el apartado "**4.1 Consideraciones preliminares**":

> Actualmente, la mayoría de las actividades de desarrollo IA requieren el uso masivo de grandes volúmenes de datos y suelen incluir el uso de miles de imágenes, audios, textos, etc. protegidos por derechos de autor con fines de análisis computacional o entrenamiento de modelos. Entre estos usos podemos encontrar la aplicación de técnicas de minería de texto y datos (como el crowling, scraping y parsing), la creación de copias técnicas o efímeras con fines de entrenamiento de modelos, entre otras. De esta forma, para incentivar la innovación y generar un entorno jurídico seguro para investigadores y desarrolladores locales, se hace necesario incluir en las leyes de derechos de autor una excepción que habilite el uso de obras con fines de análisis computacional. Esta excepción debería incluir como restricción la condición de que esos usos no compitan con la normal explotación de las obras y que no dañen de forma injustificada los intereses de los autores.
>
> Tomando en cuenta que el software y las bases de datos también están protegidas por derechos de autor y por medidas de protección tecnológicas, será necesario regular de forma clara las relaciones entre los derechos de autor, el secreto comercial y la auditabilidad de los sistemas. La auditabilidad de los sistemas de IA es de especial interés público tanto por razones de ciberseguridad como de transparencia y explicabilidad y, muchas veces, requiere la vulneración de medidas de protección tecnológica para el ingreso

a los sistemas, la realización de copias de prueba o las actividades de ingeniería inversa.

Proponemos agregar las siguientes consideraciones en el apartado "**4.2 Selección de antecedentes internacionales**":

En cuanto a las excepciones al derecho de autor con fines de análisis computacional, el antecedente más reciente en el contexto de la OMPI es el informe sobre "Los retos de los centros de investigación y los fines de la investigación en relación con los derechos de autor" (2023)[3]. Dicho informe fue solicitado a Raquel Xalabarder por el Comité de Derechos de Autor y Conexos (SCCR/OMPI) y en él la autora expresa:

> *"El papel de la lectura no humana (mecánica), como el análisis de inteligencia artificial (IA), está cobrando cada vez más importancia dentro de las metodologías de investigación. La minería de textos y datos (TDM) ha ganado protagonismo gracias a las tecnologías digitales. Gracias a las herramientas de TDM, los investigadores extraen información de una gran variedad de obras protegidas, desde trabajos académicos hasta música y publicaciones de prensa*." (traducción nuestra)

En ese mismo informe encontramos un Anexo con ejemplos de normas nacionales que contienen este tipo de excepciones al derecho de autor para actividades de investigación con fines de análisis computacional que ya están presentes en casi todas las legislaciones del Norte Global.

En cuanto a las excepciones al derecho de autor y a las medidas de protección tecnológica con fines de auditabilidad de los sistemas encontramos el informe del Grupo de Trabajo sobre Seguridad en la Economía Digital de 2022 de la OCDE[4]. En este informe se expresa que "*la ley de derechos de autor puede infringirse cuando la información divulgada contiene partes del código de software protegido por derechos de autor. Dicha protección de derechos de autor podría restringir el intercambio de información sobre vulnerabilidades con el proveedor original, lo que dificulta la implementación de las DCV-Difusión Coordinada de Vulnerabilidades- en muchos casos.*" En el documento se explica que la falta de actualización de las excepciones al derecho de autor y a las medidas de protección tecnológica implican riesgos legales para los auditores e investigadores de seguridad digital, y también se expresa que estas normas son usadas para amenazar con procedimientos jurídicos por parte de los propietarios del software que se pretende investigar.

