Asociación Judicial Bonaerense
Personería Gremial Nº 1446/85
Calle 50 Nº 712 - C.P. (B 1900 ATD) La Plata, Provincia de Buenos Aires
0221 423-1006 / 422-8594 ajb.org.ar ajb@ajb.org.ar

Aportes de la Asociación Judicial Bonaerense al Proyecto de Reglamento para el desarrollo y uso responsable de la IA de la Suprema Corte de Justicia de la provincia de Buenos Aires

La Suprema Corte de Justicia de la provincia de Buenos Aires puso en conocimiento el "Reglamento para el desarrollo y uso responsable de la Inteligencia Artificial de la Suprema Corte de Justicia de la provincia de Buenos Aires" y convocó a un proceso de consulta participativa para que magistrados, funcionarios, agentes, colegios profesionales, instituciones académicas y demás interesados formulen observaciones y aportes al proyecto (Resolución SC Nº 1719/26, Resolución RP 747/26 y Resolución SC 2020/26)[1]. Inicialmente el período establecido para la consulta fue del 8 de junio al 8 de julio, extendido luego al 8 de agosto y al 21 de agosto por la Resolución de Presidencia 894/26.

Para poder presentar las propuestas y observaciones dispuso un formulario online organizado en bloques temáticos donde debía hacerse referencia a los artículos e indicar el tipo de aporte (observación general, propuesta de modificación, incorporación de texto, supresión de texto) con una extensión máxima de 4000 caracteres y la limitación de indicar solamente un tipo de aporte para cada tema.

La Asociación Judicial Bonaerense (AJB) en su carácter de organización sindical con personería jurídica, con representación de las y los trabajadores judiciales, tras venir trabajando aspectos vinculados con la tecnología, convocó a una charla abierta para debatir el reglamento propuesto. El proceso de elaboración de su propuesta incluyó el ámbito de debate, documentos elaborados por trabajadores y trabajadores, consultas a especialistas y bibliografía especializada. La presentación se realizó el día 6 de agosto por el formulario habilitado y se envió otra presentación un poco más extensa por mesa de entradas, dado que en algunos temas la cantidad de caracteres máxima que brindaba el formulario era insuficiente para expresar la totalidad de las observaciones, lo que marca la necesidad de continuar profundizando en todos los aspectos abordados..

El presente documento busca difundir la contribución de la AJB a este proceso, por lo que contiene la versión completa de las observaciones enviadas, sumando la referencia a los articulados del Reglamento para entender su contexto y, al final, las referencias bibliográficas y normativa citada. Por lo demás, la estructura reproduce la del formulario.

[1] La difusión del formulario fue publicada el día 23 de junio de 2026, la que indicaba el formulario para realizar los aportes: https://www.scba.gov.ar/institucional/nota.asp?id=59397

Resumen

Los aportes de la Asociación Judicial Bonaerense “Reglamento para el desarrollo y uso responsable de la Inteligencia Artificial de la Suprema Corte de Justicia de la provincia de Buenos Aires” podrían sintetizarse en cuatro grandes ejes:

- **Derechos laborales, estabilidad en el empleo y condiciones de trabajo**

El reglamento expresa que la incorporación de IA implicará una transformación, reorganización y redistribución de tareas pero no hace referencia a derechos laborales ni a condiciones de trabajo. Se propone incorporar que las medidas adoptadas no implicarán despidos ni reducción de personal, debiendo en su caso recalificar a las y los trabajadores que puedan verse afectados, con información anticipada y consulta sindical previa a cualquier implementación. Se destaca que, actualmente, parte del personal de la Secretaría de Tecnología Informática posee cargos no acordes a su formación y función, por lo que se propone avanzar en su jerarquización y ampliar la planta considerando las nuevas tareas y funciones a su cargo.

Se deben proveer herramientas de trabajo (teléfonos oficiales, computadoras para trabajo remoto o fuera de la sede) en todos los casos sin trasladar costos operativos a las y los trabajadores así como implementar una capacitación continua acorde a las transformaciones. Se debe garantizar zero rating para la totalidad de los sitios web, servicios y aplicaciones que posibiliten el acceso al sistema de administración de justicia. Se rechaza el uso de IA para "estadísticas y análisis de plazos" por constituir telemetría y una forma de vigilancia laboral.

En cuanto a los deberes de los operadores se cuestiona que se traslade a las y los trabajadores la responsabilidad de garantizar la fiabilidad de herramientas que no controla. Se advierte que sistemas como OpenAI, Gemini y otros, utilizan los datos para entrenar sus modelos por defecto, y que algunas empresas solo lo excluyen en planes corporativos, vinculando estos datos civiles con usos militares (con injerencia del Departamento de Defensa de EE.UU, entre otros, de los que son contratistas).

- **Democratización y participación de todos los actores**

Se sugiere convocar, tanto en la elaboración del reglamento como en su implementación, a "la totalidad de los sectores involucrados... incluida la sociedad civil" (art. 2), e integrar la Comisión de Gobernanza con representación sindical y perfiles técnicos (art. 8), lo que aportaría mayor legitimidad y transparencia al proceso. Se propone convocar expertos en informática, telecomunicaciones y ciberseguridad para mejorar las definiciones y participar de otras fases del proceso. La AJB se pone a disposición para participar de la organización de capacitaciones (Ley Micaela, Ley Yolanda). Se propone que la revisión periódica del Reglamento (art. 33) incluya a la cadena de suministro y a los trabajadores, con una periodicidad semestral o anual, como complemento del trabajo que realicen la Comisión y la Suprema Corte. Asimismo, se ofrece colaboración en la organización, junto con universidades y el entorno científico-tecnológico, de programas que permitan fortalecer de manera conjunta la seguridad del entorno judicial.

- **Soberanía nacional y respeto de la normativa de DDHH**

Es necesario reforzar las previsiones sobre jurisdicción y competencia, de modo que toda contratación tecnológica quede sujeta a la jurisdicción argentina y se evite la prórroga de jurisdicción. En este sentido se propone revisar la asimetría de requisitos entre proveedores nacionales y extranjeros que hoy prevé el art. 10 del Reglamento. Resulta útil tener presentes marcos normativos extranjeros como la CALEA Act, el CLOUD Act y la Sección 702 FISA (EE.UU.), que habilitan el acceso estatal a datos, para evaluar su compatibilidad con la Ley 25.326 y los arts. 18, 19 y 43 de la Constitución Nacional. Recomendamos también ponderar cuidadosamente los alcances del reciente acuerdo comercial Argentina–EE.UU. vinculado al estatus de "país adecuado" en materia de privacidad, a la luz de las normas de jerarquía constitucional, y sugerimos tomar como referencia los "Principios Rectores sobre las Empresas y los Derechos Humanos" de la ONU para que toda la cadena de suministro —incluidos los proveedores extranjeros— se ajuste a los tratados de derechos humanos ratificados por Argentina (art. 75 inc. 22 CN).

La protección de derechos humanos debe ser garantizada institucionalmente, no delegada al agente. La tecnología solamente reproducirá aquello que ya ocurre dentro de la administración de justicia, pudiendo amplificar por ello su impacto negativo. Se propone agregar aspectos que contemplen la protección ambiental (Ley 25.675, Acuerdo de Escazú) por el consumo de agua y energía que implican los centros de datos.

- **Normativa sobre IA, comunicaciones y ciberseguridad**

Para enriquecer el marco de referencia del Reglamento, se propone incluir citas y remisiones a normativa y estándares relevantes que actualmente no figuran en el texto: la Ley 25.326 de Protección de Datos Personales y la Ley 27.699; la Ley 27.078 (Argentina Digital) y la Ley 19.798 de Telecomunicaciones; la Resolución 1523/2019 de la Jefatura de Gabinete de Ministros (infraestructuras críticas); el Decreto 8/2021 de la Provincia de Buenos Aires (Plan Integral de Ciberseguridad) y la Res. SC 1649/21; la Decisión Administrativa 641/21 (Requisitos Mínimos de Seguridad de la Información); la Disposición 3/2023 de la ex Dirección Nacional de Ciberseguridad; la Guía Integral de Empleo de la Informática Forense (Res. PG 483/16); estándares internacionales como el EU AI Act y el criterio Daubert para prueba pericial; y tener en cuenta aspectos que surgen del Manual de Tallin 2.0 sobre derecho internacional aplicable a operaciones cibernéticas elaborado por la OTAN, especialmente en materia de derecho internacional humanitario e infraestructuras.

En materia de derechos humanos, sugerimos incorporar el informe A/HRC/48/31 de la ONU sobre privacidad en la era digital y el informe A/80/169 de la Relatora Especial sobre la independencia de magistrados y abogados, que aportan estándares útiles para el diseño del Reglamento y el diseño de políticas públicas en materia judicial. Allí se recomienda prohibir aplicaciones de IA incompatibles con los derechos humanos hasta contar con garantías adecuadas.

Se propone prohibir los "Agentes de IA" autónomos (art. 9 inc. g) por ampliar la superficie de ataque cibernético y prescindir de control humano. Recuerda dos filtraciones de datos sufridas por la SCBA: en octubre de 2022 (15.000 registros de magistrados y funcionarios) y en marzo de 2025 (filtración

confirmada de datos de agentes judiciales). Propone crear un CERT propio y organizar programas de "bug bounty" con universidades.