[3] Xalabarder, Raquel (2023). "Los retos de los centros de investigación y los fines de la investigación en relación con los derechos de autor". Disponible en: https://www.wipo.int/meetings/es/doc_details.jsp?doc_id=621815

[4] OECD (2022). OECD Policy Framework on Digital Security. Disponible en: https://www.oecd.org/publications/oecd-policy-framework-on-digital-security-a69df866-en.htm

Proponemos agregar las siguientes consideraciones en el apartado "**4.3 Diagnóstico preliminar en IA y Propiedad Intelectual**":

> La Ley de Derechos de Autor de Uruguay (Ley 9.739) no prevé excepciones al derecho de autor (ni al régimen de medidas de protección tecnológica) que habiliten el correcto desarrollo de las actividades de análisis computacional ni de auditorías, ya sea con fines de seguridad o con fines de explicabilidad. Es por eso que resulta necesario incluir una nueva excepción en el Art. 45 de la Ley de derechos de autor (Ley 9739) que habilite el uso de obras con fines de análisis computacional. También se sugiere agregar una excepción al derecho de autor (y a las medidas de protección tecnológica) para posibilitar el ingreso, copia y análisis de los sistemas con el fin exclusivo de permitir instancias de auditabilidad cuando un juez u otra ley así lo requiera. Estas excepciones deberán explicitar que quedan estrictamente prohibidos los usos competitivos o que perjudiquen injustificadamente al autor o titular de los derechos sobre las obras.

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?

A continuación se propone la inclusión de una nueva línea que constituye el mayor **emergente de uso de IA con alto riesgo de vulneración de los derechos fundamentales en Uruguay**, por lo que debería ser analizada de forma independiente y **amerita urgente regulación**:

Linea uso de IA con fines de vigilancia policial y como prueba en el proceso penal.

Consideraciones preliminares:

El uso de la IA con fines de prevención del delito y seguridad pública pone en riesgo los derechos de los ciudadanos por su potencial de discriminación y por tratarse de una tecnología altamente intrusiva, más allá de los posibles sesgos o fallos que impliquen riesgos de discriminación. Algunas de las preocupaciones

principales en torno al uso de estos sistemas por parte de la policía y en la justicia criminal son[5]:

La vulneración de la presunción de inocencia. El derecho a la presunción de inocencia en los procesos penales es un derecho humano fundamental. Sin embargo, el creciente uso de la IA en el ámbito de la justicia penal, y más especialmente el uso de vigilancia biométrica a distancia y de ciertos tipos de software policial predictivo, plantea interrogantes sobre el alcance de este derecho y sobre cómo deben construirse y utilizarse los sistemas de IA para protegerlo.

La preservación de la igualdad procesal y el debido proceso. Una de las principales preocupaciones planteadas en los estudios sobre determinados sistemas de IA es que resultan inaccesibles para un escrutinio adecuado por parte de los acusados y sus abogados. Esto tiene graves implicaciones para el principio de igualdad de medios procesales y el derecho a un proceso contradictorio, porque sin información sobre cómo se toma una decisión, es difícil prever cómo pueden los acusados cuestionar la exactitud y legalidad de la decisión. En este sentido, uno de los principales problemas que impiden la impugnabilidad suficiente de los sistemas de IA en los procesos penales es la falta de notificación. Si a una persona no se le notifica que ha sido objeto de una decisión automatizada por parte de un sistema de IA, no tendrá la posibilidad de impugnar dicha decisión, ni la información en la que se basó la decisión. A su vez, el fenómeno de las cajas negras es otro factor de riesgo en la aplicación de la IA ya que, para preservar el debido proceso y el derecho de igualdad procesal, el sistema y sus resultados deberán ser necesariamente explicables y libres de sesgo de forma demostrable.

La falta de formación obligatoria de los actores del sistema judicial: la formación de los actores del sistema judicial es imprescindible para determinar la admisibilidad y realizar una correcta valoración de los medios de prueba digital, además de dar sentido al concepto de “intervención humana significativa” en el contexto judicial. La formación no sólo es necesaria para los usuarios primarios de los sistemas de IA, como jueces y policías que los utilizan para fundamentar sus propias decisiones. La formación también debe estar disponible para los abogados de la defensa penal, para que estén en mejores condiciones de impugnar los sistemas de IA, cuando sea necesario.