Se solicita prohibir el uso de IA en funciones críticas —interpretación de normas, valoración de pruebas, sistemas predictivos de resultados de litigios,, entre otros— para evitar vaciar de contenido la función jurisdiccional.

Se reclama análisis de impacto algorítmico y planes piloto para todos los sistemas, sumar evaluación de impacto ambiental y ciberseguridad, y precisar el protocolo de desmantelamiento y borrado seguro de bases de datos. El repositorio público debería actualizarse mensualmente, en lenguaje accesible, incluyendo los resultados de las auditorías de impacto, privacidad y ambiental.

La justicia no debe deshumanizarse por el uso de tecnología. En algunos casos, su implementación puede generar nuevas barreras de acceso a la justicia, profundizar las desigualdades existentes o crear otras nuevas, y negativamente la estructura organizativa y laboral del Poder Judicial. Por eso, antes de avanzar con estas tecnologías, se propone priorizar mejoras edilicias, la instalación de laboratorios de informática forense propios y la capacitación continua del personal, en lugar de adoptar apresuradamente herramientas comerciales extranjeras. Esto es clave para preservar la función de garantía que el Estado tiene frente a la ciudadanía y frente a sus propios trabajadores, en su rol de empleador. Por lo tanto, se propone que los recursos se destinen al fortalecimiento de las infraestructuras tecnológicas; la generación de capacidades cibernéticas soberanas; la provisión de herramientas de trabajo (dispositivos); el desarrollo de laboratorios forenses propios y la creación de herramientas que ayuden a mitigar los efectos nocivos que la IA pueda tener sobre las actividades laborales y el sistema de administración de justicia. En este sentido, se considera necesaria la capacitación continua del personal; y la colaboración con el sector universitario y científico-tecnológico argentino, entre otros.

Observaciones y aportes por bloque temático

Complete únicamente los bloques sobre los que desee formular aportes. Recuerde siempre ser preciso, concreto y justificar los mismos."

BLOQUE 1: Disposiciones generales: objetos, sujetos alcanzados, ámbito de aplicación, finalidad y definiciones.

Disposiciones del Anexo I comprendidas: Capítulo I — arts. 1° a 5°.

Observación general X
Propuesta de modificación X
Incorporación de texto
Supresión de texto X

Artículo / inciso específico sobre el que recae el aporte (si corresponde)

Artículo 1: Objeto. El presente reglamento tiene por objeto establecer los principios, normas, criterios y pautas de diseño y uso que regirán el uso de la Inteligencia artificial (IA) en la Jurisdicción Administración de Justicia.

Art. 1: se pretende regular la "IA", sin definirla adecuadamente (art. 5). En cuanto a las definiciones, es imperativo que en el proceso de elaboración del glosario se convoque a expertos en el ámbito de la informática, comunicaciones, telecomunicaciones, privacidad y ciberseguridad para obtener precisión técnica en las definiciones que se adopten. Teniendo en cuenta que de ello dependerá el alcance de la aplicación e interpretación del reglamento que se apruebe y que cualquier definición estática conlleva problemas como dejar fuera definiciones computacionales o vinculadas con tecnologías que pudieren surgir en el futuro (Lazzarini, 2022). "Alucinaciones y desinformación" se definen conjuntamente, cuando técnicamente no son lo mismo. En cuanto al "Sistema de IA protegido", desde una perspectiva de ciberseguridad, la definición es insatisfactoria. Respecto de la definición de IA adoptada literalmente de UNESCO ("se asemeja a un comportamiento inteligente"), se incurre en una imprecisión conceptual (al respecto, ver Wolberg).

Artículo 2: Sujetos alcanzados. Las disposiciones aquí contenidas son de observancia obligatoria para: ● Jueces/juezas, funcionarios/as, agentes y empleados/as de todos los órganos judiciales de todos los fueros. ● Los funcionarios y agentes que presten servicios dentro de las estructuras de gobierno de esta Jurisdicción Administración de Justicia, ● Auxiliares de la Justicia. ● Entidades externas que desarrollen, provean, integren o mantengan sistemas de IA utilizados por la Suprema Corte, en la medida que sus contratos o convenios así lo establezcan.

Art. 2: En relación a los magistrados, funcionarios, agentes y empleados, teniendo en cuenta que el incumplimiento de la norma a dictarse implicará una transformación, reorganización y redistribución de tareas; y una modificación en las estructuras de trabajo internas y de vinculación con los justiciables con impacto en los procesos judiciales y administrativos; como así también, el carácter vinculante y la potestad sancionatoria en caso de infracción, se torna imperativo convocar a la totalidad de los sectores involucrados a efectos que participen activamente en el rediseño

organizacional; teniendo en cuenta que se pretende la utilización de datos en poder de la SCBA obtenidos en su carácter de empleador, de los cuales todos los mencionados son titulares, y la SCBA depositaria en virtud del vínculo laboral (sin mencionar al proveedor que pudiera intervenir en cualquier momento).

En relación a las entidades externas que integren la cadena de suministro deberán ser sujetos alcanzados sin excepción, por tratarse de una infraestructura crítica. En relación a proveedores extranjeros, deben cumplir con las previsiones de la Sección XV de la Ley 19.550, dado que al tratarse de materia tecnológica, rigen, en principio, las Leyes 27078, 25326 (art .43, párrafo 3, CN). Cualquier entidad o persona que quiera formar parte de la cadena de suministro debe atenerse a la jurisdicción y competencia argentinas, prohibiéndose la prórroga de jurisdicción en la contratación dadas las imposibilidades materiales existentes para garantizar el cumplimiento por parte de proveedores extranjeros (al respecto, ver casos europeos en el marco de GDPR; Brasil). Se recomienda incorporar mecanismos vinculados con la responsabilidad de acuerdo con los "Principios Rectores sobre las Empresas y los Derechos Humanos" (ONU, adjuntos al informe A/HRC/17/31 del Consejo de DDHH; Res. Consejo de DDHH 17/4 del 16/06/2011), teniendo en cuenta las obligaciones asumidas por el Estado argentino, de adoptar disposiciones de derecho interno que garanticen la operatividad de los tratados internacionales de DDHH y el derecho internacional humanitario (art. 75 inc. 22 CN, Convención de Viena sobre Derecho de los Tratados, arts. 27 y 31), atento que en cualquier caso de contratación se estará afectando directamente la tutela efectiva de derechos y garantías de trabajadores, operadores y efectores de la Administración de Justicia, y especialmente de los justiciables, y de la adecuada prestación de la administración de Justicia en sí.

No se tiene en cuenta como sujetos alcanzados a las organizaciones o particulares externos cuyos sistemas interoperan con aquellos bajo responsabilidad de la SCBA.

Artículo 5: Definiciones. A los efectos del presente reglamento y de las normativas que en su consecuencia se dicten se entenderá por:

- ***Sistema o herramientas de Inteligencia Artificial:*** *Sistemas computacionales "capaces de procesar datos e información de una manera que se asemeja a un comportamiento inteligente, y abarca generalmente aspectos de razonamiento, aprendizaje, percepción, predicción, planificación o control".*
- ***Sistema de Inteligencia Artificial generativa:*** *Sistemas computacionales "que se comunican en lenguaje natural, capaces de responder a preguntas relativamente complejas y pueden crear contenido (proporcionar texto, imagen o sonido) tras una pregunta o instrucciones formuladas (prompt)".*
- ***Modelo de lenguaje de gran tamaño (LLM por su sigla en inglés):*** *Es un tipo de algoritmo de inteligencia artificial que utiliza técnicas de aprendizaje profundo y conjuntos de datos muy grandes para comprender, resumir, generar y predecir nuevo contenido. El término IA generativa también está estrechamente relacionado con los LLM, que son, de hecho, un tipo de IA generativa que se ha diseñado específicamente para ayudar a generar contenido.*
- ***Aprendizaje Automático (ML):*** *"un conjunto de técnicas que permite a las máquinas aprender automáticamente usando patrones y deducciones en lugar de instrucciones directas de una persona". o Procesamiento de Lenguaje Natural (PLN): "una técnica de aprendizaje automático que analiza grandes cantidades de datos de texto o voz humana (transcriptos o*

acústicos) en busca de propiedades específicas, como significado, contenido, intención, actitud y contexto". o Sistema de IA seguro (safe): Aquel que, durante todo su ciclo de vida —desde el diseño hasta la desactivación—, identifica, evalúa y mitiga activamente los riesgos de daños no deseados sobre las personas, instituciones y el entorno, garantizando que sus resultados no excedan lo necesario para alcanzar el objetivo legítimo perseguido y que se encuentren dentro de niveles de riesgo aceptables.