Selección de antecedentes internacionales

El Relator Especial sobre la promoción y protección del derecho a la libertad de opinión y de expresión de la ONU en su informe “La vigilancia y los derechos Humanos” (2019)[6] propone medidas drásticas. Hace un llamado urgente a

[5] Policy Paper: Regulating Artificial Intelligence for Use in Criminal Justice Systems in the EU (2022). Fair Trials. Disponible en: https://www.fairtrials.org/app/uploads/2022/01/Regulating-Artificial-Intelligence-for-Use-in-Criminal-Justice-Systems-Fair-Trials.pdf

[6] Relator Especial sobre la promoción y protección del derecho a la libertad de opinión y de expresión. «Informe sobre la vigilancia y los derechos humanos», A/HRC/41/35. (Asamblea General

establecer "*una moratoria inmediata sobre la venta y la transferencia a nivel mundial de los instrumentos que utiliza el sector de la vigilancia privada hasta que se establezcan estrictas salvaguardias de los derechos humanos en la regulación de esas prácticas y se pueda garantizar que los gobiernos y los agentes no estatales van a utilizar esos instrumentos de un modo legítimo*." y también solicita "*una regulación más rigurosa de las exportaciones de equipos de vigilancia y unas restricciones más estrictas de su utilización*".

En el "Reglamento de Inteligencia Artificial de la UE" (Art. 5 del Capítulo II "Prácticas de Inteligencia Artificial prohibidas")[7] **se prohíbe** el uso para aplicaciones policiales o de orden público de la identificación biométrica en tiempo real en lugares accesibles al público por parte de las fuerzas y cuerpos de seguridad, **salvo** en estos casos: búsqueda de víctimas potenciales de delitos; prevención de amenazas específicas y sustanciales sobre infraestructuras críticas o sobre personas físicas; prevención de ataques terroristas; y persecución de crímenes punibles con más de cinco años de privación de libertad. Antes será obligatorio valorar la probabilidad y escala del daño posible sin esos sistemas y del daño que esos podrían ocasionar; mediara **autorización judicial** o administrativa vinculante; y se impondrán limitaciones temporales, geográficas y personales.

Otro antecedente importante es la "Resolución del Parlamento Europeo, de 6 de octubre de 2021, sobre la inteligencia artificial en el Derecho penal y su utilización por las autoridades policiales y judiciales en asuntos penales" [8]. Esta resolución aborda el uso de la inteligencia artificial (IA) en el ámbito del derecho penal, centrándose en su aplicación por parte de las autoridades policiales y judiciales. El documento subraya la necesidad de establecer un marco regulatorio robusto que garantice el respeto de los derechos fundamentales, la privacidad y la protección de datos. Además, enfatiza la importancia de la transparencia, la supervisión humana y la responsabilidad en el uso de sistemas de IA para prevenir sesgos y discriminaciones. La resolución también insta a que se realicen evaluaciones de impacto y auditorías regulares de estos sistemas para asegurar su conformidad con los estándares éticos y legales de la Unión Europea.

En esta Resolución, el Parlamento Europeo destaca el potencial de la IA para mejorar la eficiencia y eficacia en la lucha contra la delincuencia, pero también advierte sobre los riesgos asociados, como la posibilidad de errores judiciales y la

de las Naciones Unidas, 28 de mayo de 2019). Disponible en:. https://www.undocs.org/es/A/HRC/41/35

[7] Reglamento de Inteligencia Artificial de la Unión Europea aprobado por Resolución legislativa del Parlamento Europeo, de 13 de marzo de 2024 Disponible en: https://www.europarl.europa.eu/doceo/document/TA-9-2024-0138_ES.pdf

[8] Resolución del Parlamento Europeo, de 6 de octubre de 2021, sobre la inteligencia artificial en el Derecho penal y su utilización por las autoridades policiales y judiciales en asuntos penales (2020/2016(INI)). Disponible en: https://www.europarl.europa.eu/doceo/document/TA-9-2021-0405_ES.html

violación de derechos humanos. La resolución propone la creación de un marco legal específico para el uso de la IA en el ámbito penal, que incluya directrices claras sobre la recopilación y el procesamiento de datos, así como medidas para garantizar la equidad y la no discriminación. Además, recomienda que las autoridades y profesionales del derecho reciban formación adecuada sobre el uso y las implicaciones de la IA, asegurando así una aplicación justa y segura de estas tecnologías en el sistema judicial.