- ***Sistema de IA protegido (secure):*** *Aquel que implementa medidas técnicas y organizativas robustas para preservar la integridad, confidencialidad y disponibilidad de los datos y procesos, resistiendo accesos no autorizados, manipulaciones maliciosas o ciberataques, y que cuenta con marcos de acceso a los datos que respeten la privacidad y garanticen la calidad de la información utilizada.*
- ***Sistema de IA confiable (trustworthy):*** *Aquel cuyo funcionamiento es transparente, explicable, trazable y sometido a supervisión humana efectiva; que respeta los derechos fundamentales, la democracia y el Estado de Derecho; que actúa de manera consistente con valores éticos verificables; y cuya cadena de responsabilidad es clara e identificable a lo largo de todo su ciclo de vida.*
- ***Algoritmo:*** *Serie de instrucciones para realizar cálculos u otras tareas, ya sea en matemáticas o en informática. En el caso de la inteligencia artificial, un algoritmo proporciona las reglas o instrucciones que permiten a un computador aprender a aprender del entorno y realizar un conjunto de tareas.*
- ***Análisis de Impacto Algorítmico (AIA):*** *Proceso que se desarrolla en la fase de pilotaje o diseño preliminar con el objetivo es anticipar posibles impactos antes que el sistema entre en operación. Permite ajustar parámetros, detectar riesgos tempranos (p.e. sesgos), y evaluar el desempeño de la herramienta en condiciones reales controladas, para luego decidir sobre su posible implementación definitiva Este análisis es fundamental para valorar si una herramienta determinada es técnicamente viable, socialmente aceptable y jurídicamente compatible con el contexto institucional en el que se pretende aplicar.*
- ***Evaluación de impacto algorítmico (EIA):*** *Proceso que permite evaluar el desempeño del sistema, si emergen sesgos no contemplados en el diseño, si los datos utilizados han perdido representatividad, o si cambios institucionales hacen necesario ajustar su funcionamiento. La EIA permite así corregir desvíos actualizar medidas de mitigación (o adoptarlas en aquellos casos en que no se llevó a cabo una AIA) y asegurar que la herramienta sigue cumpliendo con los estándares éticos y jurídicos exigidos.*
- ***Ciclo de vida de los sistemas de IA:*** *Ciclo que incluye las etapas de prediseño, diseño, desarrollo, evaluación, prueba, despliegue, uso, venta, adquisición, operación y desmantelamiento.*
- ***Prompt o input:*** *Instrucción, consulta o conjunto de datos de entrada que un usuario introduce en un sistema de IA para generar una respuesta.*
- ***Alucinaciones y desinformación:*** *Resultados imprecisos o inexactos que pueden generar los sistemas de IA generativa, especialmente los basados en modelos de lenguaje de gran tamaño (LLM).*
- ***Sesgo de Inteligencia artificial:*** *el sesgo de IA es una diferencia sistemática en el tratamiento de ciertos objetos, personas o grupos (por ejemplo, estereotipos, prejuicios o favoritismo) en comparación con otros mediante algoritmos de IA. Este tipo de sesgos resultan de los datos*

usados para entrenar el algoritmo, lo que puede reforzar prejuicios de raza, género, sexualidad, etnia o discapacidad.

- *Operador judicial: Toda persona humana perteneciente a la estructura del Suprema Corte de Justicia —o que actúe en su nombre o bajo su autoridad— que, en el ejercicio de sus funciones jurisdiccionales o administrativas, utilice, supervise, gestione o tome decisiones a través de la utilización de un sistema de inteligencia artificial, asumiendo responsabilidad directa sobre las condiciones de uso, la supervisión humana del sistema y las consecuencias jurídicas de los resultados producidos por dicho sistema en el marco de la actividad judicial.*

Las definiciones precedentes han sido elaboradas tomando como referencia, entre otros instrumentos y documentos especializados, las "Directrices para el Uso de Sistemas de Inteligencia Artificial en Cortes y Tribunales" de la Organización de las Naciones Unidas para la Educación, la Ciencia y la Cultura (UNESCO, 2026); "Inteligencia Artificial en los Poderes Judiciales de Latinoamérica: Reflexiones y Lineamientos para las Américas" del Centro de Estudios de Justicia de las Américas (CEJA, 2025); la Resolución A/RES/78/265 de la Asamblea General de las Naciones Unidas; el Acuerdo PCSJA24-12243 de la Corte Constitucional de Colombia y demás estándares, lineamientos y documentos técnicos nacionales e internacionales aplicables en la materia.

Art. 5: no se citan los estándares, lineamientos y documentos técnicos nacionales e internacionales aplicables en la materia. Ello impide conocer con precisión la fuente de las definiciones técnicas adoptadas, lo que impide la posibilidad de dotar de rigor de la norma.

Observación, fundamentación y/o redacción propuesta:

Se propone la modificación de los arts. 1, 2, 4 y 5.

Art. 1: Se recomienda convocar expertos en la materia, a los efectos de la elaboración del glosario, lo que permitirá, en definitiva, definir el objeto adecuadamente. Se aplica lo mismo para el art. 5.

Art. 2: Se recomienda convocar a las representaciones legalmente constituidas de los sectores involucrados, incluida la sociedad civil, con la finalidad que participe activamente en la totalidad del proceso de elaboración de la norma, atento el alcance e impacto que el mismo tendrá sobre el servicio de justicia, y respecto de la forma de trabajo, tratándose de una verdadera reforma judicial que implicará la reorganización de la carrera, distribución, redistribución de tareas y puestos; creación de nuevas áreas de trabajo; necesidad de capacitación continua que permita la adecuada incorporación de la tecnología en el trabajo diario, entre otros aspectos más difíciles, tales como la ciberseguridad y la vigilancia, y la incorporación de evidencia al proceso. Respecto de este último punto, es necesario ser precavidos de no invadir esferas reservadas a otros poderes del Estado, dado que las previsiones contenidas en el "Bloque 2" impactan directamente en el proceso en cualquier fuero en el que se pretenda aplicar, tanto en sede administrativa como judicial, corriendo el riesgo de legislar en materia procesal, o tornar ineficaz y privar de operatividad el derecho de defensa.

Debe evaluarse también si las actividades judiciales que se pretende mediar tecnológicamente pueden ser realizadas por trabajadores, la necesidad de creación de cargos e incorporación de nuevos trabajadores (del cargo o jerarquía que se trate), especialmente perfiles vinculados con tecnologías. Ello incluye también los costos, dado que la infraestructura tecnológica requerida para el despliegue de tecnologías como las que se pretende regular a gran escala, conlleva un gasto

extremadamente elevado, usualmente en moneda extranjera, y en muchos casos sujetos a variables de precio atadas al mercado internacional, siendo excesivamente mayor a aquel que podría destinarse a la incorporación de nuevos trabajadores. A su vez, se deberá tener en cuenta si se trata de una empresa con poder significativo de mercado, lo que cobra especial relevancia en la Sociedad de la Información, tanto para los ciudadanos de a pie y los trabajadores, como para el Estado; o si se trata de una empresa que es contratista o que hizo el desarrollo conjuntamente con otro Estado.

Se recomienda que la norma que en definitiva se dicte sea de cumplimiento obligatorio para los proveedores que contraten con la Administración de Justicia, por tratarse de una infraestructura crítica. Caso contrario, no podrá garantizarse el cumplimiento de ninguno de los aspectos que se pretende regular, a menos que se tenga control total de la infraestructura tecnológica, es decir, una infraestructura soberana.

Artículo 4: Finalidad. La integración de sistemas de IA en la Jurisdicción Administración de Justicia persigue las siguientes finalidades: mejorar la eficiencia en la gestión de los procesos judiciales y procedimientos administrativos; fortalecer el acceso a la justicia eliminando barreras tecnológicas, lingüísticas y geográficas; apoyar la función jurisdiccional sin sustituir el razonamiento jurídico y el juicio humano; garantizar la transparencia, la rendición de cuentas y la impugnabilidad en el uso de herramientas de IA; y proteger los derechos fundamentales de todas las personas que intervienen en procesos judiciales y/o administrativos en la órbita de la Suprema Corte.

Art. 4. Se propone que a la hora de determinar las finalidades perseguidas con la implementación de tecnologías, se priorice la protección de los derechos humanos y su efectivo ejercicio en el ámbito del proceso judicial y/o administrativo, por sobre la eficiencia en la gestión de los procesos judiciales y procedimientos administrativos: el orden de los factores altera el producto.

En cuanto a la eliminación de barreras, la sola implementación de herramientas tecnológicas no implica necesariamente la eliminación de barreras; máxime en los casos en que se trata de adopción de herramientas tecnológicas diseñadas, desarrolladas, entrenadas y pensadas desde una lógica e idioma extraños a la sociedad y el territorio en que pretende desplegarse.

Art. 5: Se recomienda convocar a expertos en la materia, con la finalidad de elaborar un glosario adecuado. También, dar publicidad a la totalidad de las fuentes utilizadas, atento el impacto de la norma.

BLOQUE 2: Principios rectores

Disposiciones del Anexo I comprendidas: Capítulo II — art. 6° (protección de derechos humanos, no discriminación, igualdad, equidad procesal, privacidad, proporcionalidad, seguridad, explicabilidad, auditabilidad, transparencia, responsabilidad, supervisión humana, gobernanza, entre otros).

Observación general X
Propuesta de modificación
Incorporación de texto
Supresión de texto X

Artículo / inciso específico sobre el que recae el aporte (si corresponde):

Artículo 6: El uso y aprovechamiento de los sistemas de inteligencia artificial se regirá por los principios que a continuación se detallan:

Protección de los derechos humanos: Implica tomar las medidas necesarias para respetar, proteger y promover los derechos humanos y el estado de derecho a lo largo de todo el ciclo de vida de los sistemas de IA. debiendo existir salvaguardas eficaces respecto de los sistemas de IA que puedan representar un alto riesgo para los derechos humanos, así como como la implementación de las evaluaciones de rendición de cuentas. El despliegue de sistemas de IA debe proteger especialmente los derechos de las mujeres y las niñas, las personas con discapacidad, los niños, las minorías y otras grupos y/o poblaciones en situación de marginación y/o vulnerabilidad. Aunque todos los derechos humanos pueden verse potencialmente afectados por ciertos sistemas de IA a lo largo del ciclo de vida de estas herramientas, los siguientes son especialmente importantes en el contexto de los procedimientos judiciales y administrativos.