Diagnóstico preliminar

El Ministerio del Interior ha venido construyendo un ecosistema de vigilancia automatizada en apoyo al cumplimiento de sus cometidos basada tanto en IA como en otro tipo de sistemas. Este ecosistema no ha sido acompañado por la debida regulación ni por criterios de transparencia proactiva que aporten confianza sobre su funcionamiento. No existe ninguna regulación relacionada con el uso policial de los sistemas recientemente adquiridos por el Ministerio del Interior. Por ejemplo, el de reconocimiento facial automatizado, el software UCINET (software de inteligencia sobre fuentes abiertas como redes sociales), el sistema ShotSpotter (sistema que implica la colocación de micrófonos en las calles para que una IA detecte disparos) o inclusive un software de analítica de cámaras para "determinar conductas sospechosas que puedan advertir al policía antes de que se produzca el delito".

En Uruguay, el control del uso de las bases de datos personales utilizadas en las actividades de "seguridad pública, la defensa, la seguridad del Estado y sus actividades en materia penal, investigación y represión del delito" no están alcanzadas por las obligaciones que establece la Ley 18331 de Protección de Datos Personales (LPDP Art. 3 Lit. B y Art. 25)[9].

Con respecto al software de Reconocimiento Facial Automatizado (RFA) que el Ministerio del Interior adquirió en febrero de 2020 vía licitación pública, resaltamos que esta adquisición se encuentra relacionada con la aprobación de la creación de una base de datos de identificación facial para su tratamiento con fines de seguridad pública a cargo de la Secretaría del Ministerio del Interior (arts. 191 y 192 de la Ley de Presupuesto 2020). De esta forma se habilita el uso de las fotografías de rostros (e información asociada a ellas) de las cédulas de identidad y los pasaportes de la base de la Dirección Nacional de Identificación Civil (DNIC) para crear una base biométrica con una finalidad diferente a la de identificación. Son muchas las cuestiones que surgen de esta contratación y habilitación masiva para el uso de

[9] "No obstante, cabe indicar que, aun en los casos indicados en el párrafo anterior, se ha interpretado por parte de la URCDP que igualmente resultan aplicables con carácter general los principios de la protección de datos personales" Ver consulta al Consejo Ejecutivo de la URCDP publicada en: Informe "Fuera de Control. Uso policial del reconocimiento facial automatizado en Uruguay". Datysoc (2022), pag. 49. Disponible en: https://datysoc.org/wp-content/uploads/2022/03/Informe-reconocimiento-facial-automatizado-Uruguay-2022-Datysoc.pdf

datos biométricos de toda la población ¿Con qué fines exactos es que se contrató el sistema?, ¿Quién autoriza el uso del sistema de RFA?, ¿Cómo se auditará el uso del sistema?, ¿Cómo se controlará el acceso al sistema?, ¿Cómo debe proceder un oficial ante un match biométrico en los diferentes contextos de uso?, ¿Cuándo puede aceptarse un match biométrico como prueba?, ¿Cómo se valorará esta prueba?, ¿Cómo se abordará la posibilidad de sesgos en el sistema?, ¿Cuándo y cómo se informará al imputado de la existencia de este tipo de prueba?, ¿Cómo se abordarán las diferencias entre un match biométrico en ambiente controlado y uno en ambiente no controlado?, ¿Cómo se eliminarán estos datos personales cuando ya no sean necesarios? Nada de esto se ha definido aún y la mayoría de estas decisiones **deberían fijarse a través de normas de rango legal precisas y públicamente accesibles**.