Protección de los DDHH: deben adoptarse en todo momento por la totalidad de los agentes, por mandato constitucional y convencional, y es responsabilidad política del Estado y hace a su función de garantía. No se indica si las salvaguardas eficaces a las que se refiere son de tipo legal, técnico, o ambas. Por sus características propias, y el ámbito en que se pretende implementar, hay un alto riesgo de lesión a los derechos humanos. No se indica cómo se instrumentará la rendición de cuentas y en qué consistirá. Se recomienda tener en cuenta el Informe A/80/169 de la Relatora Especial sobre la independencia de los magistrados y abogados, que advierte del impacto en áreas críticas como el sector justicia y sobre el riesgo de pérdida de soberanía por la alta concentración de poder de las empresas y estados que controlan las infraestructura. En cuanto a los grupos vulnerables, debe tenerse en consideración los grupos identificados y lineamientos establecidos por la CIDH, como así también, las interseccionalidades existentes.

a) No discriminación: Adoptar, desplegar y utilizar sistemas de IA que busquen alcanzar objetivos mediante procesos que salvaguarden la equidad y garanticen un acceso inclusivo a la tecnología. Prevenir el desarrollo y las aplicaciones sesgadas de sistemas y resultados de IA que puedan agravar, reproducir, reforzar o perpetuar la discriminación basada en raza, color, ascendencia, género, edad, idioma, religión, opinión política, condición nacional, étnica, social o económica, discapacidad y cualquier otro motivo.

Inc. a: No discriminación. Para prevenir el desarrollo y aplicaciones sesgadas de tecnologías, y sus impactos, se debería contar con datos de calidad, efectuar correcciones, auditorías, trabajar con los operadores sobre esos sesgos, pues serán ellos los que alimenten y entrenen el sistema que se utilice. La tecnología solamente reproducirá aquello que ya ocurre dentro de la administración de justicia, amplificando y afianzando su impacto negativo.

b. Igualdad: Garantizar el acceso y el trato igualitario para todos ante los tribunales, independientemente de sus capacidades digitales. La implementación de herramientas de IA en lo judicial debería tener en cuenta a quienes no pueden permitirse estas tecnologías, carecen de alfabetización digital o enfrentan otras barreras tecnológicas. Para ello, es pertinente seguir el principio de No Dejar a Nadie Atrás (LNOB), desarrollado como parte de la Agenda de las Naciones Unidas para el Desarrollo Sostenible, para abordar la exclusión digital.

Inc. b: Igualdad: la garantía de acceso y trato igualitario recae exclusivamente en los agentes y es responsabilidad institucional del Poder Judicial, aplique o no tecnologías para ello. Debe tenerse en cuenta la conectividad y alfabetización digital de la totalidad de las partes involucradas y, en especial, los niveles de lecto comprensión, la brecha digital y la capacidad de comprender el funcionamiento, implicancias y consecuencias del uso de tecnologías en el proceso.

c. Equidad procesal: Evaluar las implicaciones de los sistemas de IA para garantizar la equidad procedimental a lo largo de todo su ciclo de vida y evitar despliegues que vulneren este derecho.

Inc. c: Equidad procesal: Debe ser garantizada por los operadores..

d. Derecho a la privacidad y protección de datos personales: La adopción, despliegue y utilización de sistemas de inteligencia artificial en el ámbito de la administración de justicia deben garantizar la protección efectiva del derecho a la privacidad y a la protección de los datos personales de todas las personas involucradas en los procesos judiciales y procedimientos administrativos. La utilización de herramientas de IA deberá evitar la generación de riesgos de divulgación indebida de datos personales y prevenir el acceso no autorizado a los mismos por parte de terceros, a lo largo de todo el ciclo de vida del sistema.

Inc. d: Privacidad y protección de datos: en la adopción, despliegue y utilización de tecnologías aplica plenamente la teoría del riesgo (art. 1757 CCyC); se deben adoptar todas las medidas tendientes a garantizar la protección efectiva del derecho a la privacidad y a la protección de datos personales de todos los involucrados en los procesos judiciales y administrativos. En todos los casos donde nos encontremos frente a tratamiento automatizado de información, pueden existir riesgos de divulgación indebida de datos personales (art. 157 bis CP) y accesos no autorizados (arts. 153, 153 bis CP). El cumplimiento del objetivo depende de la robustez e implementación de la política de seguridad informática de la organización. Se debe cumplir estrictamente la Ley 25326 y los criterios sentados por la CSJN in re “Halabi” y “Torres Abad”, caso SRFP (CABA), como así también tener en cuenta el precedente de la CIDH “Colectivo de Abogados José Alvear Restrepo c/ Colombia”.

e. Libertad y seguridad: Ninguna persona podrá ser detenida, privada de su libertad, sometida a medida cautelar restrictiva o afectada en sus derechos fundamentales con base, total o parcial, en decisiones adoptadas mediante sistemas de inteligencia artificial, cuando dicha persona no haya sido informada del uso de tales sistemas, no pueda comprender los criterios mediante los cuales el sistema produjo el resultado que la afecta, o no cuente con medios efectivos para impugnar o apelar tanto el proceso de toma de decisiones como la decisión en sí misma.

Inc. e: Libertad y seguridad: la prohibición inicial pierde sentido al habilitar la excepción bajo presunto consentimiento informado. Este punto corre el riesgo de convertirse en una ficción o presunción. El deber de información no puede desconocer que al informar a la persona sobre del uso de la herramienta, los criterios utilizados por el sistema, implica acreditar que comprendió adecuadamente el funcionamiento del mismo. En cuanto a los medios efectivos para impugnar o apelar tanto el proceso de toma de decisiones como la decisión en sí misma, ello no evita la restricción del derecho (la impugnación o apelación se realiza ex post facto ante el juez). En el texto propuesto se prohíbe la delegación de toma de decisiones, pero la redacción de este ítem lo habilita, lo que da margen a discrecionalidad y, eventualmente, arbitrariedad. Se debe garantizar que los

sistemas no atenten contra la aplicación de los principios in dubio pro (reo, operario, natura, infancia, persona, etc.).

Proporcionalidad: La adopción, despliegue y utilización de sistemas de IA deben como objetivo lograr fines legítimos y proporcionales en el contexto de su uso.

Proporcionalidad: a la hora de determinar la necesidad de diseño, desarrollo, adopción, despliegue y utilización de sistemas de IA, se debe ponderar si la injerencia sobre derechos será proporcional o no a los fines perseguidos, evitando el uso cuando ello no se cumpla.

Seguridad de la información: La adopción, despliegue y utilización de sistemas de IA deben asegurar la aplicación de estándares para asegurar la integridad, confidencialidad y disponibilidad de la información, cumpliendo con las obligaciones establecidas en las leyes aplicables, en los lineamientos de este Reglamento y demás normativa que en su consecuencia se dicte.

Seguridad de la información: Se debe adoptar la política de privacidad y seguridad desde el diseño. Se recomienda adoptar medidas para prevenir ataques, y establecer claramente una política de seguridad. La totalidad de la normativa aplicable debe ser de acceso público.

- *Explicabilidad: La adopción, despliegue y utilización de sistemas de IA deberán proporcionar información —tanto a quienes despliegan la herramienta como a sus usuarios— sobre las entradas, razonamientos, resultados y funcionamiento de los sistemas de IA, haciendo que estos elementos sean comprensibles, interpretables y rastreables para las personas humanas.*
- *Auditabilidad: La adopción de medidas administrativas y legales para asegurar y permitir que los sistemas de IA puedan ser auditados durante su despliegue.*
- *Justicia transparente y abierta/ Transparencia: La adopción, despliegue y utilización de sistemas de IA deben ser transparentes en cuanto a cómo se desarrollaron, cómo funcionan, cuáles son sus datos de entrenamiento, sus limitaciones (incluido el margen de error), sus capacidades y el propósito de los sistemas. Asimismo, deben informar de manera adecuada y oportuna cuándo y cómo se despliegan, cómo funcionan estas herramientas, especialmente cuando las decisiones tomadas con o basadas en ellas puedan afectar los derechos y libertades de individuos o comunidades., de forma tal que permita a los usuarios e interesados su pleno conocimiento y la efectiva posibilidad de contradicción.*

Explicabilidad, auditabilidad y transparencia: teniendo en cuenta que la administración de justicia es un área crítica, los modelos que se implementen deben ser explicables, auditables y se debe impulsar una política de transparencia en todo el ciclo de vida de los sistemas, incluidas las bases de datos utilizadas para entrenamiento, debiendo los repositorios ser de acceso público y privilegiarse los desarrollos de código abierto (ver experiencia Apertus, en Suiza).

Supervisión y toma de decisiones humanas: Los operadores judiciales no deben delegar ninguna parte de su mandato ni depender exclusivamente de los sistemas de IA para adoptar decisiones o automatizar procesos completos que puedan afectar negativamente los derechos de individuos, comunidades o colectivos. Deben preservar la posibilidad de intervención humana en todos los procesos de toma de decisiones en los que se despliegue los sistemas de IA. Las herramientas de IA no deben sustituir el análisis independiente de hechos, leyes y pruebas por parte del responsable de la toma de decisiones.

Supervisión humana: se debe distinguir claramente entre la supervisión del operador no técnico (abogados u otros), de la supervisión humana técnica (en cabeza de la Comisión de Gobernanza y Uso de la IA). La UNESCO pone especial énfasis en la responsabilidad de jueces y magistrados en la no delegación de toma de decisiones o automatización de procesos, lo cual es relevante debido a la jerarquía de su rol y función respecto de los demás operadores (empleados y funcionarios).

Diseño participativo y centrado en el ser humano: El desarrollo, despliegue y uso de sistemas de IA debe seguir principios de diseño centrados en el ser humano para complementar y ampliar las capacidades de la organización en la que se insertan y respetar la dignidad y la autonomía humanas.

Diseño participativo y centrado en el ser humano. La definición adoptada omite la participación de miembros del poder judicial y del público que estaban incluidas en el documento de la UNESCO. Sostenemos la relevancia de garantizar la participación de todos los actores involucrados a lo largo de todo el proceso.

Observación, fundamentación y/o redacción propuesta:

Los "principios rectores" son para la organización, pues son los agentes aquellos que la entrenan con el uso. A nivel institucional, se deben tener en cuenta los riesgos identificados por la Relatora Especial en el Informe A/80/169. Se debe poner especial énfasis en la capacitación continua de la totalidad de la masa de trabajadores, especialmente aquellos que ocupan cargos decisorios, para que adquieran alfabetización digital y en tecnologías, en particular aquellas cuyo uso se pretende regular, teniendo en cuenta los marcos regulatorios existentes vinculados con la responsabilidad funcional, a fin que las nuevas responsabilidades que se pretenda crear sean realistas y claramente definidas en relación con el uso de las herramientas. Se deben adoptar medidas que reduzcan los riesgos de delegación cognitiva y aquellas que restrinjan indebidamente la autodeterminación informativa.

Para la efectiva tutela de cualquiera de los derechos y garantías enumerados en el art. 6, como así también todos aquellos que allí no constan pero están incluidos en los tratados internacionales de DDHH y la CN, se deberá garantizar que las empresas proveedoras extranjeras se ajusten a la legislación local. Ello es especialmente importante en relación con empresas extranjeras sometidas a jurisdicción de terceros estados que no han ratificado y/o adherido a los mismos tratados internacionales de DDHH o que no reconocen el mismo nivel de protección que en nuestro país (al respecto, Bloque 8).

En relación a "No discriminación", para prevenir el desarrollo y aplicaciones tecnológicas sesgadas, y sus impactos negativos, se debería contar con datos de calidad, trabajar en la eliminación de sesgos desde el diseño, efectuar correcciones, auditorías, trabajar con los operadores sobre esos sesgos, pues serán éstos los que alimenten y entrenen el sistema que se utilice. La tecnología solamente reproducirá aquellos sesgos presentes dentro de la administración de justicia, amplificando y afianzando su impacto negativo. Deben implementarse procesos de mitigación de sesgos a lo largo de todo el ciclo de vida del sistema.

Igualdad: la garantía de igualdad y acceso a la justicia no puede operar sin conectividad. En relación a las personas que "no pueden permitirse estas tecnologías", deberá ser el Poder Judicial el que las ponga a disposición de la parte que lo requiera, garantizando la igualdad en el acceso y en el uso, brindando todas las herramientas necesarias para ello. Se debe garantizar la atención personal

presencial; como así también diseñar sitios web y sistemas accesibles, inclusivos y de fácil uso desde cualquier dispositivo básico. En cuanto al acceso en términos de conectividad y costos, y con la finalidad que el acceso a la justicia por medios tecnológicos no implique una erogación para el justiciable, se debería gestionar institucionalmente la implementación de zero rating o tarifa cero en la totalidad de los sitios, servicios y aplicaciones del ámbito judicial, de forma tal que el acceso no dependa de la capacidad económica de la persona, sea cual fuere su rol, incluidos los trabajadores de todas las jerarquías.

Equidad procesal: debe ser garantizada por los responsables de los órganos jurisdiccionales. Se impone garantizar el debido proceso, la igualdad de armas, el control de la prueba y el contradictorio en el proceso. Se propone implementar laboratorios de informática forense, como así también propiciar la investigación y desarrollo de herramientas propias (como referencia, ver propuesta Info-Lab, Guía GT-LIF). Sería prudente, primero, unificar criterios en torno a los protocolos de tratamiento de información y evidencia digital.

Privacidad: se analizará en el Bloque 8.

Libertad y seguridad: sistemas orientados a objetivos como los que se pretenden implementar fueron cuestionados por discriminatorios (caso COMPASS, “State vs. Loomis”, 2016; SRFP, “ODIA y otros c/ GCBA s/ amparo). Estos sistemas resultan incompatibles con el ordenamiento nacional y convencional en materia de protección de DDHH y garantías; implican una vigilancia masiva, y pretenden reemplazar funciones realizadas por técnicos y especialistas. En Argentina, la identificación biométrica en tiempo real ya fue declarada inconstitucional (SRFP CABA). Se reitera la necesidad de contar con laboratorios de informática forense propios.

Viabilidad de los beneficios: Antes de adoptar sistemas de IA, deben evaluarse tanto los beneficios potenciales específicos (para el poder judicial, los usuarios y el público) como su capacidad institucional para generarlos.

Viabilidad de los beneficios: se propone incorporar la obligación de realizar las evaluaciones de impacto y riesgo de manera previa a la adopción de las tecnologías propuestas, con participación de los actores involucrados. Los beneficios que pueda brindar el uso de la herramienta no se garantizan sin una adecuada aplicación de la legislación procesal y de fondo.

Precisión y fiabilidad: La adopción, despliegue y utilización de sistemas de IA deben ser precisos, es decir, deben proporcionar información útil y relevante y producir resultados y predicciones correctas, y sistemas de IA fiables, es decir, que funcionen “correctamente con una variedad de entradas y en una variedad de situaciones”.

Precisión y fiabilidad, no existen los sistemas totalmente fiables, por ello es que se los audita permanentemente. Los modelos predictivos en muchos casos son clasificados como de riesgo inaceptable o prohibido.

Explicabilidad y auditabilidad, se debe contar necesariamente con el acceso al código fuente, bases de datos de entrenamiento, y demás información técnica. Se recomienda la aplicación de los estándares fijados en el precedente “Daubert v. Merrel Dow Pharmaceuticals Inc” (Corte Suprema USA, plasmado luego en la Regla Federal de Evidencia 702 y cctes.).

Justicia transparente/ abierta: se indica la transparencia como deber “especialmente cuando las decisiones tomadas con o basadas en ellas puedan afectar derechos y libertades”, siendo esta habilitación de uso contradictoria con el art. 6 inc. e, y con el criterio de “Supervisión humana y toma de decisiones”, por ejemplo.

Concientización y uso informado: Implica la comprensión de las funcionalidades, tipos de uso, posibles impactos, limitaciones y riesgos de los sistemas de IA disponibles, para tomar decisiones informadas sobre su implementación; el conocimiento del propósito previsto del uso de un sistema de IA específico para llevar a cabo actividades judiciales; y mantenerse al día de los avances tecnológicos.

Concientización y uso informado: la capacitación y concientización debe realizarse de manera continua, debiendo la SCBA propiciar los espacios a tal fin. De esa manera, se podrá cumplir el objetivo fijado en “Responsabilidad”, dado que se exige que los operadores estén capacitados y comprender los impactos de la tecnología. Los desarrollos de sistemas deben estar en cabeza de la Comisión, o de los laboratorios de informática forense, no de los organismos, dado que en los mismos no hay perfiles técnicos especializados en tecnología (ingenieros).

Rendición de cuentas y contestabilidad: Importa garantizar la rendición de cuentas, informando y explicando cómo y por qué ciertas herramientas de IA fueron adoptadas, así como los resultados obtenidos (o no) con su despliegue. Además, introduce mecanismos que permitan a las partes afectadas impugnar y contrainterrogar cualquier resultado producido por un sistema de IA que pueda influir en el resultado del caso en cuestión, así como impugnar las decisiones y responsabilizar a los operadores judiciales por sus errores.

Rendición de cuentas y contestabilidad: no se indican cuáles son los mecanismos que introduce que permitan a las partes afectadas impugnar y contrainterrogar cualquier resultado producido por estos sistemas.

Supervisión y toma de decisiones humana: se propone modificación del texto. Donde dice “Deben *preservar* la posibilidad de intervención humana”, debería decir “Debe ***garantizarse*** la posibilidad de intervención humana”.

Diseño participativo y centrado en el ser humano: El desarrollo, despliegue y uso de sistemas de IA debe seguir principios de diseño centrados en el ser humano para complementar y ampliar las capacidades de la organización en la que se insertan y respetar la dignidad y la autonomía humanas

Diseño participativo y centrado en el ser humano: se recomienda adoptar políticas de privacidad y seguridad desde el diseño e incluir la participación de miembros del poder judicial y del público o demás actores involucrados para garantizar la participación efectiva.