También vale la pena destacar que ni en el Código del Proceso Penal o en la Ley de Procedimiento Policial contamos con ninguna regulación sobre admisibilidad o valoración de la prueba digital, ni con protocolos públicos sobre el uso de la IA adquirida por el Ministerio del Interior, ni con la formación de los actores judiciales en torno al funcionamiento de esta IA.

Recomendaciones regulatorias sobre el uso policial de la IA

Siguiendo las recomendaciones de la Relatoría de Libertad de Expresión de la ONU, se sugiere imponer una moratoria en la adquisición de software de vigilancia hasta que no exista una base legal que regule adecuadamente el ecosistema de vigilancia policial.

Con el objetivo de establecer una regulación estricta sobre su uso y brindar garantías contra los actos discriminatorios y contra su uso abusivo o arbitrario deberían introducirse las modificaciones necesarias en el Código del Proceso Penal y en la Ley de Procedimiento Policial para regular el tema de forma adecuada, incluyendo:

- La obligación de realizar un análisis de impacto (en lo posible público) sobre los derechos fundamentales antes de adquirir soluciones de IA con fines de vigilancia, así como conocer y declarar de antemano los fines exactos para los que se contrata.
- Establecimiento de líneas rojas en cuanto a qué usos están estrictamente prohibidos a la policía y qué usos requieren orden judicial,
- La posibilidad de exigir la auditabilidad y explicabilidad algorítmica, la trazabilidad, protocolos de control de acceso y la descripción de responsabilidades detalladas sobre quienes usan estos sistemas de vigilancia.
- El entrenamiento adecuado de los funcionarios policiales, jueces y fiscales sobre el funcionamiento y limitaciones del sistema mediante una certificación obligatoria.

Recomendaciones específicas relacionadas con vigilancia biométrica y reconocimiento facial:

- La prohibición del enrolamiento masivo de toda la población en el sistema de reconocimiento facial adquirido por el Ministerio del Interior. Esto implica la derogación de los arts. 191 y 192 de la Ley de Presupuesto 2020, estos artículos violan el principio de presunción de inocencia.
- La prohibición del uso de vigilancia biométrica en tiempo real y sin orden judicial en espacios públicos.
- Los mecanismos obligatorios de análisis de impacto y de evaluación de riesgo junto con mecanismos de rendición de cuentas y seguimiento.
- Regulación específica de la admisibilidad, valoración y diligenciamiento de los matches biométricos como métodos de investigación y como prueba digital.

APORTE DE LA COMISIÓN DE DERECHO INFORMÁTICO Y TECNOLÓGICO DE LA ASOCIACIÓN DE ESCRIBANOS DEL URUGUAY.

Consulta: Bases para la discusión de contenidos del informe preliminar previsto en el art. 74 de la Ley No. 20212 (AGESIC)

1. ¿Cuáles son las recomendaciones específicas que podría realizar desde su experiencia para promover las líneas definidas en el presente documento?

En cuanto a la gobernanza, una definición primaria, debería ser si resulta necesaria que la normativa sea general o sectorial, dado que existen sectores con una alta sensibilidad institucional, social y económica. En ambos casos y tal como sucede con el Reglamento de Inteligencia Artificial de la Unión Europea, sería conveniente enfocarlo desde los riesgos que podría provocar, así como en la asignación y distribución de responsabilidades por daños (dada la multiplicidad de actores que pueden participar) para garantizar reparaciones equitativas a las personas perjudicadas.

Será un desafío, resolver el tema de asignación de responsabilidades por el uso de la IA, en un sistema donde puede no estar radicado en Uruguay, pero cuyas consecuencias serán soportadas en nuestro país.