Gobernanza y colaboración multiactor: Las organizaciones judiciales deben consultar a diversos interesados, realizar consultas públicas e implementar enfoques de participación ciudadana a lo largo del ciclo de vida del sistema de IA, especialmente a quienes puedan verse afectados directa o indirectamente por su despliegue.

Gobernanza y colaboración multiactor: Ver comentario art. 2 y Bloque 3.

Adecuación a buenas prácticas y estándares colectivos. Importa la adopción prácticas y estándares que se adecúen a los principios, diseño y funcionamiento de la Jurisdicción Administración de Justicia, en el marco de las definiciones que adopten sus autoridades, tanto en sede de administración como en su faz jurisdiccional.

Adecuación a buenas prácticas y estándares colectivos: primero debe garantizarse la efectiva aplicación de la normativa procesal por parte de los operadores; y por otro lado, la posibilidad de forzar el cumplimiento de la legislación nacional cuando se contrate infraestructura tecnológica a empresas, sobre todo extranjeras. Al respecto, ver Bloque 8.

Seguimiento, mejoramiento y adaptación continua. Para el uso de sistemas de IA se consultarán permanentemente los avances jurídicos, sociológicos y tecnológicos que se vayan implementando, así como los esquemas de mejora y control que se construyan en forma progresiva.

Seguimiento, mejoramiento y adaptación continua: deben indicarse los criterios que se utilizarán, y tener en cuenta que los desarrollos tecnológicos en muchos países se desarrollan teniendo en cuenta el sistema legal en que serán desplegados, el que puede colisionar con el nacional (ver comentario párrafo 2, en este Bloque).

Prevención de riesgos. Aplicación estándares adecuados de identificación, evaluación, gestión, mitigación y control sobre situaciones que generen riesgo por la aplicación de herramientas de IA, en aspectos como imprecisiones, desactualizaciones, alucinaciones, sesgos o inconsistencias.

Prevención de riesgos: debe orientarse a la totalidad de las infraestructuras, no solamente los sistemas de IA, debiendo adoptarse un enfoque de ciberseguridad amplio.

Se propone incorporar dentro de los Principios Rectores uno específico vinculado con la prevención y mitigación de riesgos vinculados con daños ambientales, teniendo en cuenta la Ley General de Ambiente nro. 25675 y Acuerdo de Escazú (Ley 27566), fomentando el uso de tecnologías que reduzcan el impacto ambiental, dado que el pasivo ambiental que implica la instalación de centros de datos incluye el consumo masivo de recursos, generación de residuos peligrosos y alteración climática local, uso excesivo de agua, acumulación de basura electrónica. Se debería contar con mecanismos para el tratamiento de residuos electrónicos.

BLOQUE 3: Gobernanza: Comisión de Gobernanza, Uso de la IA, integración, funciones y provisión tecnológica.

Disposiciones del Anexo I comprendidas: Capítulo III -arts. 7° al 13°.

Observación general X
Propuesta de modificación X
Incorporación de texto
Supresión de texto

Artículo / inciso específico sobre el que recae el aporte (si corresponde)

Artículo 8: Integración. La Comisión estará integrada por las Secretarías de Planificación, de Tecnología Informática y de Servicios Jurisdiccionales de esta Suprema Corte de Justicia, quienes ejercerán sus funciones de manera conjunta.

La Comisión podrá requerir la colaboración y asesoramiento de las restantes áreas de la Suprema Corte, de organismos, de los Colegios de Magistrados y Funcionarios, Asociaciones Sindicales, del Colegiado de la Abogacía, y otros Colegios Profesionales, de las Universidades, de empresas y de expertos externos acreditados, cuando la complejidad técnica, jurídica o ética de las materias a tratar así lo requiera.

Art. 8: La integración de la Comisión de Gobernanza y Uso de la Inteligencia Artificial debe contar con participación de la representación legal de los trabajadores judiciales, así como también de perfiles técnicos, pudiendo establecerse mecanismos de cooperación o colaboración con el sector científico-tecnológico y universitario nacional. Ello dotará de mayor transparencia a la gestión de la Comisión y de mayor legitimidad a la hora de establecer marcos de trabajo con las herramientas propuestas, y hará posible la colaboración multiactor dispuesta en el art. 6.

Artículo 9: Funciones. La Comisión tendrá las siguientes funciones:
g) Propiciar la implementación de Agentes de Inteligencia Artificial, propios o externos, los que deberán cumplir estrictamente con los requisitos de seguridad, trazabilidad, auditoría, supervisión humana, individualización y demás principios rectores del presente Reglamento.

Art. 9: en cuanto al inciso g) “propiciar la implementación de Agentes de Inteligencia Artificial, propios o externos”, se propondrá la prohibición de tal supuesto en función de lo plasmado en el art. 19 inc. 2 del Reglamento, atento que implica una ampliación de la superficie de ataque cibernético, sumado al hecho de que los mismos han sido diseñados para actuar de manera autónoma para llegar al resultado requerido, es decir, prescinden de control humano en medio de la operatorias.

i) Publicar un informe anual sobre el estado de implementación de la IA en el ámbito de la Suprema Corte, los impactos identificados, las auditorías realizadas y las medidas adoptadas o recomendadas.

En relación al inciso i, la publicación de informes sobre el estado de implementación de tecnologías en el ámbito de la SCBA debería ser semestral, así como también los impactos identificados, auditorías realizadas y medidas adoptadas o recomendadas, a fin que el conjunto de los sujetos alcanzados y la población en general tenga conocimiento efectivo de estos aspectos, reforzando la transparencia y rendición de cuentas.

j) Elaborar, en coordinación con el Instituto de Estudios Judiciales, los programas de capacitación y actualización correspondientes, asegurando que contemplen las distintas funciones y niveles de responsabilidad del personal judicial.

Art. 9 inc. j La Asociación Judicial Bonaerense, en su calidad de representante sindical, participa de la elaboración de programas de capacitación y actualización coordinados por el Instituto de Estudios Judiciales para ampliar el alcance de formación. Su participación está avalada además por normas provinciales que incluyen la participación de la organización sindical en la garantía de estos derechos.

Tal es el caso de la Ley Micaela (art. 3 de la Res. SC N° 825/22 y art. 4 Ley nacional N° 27499) y de la Ley Yolanda (art. 4 Ley 15276).

Artículo 10. Selección del modelo de provisión tecnológica. "La Comisión" evaluará y propondrá, en cada caso, el modelo de provisión tecnológica (desarrollo interno, desarrollo a medida por tercero, sistema de código abierto o herramienta comercial), a propuesta de la Secretaría de Tecnología Informática, considerando las implicaciones de cada opción para la independencia judicial, la seguridad de la información, la transparencia, la explicabilidad y la auditabilidad. Se dará preferencia a modelos que permitan el mayor control institucional sobre los datos de entrenamiento, el funcionamiento del sistema y la corrección de errores.

Cuando se opte por proveedores externos, deberá suscribirse un convenio que garantice el acceso a auditorías algorítmicas y la compatibilidad con las leyes de protección de datos y con el presente Reglamento.

Art. 10: Se establecen requisitos más elevados para los proveedores nacionales que los extranjeros, colocando a los primeros en posición de desventaja, sin indicar los motivos, afectando los incentivos para el desarrollo de capacidades tecnológicas soberanas. No se indica cómo se garantizarán las auditorías algorítmicas. No se indica cómo la Comisión evaluará la conveniencia o no de determinado modelo de provisión tecnológica, ni los parámetros a considerar. Tampoco, si se someterá a escrutinio público de manera previa, con la finalidad de recibir observaciones. No se indica cómo se garantizará la realización de auditorías físicas, ni cómo se distribuirán las responsabilidades en caso de contratación con proveedores extranjeros. Como se indicó en el Bloque 2, se debe evitar en lo posible contratar a empresas extranjeras sometidas a jurisdicción de terceros estados que no han ratificado y/o adherido a los mismos tratados internacionales de DDHH o que no reconocen el mismo nivel de protección de DDHH que en nuestro país (al respecto, ver revelaciones caso Snowden, Assange, CLOUD Act, CALEA Act, Sección 702 FISA; tecnologías alcanzadas por el Acuerdo de Wassenaar; participación del proveedor en desarrollos militares; si se trata de personas jurídicas de derecho público extranjeras; aspectos geopolìticos, conflictos de intereses, entre otros). En este punto, se destaca que en el mes de febrero del corriente el Estado Argentino suscribió un acuerdo comercial con el gobierno de EEUU, donde se pretende brindar a este último estatus de país adecuado en términos de privacidad para la transferencia transfronteriza de datos personales.

Observación, fundamentación y/o redacción propuesta:

Art. 8: Se propone que la Comisión de Gobernanza esté integrada por las Secretarías de Planificación, de Tecnología Informática y de Servicios Jurisdiccionales de la SCBA, y también por representantes de los sectores mencionados en el párrafo 2, lo que dará mayor transparencia y legitimidad a las decisiones que se adopten. Las convocatorias a colaborar y asesorar a la Comisión deben ser permanentes, atento los niveles de riesgo que implica la adopción de estas tecnologías en un área crítica como el de Administración de Justicia.

Art. 9 inc. g: Se propone la prohibición de implementación de agentes de IA, atento implica serios riesgos para la seguridad y privacidad: acceso excesivo a datos sensibles, borrado de archivos o envío masivo de datos por fallos que permiten la interceptación, supresión o desvío de los mismos; inyección de instrucciones maliciosas (prompt injection), falta de posibilidades de control de su

autonomía operativa; imposibilidad de controlar el uso de agentes no autorizados por parte de los operadores, eludiendo los controles de seguridad del área de tecnologías; facilidad de propagación de errores o fallas a través de sistemas interconectados; creación de informes o fuentes falsas, o toma de decisiones en base a información o datos inventados. Los agentes de IA, dada su capacidad para ejecutar acciones sin intervención humana, amplían drásticamente la superficie de ataque y los daños potenciales, entre otros.

Art. 9 inc. i: se propone que los informes se publiquen semestralmente (como mínimo), a efectos de reforzar la transparencia y rendición de cuentas, y el acceso a la información pública.

Art. 9 inc. j incorporar a la representación sindical en la elaboración de programas de capacitación y actualización a efectos de contribuir a que la adquisición de conocimientos sea continua y escale, lo que a la vez incide en el desarrollo de capacidades cibernéticas propias.

Art. 10: las garantías enumeradas en el párrafo 2do. deben exigirse en todos los casos y requerirse mecanismos para que impacte en todos los participantes de la cadena de suministro, exigiendo a los proveedores el cumplimiento en función de sus capacidades.. En cuanto a la compatibilidad con las leyes de protección de datos y el Reglamento que dicte la SCBA, se remite a lo indicado por ONU en los "Principios Rectores sobre las Empresas y los Derechos Humanos" y a lo resuelto por la ONU en el informe "El derecho a la privacidad en la era digital". Se debe evitar a toda costa la prórroga de jurisdicción y competencia en materia de contratación informática, por tratarse de infraestructuras críticas y en defensa de la soberanía. Se recomienda tener en cuenta los riesgos para la privacidad y la seguridad mencionados al analizar el art. 6, teniendo en cuenta la función de garantía del Estado y la obligación que pesa sobre el mismo de controlar las infraestructuras que se encuentren en su territorio o jurisdicción, atento que el campo de las comunicaciones y las tecnologías es en la actualidad teatro de operaciones cibernéticas, incluso con impacto cinético (ver Reglas 1 y 2 Manual de Tallin 2.0 sobre Derecho Internacional aplicable a las operaciones cibernéticas de OTAN, Cambridge University Press, 2013). Teniendo en cuenta que la Ley 25326 es reglamentaria del art. 43 CN (en sintonía con los art. 12 DUDH, arts. 17 y 19 PIDCP, arts. 11, 12 y 13 CADH, entre otros), y la jerarquía que la CN da a los acuerdos como el referido, ubicándolos por debajo de los tratados internacionales del art. 75 inc. 22, y que prácticamente la totalidad de los derechos pueden verse afectados en caso de violaciones a la privacidad, es que se debe exigir que los proveedores cumplan con las normas de nuestro país y adecúen su operatoria a las exigencias que de ellas derivan; caso contrario, se compromete la responsabilidad internacional del Estado argentino. ONU ya indicó que la totalidad de la normativa de DDHH es plenamente aplicable y vigente en el entorno digital.

BLOQUE 4: Área técnica operativa: Secretaría de Tecnología Informática

Disposiciones del Anexo I comprendidas: Capítulo IV -arts. 14° y 15°.

Observación general X
Propuesta de modificación
Incorporación de texto X
Supresión de texto X

Artículo / inciso específico sobre el que recae el aporte (si corresponde)

La aplicación real de herramientas de IA en el sistema de administración de justicia otorga un rol activo y central de la Secretaría de Tecnología Informática, sumando nuevas tareas a las ya existentes, en un proceso de transición que supone trabajo intensivo en la aplicación de planes pilotos y nuevas herramientas, así como de su evaluación.

Los relevamientos realizados por la Asociación Judicial Bonaerense en ese sector de trabajadores indican problemas en la jerarquización del personal en tanto su formación técnica y profesional no es reconocida salarialmente. Por ejemplo, se identificaron algunas situaciones de trabajadores que poseen títulos técnicos y una antigüedad mayor a 15 años que actualmente tienen cargos correspondientes al nivel 12 (Of. 4°), 14 (Of. 2°) o 15.

Por tanto, es necesario que la Comisión de Gobernanza y Uso de Inteligencia Artificial tenga entre sus tareas determinar la cantidad o el volumen de trabajo que implica desarrollar las acciones incluidas en el presente Reglamento y, en particular, las especificadas en los caps. IV y X. En consonancia, se deberá analizar la capacidad existente en la planta actual para realizar las tareas encomendadas, realizar propuestas de jerarquización de las y los trabajadores del sector informático vinculado a sus funciones reales y formación y especificar cantidad y perfiles a incorporar en este nuevo proceso. En este sentido, sería importante otorgar oportunidades de formación a los y las trabajadoras que actualmente están en la planta posibilitando un reconocimiento a la trayectoria que priorice el conocimiento sobre el funcionamiento del sistema de administración de justicia.

Los avances en el proceso de digitalización y de implementación del expediente electrónico en la provincia de Buenos Aires y, en particular desde la pandemia por COVID-19, , este sector sufrió una sobrecarga de trabajo que muchas veces los llevó a extender su horario laboral por fuera de la jornada estipulada. Además se verificó gran variabilidad de la cantidad de puestos asistidos por agente (entre 50 y 129) y de usuarios a los que se brinda soporte en una diversidad de sistemas de gestión asistidos. Cabe destacar que sistemas como Augusta o el Portal de Notificaciones y Presentaciones Electrónicas implican asesorar a actores externos como, por ejemplo, abogados en el uso de los mismos. Además, se debe considerar cómo afecta la implementación de los nuevos sistemas al equipamiento actual tanto en términos de hardware como de software y los problemas que pueden ocasionarse debido al mal funcionamiento de equipos.

Artículo 14: La Secretaría de Tecnología Informática es el área técnica operativa en materia de sistemas de inteligencia artificial, teniendo a cargo su desarrollo, implementación, integración, operación y soporte técnico a lo largo de todo su ciclo de vida. A tales efectos, le corresponderá:

a) Evaluar su viabilidad técnica y compatibilidad;
b) Configurar, ajustar y, en su caso, entrenar modelos;
c) Implementar técnicamente los sistemas y casos de uso aprobados;
d) Gestionar y garantizar la calidad y resguardo de los datos utilizados;
e) Realizar pruebas, validaciones y monitoreo de desempeño;
f) Garantizar la trazabilidad, auditabilidad, seguridad, actualización y funcionamiento eficiente de los sistemas;
g) Detectar y reportar incidentes, errores, sesgos o desvíos;
h) Documentar su funcionamiento y evolución;

i) Adoptar las medidas de seguridad y de gestión de riesgos necesarias en la utilización de los sistemas de IA cuya utilización se habilite.
j) Brindar asistencia técnica y elaborar informes para la Autoridad de Aplicación.
k) Realizar auditorías periódicas sobre el desempeño de los sistemas en uso.

En el ejercicio de sus funciones, la Secretaría de Tecnología Informática deberá asegurar que los sistemas de inteligencia artificial sean desarrollados y operados de conformidad con los principios rectores establecidos en el presente Reglamento.

Art. 14: la Secretaría de Tecnología Informática deberá asegurar que los sistemas de inteligencia artificial sean desarrollados y operados de conformidad con los principios establecidos en el presente reglamento. A fin de garantizarlo, debería incluirse un proceso de formación previo a la implementación de planes pilotos; siempre y cuando se garantice lo expresado como observaciones para el bloque 2.

Artículo 15: Límite de las facultades técnico-operativas. En ningún caso las funciones asignadas a la Secretaría de Tecnología Informática implicarán facultades decisorias respecto de la aprobación, autorización o clasificación de los sistemas de inteligencia artificial. Dichas atribuciones corresponden exclusivamente a la Suprema Corte de Justicia a propuesta de la Comisión, conforme al procedimiento que oportunamente se establezca en el presente Reglamento.

Art. 15: se expresa que *en ningún caso* la Secretaría de Tecnología Informática tiene facultades decisorias sobre la aprobación, autorización o clasificación de los sistemas de inteligencia artificial dado que dichas atribuciones corresponden exclusivamente a la Suprema Corte de Justicia a propuesta de la Comisión. Esta formulación es taxativa y excluye la posibilidad de objetar ante la posibilidad de adoptar un sistema que pueda contener riesgos ignorados por las autoridades que no son idóneas en el tema.

Observación, fundamentación y/o redacción propuesta:

Se propone agregar al art. 14: “Para cumplir con las funciones encomendadas será necesario ampliar la planta de la Secretaría de Tecnología Informática, así como también evaluar la jerarquización del personal actual considerando y ponderando la idoneidad y formación específica que implica llevar adelante las tareas requeridas”.