En materia judicial, entendemos que puede resultar recomendable “utilizar sistemas de IA de "caja blanca", que se basan en técnicas que sirven para realizar predicciones, clasificaciones y detecciones inteligentes que presentan

beneficios enormes a la tarea judicial y a la transformación digital de las organizaciones, sin el riesgo de inexplicabilidad de las cajas negras"[1]

El sistema “PretorIA” creado por el Laboratorio de Innovación e Inteligencia Artificial de la Facultad de Derecho de la Universidad de Buenos Aires (UBA IALAB), sistema predictivo desarrollado para ser utilizado por la Corte Constitucional de Colombia, puede ser altamente recomendable

“PretorIA combina funcionalidades basadas en sistemas expertos y técnicas de *machine learning* (aprendizaje automático) de caja blanca”[2]

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?

Para poder determinar estos criterios y a través de ellos poner la IA al servicio del ciudadano y lograr un mayor bienestar social se debería pensar, como país, cuáles son los límites que estamos dispuestos a establecer para los diferentes desarrollos de IA y así regularlos.

Establecer las correspondientes evaluaciones de impacto de un desarrollo IA para minimizar los riesgos sobre los derechos humanos.

---

[1] Tratado de inteligencia artificial y derecho : tomo II / Juan Gustavo Corvalan... [et al.] ; dirigido por Juan Gustavo Corvalan. - 2a ed. - Ciudad Autónoma de Buenos Aires : La Ley, 2023. Libro digital, Book "app" for Android Archivo Digital: descarga y online ISBN 978-987-03-4642-5

[2] Obra citada

En estos temas se evaluará tomar como base el reciente Reglamento UE de IA

3. ¿Ha identificado potenciales mejoras o modificaciones a la regulación vigente que puedan colaborar en el desarrollo de la IA en Uruguay?

En el apartado 3.3. "Diagnóstico preliminar en materia de IA y Derechos Humanos" del documento puesto a consulta se destacan "7 aspectos centrales, vinculados a los puntos mencionados por el Alto Comisionado de las Naciones Unidas para los Derechos Humanos, y detallados arriba…"

En este informe nos detendremos en dos de las preguntas allí explicitadas:

1.- ¿Cuáles son los alcances de la transparencia y explicabilidad a ser garantizados en el marco del desarrollo de sistemas de IA centrados en la persona?

Respondiendo a esta pregunta decimos que si bien en nuestra normativa vigente, podríamos aplicar la ley No. 18331 en lo que respecta a datos personales, utilizando los principios de finalidad y previo consentimiento informado, dado el impacto que la IA tanto en su desarrollo como en su aplicación tiene sobre la persona y la sociedad ellos deberían ser reforzados en su definición y aplicación. El previo consentimiento informado debería establecer claramente la información que se le debe entregar ya sea al consumidor de un servicio IA o a quien compra un producto IA. (juegos para niños, gafas, chat GPT) No es suficiente lo establecido por art.9 ley No. 18331.

Se llega a esta conclusión por el tipo de datos personales que se pueden llegar a utilizar en el entrenamiento de la IA, los que pueden ser datos biométricos y datos sensibles los cuales pueden ser vulnerados al momento de su tratamiento. En cuanto al principio de finalidad su definición más explícita y enfocada al desarrollo de la IA ayudaría a una mayor transparencia.

“Entendemos imprescindible que un esquema regulatorio” ponga su centro en el ser humano y “contemple la obligatoriedad de las empresas de explicitar dónde y cómo se utilizan las tecnologías de inteligencia artificial y las técnicas automatizadas en sus plataformas, servicios y aplicaciones, asimismo, el deber de prevenir y asegurar que los equipos y sistemas de IA reflejen actitudes no discriminatorias y eviten sesgos”[3]

“En materia de scoring realizados por IA, no se podrá considerar datos personales que no formen parte del elenco de datos para cuya finalidad se hace el estudio.

El resultado del scoring deberá contar con todos los principios de la IA, a los efectos de ser debidamente explicado por un ser humano al afectado por el mismo

No se podrá utilizar datos sintéticos en el ámbito notarial o contractual.

---

[3] Tratado de inteligencia artificial y derecho : tomo II / Juan Gustavo Corvalan... [et al.] ; dirigido por Juan Gustavo Corvalan. - 2a ed. - Ciudad Autónoma de Buenos Aires : La Ley, 2023. Libro digital, Book "app" for Android Archivo Digital: descarga y online ISBN 978-987-03-4642-5 1. Inteligencia Artificial. 2. Derecho. I. Corvalan, Juan Gustavo, dir. CDD 346.002

En las políticas de privacidad se deberá explicitar si se utilizan datos sintéticos y como se utilizan”[4]

4. ¿Existen otros aspectos que no han sido considerados y que deban analizarse?

Se deberá preveer una nueva brecha tecnológica, mucho más profunda que las anteriores, donde muchas personas quedarán al costado del camino con el peligro de caer en situaciones de vulnerabilidad.

Por otra parte “adaptabilidad y la adquisición de nuevas habilidades siempre han sido imperativas en el cambiante mundo del derecho. Sin embargo, en la era digital y la inteligencia artificial, estas habilidades evolucionan y deben adaptarse a los retos y oportunidades que ofrecen las nuevas tecnologías

“Un ejemplo de ello es el *legal prompt engineering*, una habilidad emergente que se refiere a la capacidad de interactuar y comunicarse eficazmente con agentes conversacionales basados en IA, como es el caso de ChatGPT.

En ese entendimiento, veremos que el *legal prompt engineering* es una habilidad crucial que abarca y mejora varios aspectos de la práctica jurídica en la era digital, no solamente en la búsqueda de información sino también en la confección escritos legales, la argumentación de casos de manera efectiva o el diseño de estrategias jurídicas mejoradas a través de la interacción precisa y efectiva con agentes conversacionales sofisticados. Esta adaptación

[4] Ob.citada

no solo es necesaria, sino que puede ofrecer grades oportunidades para acentuar el camino de la reconversión y optimizar el curso de práctica legal y el desarrollo de la justicia inteligente en la era de las máquinas”[5]

Esc. Elisabeth Bouvier Villa
Esc. Javier Wortman

[5] Obra citada

En este documento reunimos los aportes del Grupo Asesor IA para presentar a al Poder Legislativo previsto en el art. 74 de la Ley N° 20.212 a cargo de Agesic.

Los aportes son realizados por el Grupo Asesor en Inteligencia Artificial de la Cámara Uruguaya de Tecnologías de la Información

Institucionalidad y Gobernanza *(Ref. Capítulo 2 del documento)*
El objetivo de esta línea es la determinación de los aspectos fundamentales para asegurar una adecuada institucionalidad de la Inteligencia Artificial en nuestro país.
Comentarios
El documento muestra que la institucionalidad existente es adecuada para tratar los desafíos planteados. Si que es fundamental contar con grupos asesores con participación de todos los actores, que funciones de forma regular.
El concepto de grupos de trabajo es claro, pero los mismos deberían tener mayor injerencia en la definición de políticas, que son articulados, gestionados y liderados por AGESIC. Sería bueno darles mayor transcendencia y poder de decisión que un grupo de trabajo. Se comparte el rol de la URDCDP Agesic debe impulsar el desarrollar sistemas de inteligencia artificial pero no será conveniente que los desarrolle. También me parece adecuado definir criterios y mecanismos de fiscalización de que son bien aplicados los criterios.
En el camino para la incorporación de la IA como un aspecto central para creación de soluciones innovadoras, es un camino que implica tomar riesgos (como toda innovación). Cuando una solución es desarrollada para dar un servicio público (y en muchos casos en temáticas sensibles), el impacto del fracaso es mayor, y esto puede llevar a que la innovación se enlentezca por no tomar estos riesgos. Se debe incorporar dentro de la gobernanza mecanismos para resolver este tipo de “conflictos”.
Buscar evaluar las soluciones desarrolladas por el ecosistema uruguayo, bajo estándares internacionales a nivel de impacto de la solución, calidad de datos, etc de tal forma que las soluciones que sean evaluadas localmente bajo este estándar pueden ser “exportadas” para otros países donde se utilice en el mismo estándar.

Derechos Humanos *(Ref. Capítulo 3 del documento)*
El objetivo de esta línea es plantear cuales son los riesgos que en el marco del desarrollo de una política publica 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.
Comentarios

Es importante identificar los casos a los cuales se está aplicando. Se debería ver diferentes ciencias para evaluar el impacto en los DH. Sería aconsejable armar un comité o grupo de trabajo específico de este tema y las implicancias que pude tener a largo plazo.
El abordaje de clasificación de riesgos, si bien es apropiado, exige mucha cautela para que no constituya una barrera a la innovación y a la inversión en IA. Las definiciones tienen que ser suficientemente precisas para dar garantías jurídicas y suficientemente flexibles para adaptarse a los contextos. Por ejemplo: no es lo mismo un sistema de reconocimiento facial para hacer vigilancia a los ciudadanos que un sistema de reconocimiento facial para encontrar niños desaparecidos.
Tal como se describe en el documento de Agesic, el marco legal e institucional actual ya es apropiado para el manejo de la mayoría de los riesgos potenciales. Actualizaciones hechas a la ley de protección de datos personales ya previenen algunos de los problemas potenciales.

Propiedad intelectual *(Ref. Capítulo 4 del documento)*
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. *SIN COMENTARIOS.*

Infraestructura y Ciberseguridad *(Ref. Capítulo 5 del documento)*
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.
Comentarios
La infraestructura y la arquitectura tecnológica debe acompañar a la estrategia del país en políticas de IA. El procesamiento de los algoritmos y el control sobre la misma resulta clave para generar las capacidades a nivel país y tener la independencia para impulsar esta tecnología. A nivel de Infraestructura hay que diferenciar la misma con la disponibilidad para brindar servicios y otras para investigaciones e Innovación. Resulta importante profundizar en una estrategia país de que cosas pueden ser habilitadas llevar a la nube y utilizar sus algoritmos y cuáles no. Por último, es necesario plataformas de interoperabilidad para mejorar la calidad de datos y de esa forma la interoperabilidad de sistemas.

Línea trabajo y Capacitación IA

(Ref. Capítulo 6 del documento)

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.

Comentarios

En este campo hay tres grandes grupos para capacitar:

- Asociado a la reconversión, es necesario familiarizar a las personas trabajadoras con estas tecnologías para que lo incorporen en sus ámbitos de trabajo. Se requiere para tener empresas e industria más competitiva.
- Personal que va a desarrollar los modelos, no tienen que ser áreas técnicas.
- Concientizar a la ciudadanía de las fortalezas que el buen uso brinda y amenazas que puede generar si se da un mal uso a la misma.

Línea responsabilidad civil y derechos del consumidor

(Ref. Capítulo 7 del documento)

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.

Comentarios

En un país productor de tecnología como Uruguay y donde se apuesta al crecimiento de la incidencia de esta industria en la economía, es importante dar adecuada protección a los desarrolladores y fabricantes de las aplicaciones de IA. La responsabilidad debe estar asociada al incumplimiento de las normativas legales vigentes y a casos de probada negligencia. La sobreregulación en este punto puede generar responsabilidades que impongan una barrera alta a los emprendedores.

Línea de medidas de promoción para la IA

(Ref. Capítulo 8 del documento)

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

Comentarios

Se entiende importante generar los espacios con políticas públicas que impulsen la inclusión de esta tecnología en industrias que queremos potenciar a nivel país. Ejemplo el Agro.

Definir políticas y prácticas del buen uso de los datos y sus entrenamientos. Generar sellos que validen a las empresas que lo aplican. Estos sellos pueden

ser reconocidos globalmente mejorando la calidad de los servicios que brindan las empresas, por otro lado, se da garantías a la ciudadanía que las buenas prácticas son aplicadas.