Se propone agregar a las funciones de la Comisión especificadas en el art. 9 los siguientes incisos, dado que en ella se omite la evaluación de carga de trabajo y de incorporación de personal.

m) Determinar la cantidad o el volumen de trabajo que implica desarrollar las acciones incluidas en el presente Reglamento, especificando el impacto para la Secretaría de Tecnología Informática y sus delegaciones y potencialmente a otros sectores dentro del sistema de administración de justicia.

n) Analizar las capacidades existentes en el personal para asumir nuevas funciones, jerarquizando su formación técnico-profesional y estableciendo un sistema de promoción y capacitación que priorice a aquellos que se encuentran trabajando en el Poder Judicial para poder realizar nuevas funciones.

o) Determinar la cantidad de trabajadores y trabajadoras en el área de informática y otras a incorporar para cumplir con los objetivos propuestos.

BLOQUE 5: Niveles de riesgo: estratificación, sistemas de bajo y alto riesgo, sistemas prohibidos o restringidos.

Disposiciones del Anexo I comprendidas. Capítulo V -arts. 16° al 19°.

Observación general X
Propuesta de modificación X
Incorporación de texto X
Supresión de texto

Artículo / inciso específico sobre el que recae el aporte (si corresponde)

Artículo 16. A los efectos del presente Reglamento, los sistemas de IA se clasifican en tres categorías según su nivel de riesgo para los derechos de las partes, la independencia judicial y la integridad del proceso: sistemas de ***bajo riesgo****, sistemas de* ***alto riesgo*** *y* ***sistemas prohibidos o de uso expresamente restringido****. La clasificación de cada sistema será determinada por la Comisión y puesta a consideración de la Suprema Corte de Justicia para su aprobación.*

La Comisión deberá actualizar la clasificación ante cambios significativos en las funcionalidades, el contexto de uso o los hallazgos de auditorías o evaluaciones de impacto.

Art. 16: En cuanto a la clasificación de los sistemas, los informes y motivos que orienten a clasificarlos en un tipo u otro deben ser públicos. Se requiere mayores precisiones metodológicas que indiquen cómo se verificará qué clasificación corresponde asignar a cada tipo de sistema.

Artículo 17. Sistemas de IA de bajo riesgo — Gestión administrativa. Corresponden a esta categoría los sistemas de IA utilizados para funciones de gestión administrativa, que presentan bajo riesgo de afectación a los derechos fundamentales y alto potencial de mejora en eficiencia y acceso. Se encuentran incluidos, de manera enunciativa y no taxativa:
• Gestión documental, clasificación y organización de expedientes.
• Programación y asignación de audiencias.
• Anonimización y pseudo-anonimización de resoluciones judiciales.
• Transcripción automática de audiencias (voz a texto).
• Traducción de documentos a idiomas locales.
• Chatbots de atención ciudadana con información general sobre trámites.
• Estadísticas, indicadores de desempeño y análisis de plazos en los procesos judiciales.
• Corrección ortográfica y gramatical de documentos.

Art. 17: Sistemas de IA de bajo riesgo - Gestión administrativa: aunque sea bajo, el riesgo de afectación de derechos fundamentales es sustancialmente mayor que los beneficios que pudieran obtenerse. En todos los casos deben adoptarse medidas para garantizar la protección de datos personales, por las características propias de funcionamiento de dichas tecnologías. No enunciar

taxativamente impide conocer si se ha utilizado o no esta tecnología (shadow AI o uso de IA en las sombras, lo que se intenta prevenir, e incluso se prohíbe en el reglamento). En cuanto a las actividades enunciadas, algunas de ellas requieren de automatización, no necesariamente del uso de herramientas como las que se pretende regular. Algunas de las actividades enunciadas no implican utilización de sistemas de IA, sino automatización. En cuanto al uso para "Estadísticas, indicadores de desempeño y análisis de plazos en los procesos judiciales", se trata de uno de los tipos de usos prohibidos en el marco, por ejemplo, del EU IA Act: la realización de estas actividades implica el uso de telemetría es la forma en que se mide, recopila y analiza de manera remota el rendimiento, ubicación y comportamiento de la masa de trabajadores de todas las jerarquías. Se debe prohibir el uso destinado a monitorización, vigilancia y control y análisis conductual; y el uso de herramientas de este tipo en general. En caso que se determine que serán utilizadas, se deben cumplir con la información y notificación previa. En cuanto a la protección de los derechos de trabajadores que pudieran verse afectados por la implementación la "IA de bajo riesgo", se espera que se determine previamente el nivel de supervisión humana de las tareas que se verán modificadas, que contemplen información anticipada y consulta sindical previo a la implementación, que se evalúe el impacto y la gestión de riesgos laborales derivados de las modificaciones en el nuevo proceso, que se garantice el empleo y la reconversión profesional para quienes pudieran ver afectada su tarea y se garantice la protección de datos personales y prevención de sesgos algorítmicos en su aplicación, y la prevención en materia de seguridad e higiene.

Artículo 18. Sistemas de IA de alto riesgo. Apoyo a la función jurisdiccional. Corresponden a esta categoría los sistemas de IA que asisten funciones críticas de la función jurisdiccional, incluyendo la interpretación de normas, la valoración de pruebas, la predicción de resultados de litigios, el análisis de jurisprudencia y la generación de propuestas de resolución o sentencia.

Los sistemas de esta categoría solo podrán utilizarse en el ámbito de la Jurisdicción Administración de Justicia previo cumplimiento de los siguientes requisitos:

1. Análisis de Impacto Algorítmico favorable
2. Informe favorable de La Comisión y autorización expresa de la Suprema Corte.
3. Implementación de supervisión humana significativa
4. Mecanismos de impugnación accesibles para las partes procesales respecto de los resultados producidos por el sistema.
5. Registro en el repositorio público de sistemas de IA.
6. Plan de monitoreo continuo y revisión periódica aprobado por la Comisión.

Bajo ninguna circunstancia los sistemas de IA de alto riesgo sustituirán el juicio del juez. Sus resultados se emplearán exclusivamente como apoyo informativo, siendo la decisión final responsabilidad exclusiva de la persona juzgadora.

Art. 18: se propone la prohibición de implementar tecnologías que impliquen la asistencia de funciones críticas, tales como interpretación de normas, valoración de pruebas, predicción de resultados de litigios, análisis de jurisprudencia y generación de propuestas de resolución o sentencia. Se pretende, con ello, evitar la delegación cognitiva y vaciar de contenido la función jurisdiccional, que exige años de capacitación.

Artículo 19. Sistemas de IA prohibidos o de uso restringido. Quedan expresamente prohibidos en el ámbito de la Suprema Corte los siguientes usos de sistemas de IA:

1. La automatización plena de decisiones jurisdiccionales, incluidas las decisiones de admisibilidad, cautelares, de fondo o cualquier otra que la ley atribuya exclusivamente al juez.
2. El uso de sistemas de IA que operen sin posibilidad de supervisión humana real y efectiva sobre sus resultados.
3. El uso de herramientas de IA que reproduzcan sesgos discriminatorios por raza, género, origen, religión, condición económica, discapacidad u otro motivo.
4. El uso de herramientas de IA externas que procesen datos judiciales confidenciales sin las garantías de anonimización, cifrado y protección de datos personales, requeridas por la legislación nacional aplicable y el presente Reglamento.
5. El uso de sistemas de IA generativa cuyos términos de servicio autoricen al proveedor a utilizar los datos de los usuarios para el entrenamiento de modelos futuros, cuando dichos datos incluyan información judicial confidencial.
6. La generación de material probatorio de forma sintética o automatizada.
7. La utilización de sistemas de IA, para la elaboración total o parcial de informes o dictámenes periciales, sin la participación activa del perito habilitado conforme a la legislación procesal aplicable. Se entiende por participación activa la validación de la metodología empleada, la evaluación crítica de los resultados, la asunción personal de las conclusiones y la suscripción del dictamen con firma y sello profesional. La prohibición no alcanza a las operaciones computacionales que, por carecer de las capacidades definidas en el artículo 5, produzcan resultados determinísticos, verificables y reproducibles -tales como la verificación de funciones hash, la validación de firmas digitales conforme a la Ley N° 25.506 o la consulta de revocación de certificados digitales-, las que igualmente requerirán suscripción pericial con constancia del procedimiento y resultado. Cuando el dictamen incorpore ambas componentes, la prohibición se aplicará exclusivamente a la basada en sistemas de IA. El uso autorizado de sistemas de IA en pericias quedará sujeto a las obligaciones del artículo 29.
8. El uso de sistemas de predicción del riesgo de reincidencia con efectos vinculantes para decisiones de libertad, prisión preventiva o libertad condicional, salvo que exista norma legal expresa habilitante y previo Análisis de Impacto Algorítmico favorable con auditoría externa independiente.

La Comisión podrá recomendar la ampliación o reducción de esta nómina, para su consideración por parte de la Suprema Corte, ante la aparición de nuevas tecnologías o usos que se configuren riesgos equivalentes o superiores a los aquí enumerados, o en su caso, mitiguen los mismos.

Art. 19: La prohibición es adecuada, debiendo suprimirse las palabras “o de uso restringido”. Ello, atento que colocarlos como “prohibidos o de uso restringido” puede concretar el serio riesgo de que esos sistemas que, en principio se prohíbe utilizar, terminen siéndolo por vía de excepción (uso restringido), haciendo obsoleta la prohibición. Se debe tener en cuenta que el art. 19 inc. 2 incluye a los agentes de inteligencia artificial. Dentro de esta categoría se encuentra el uso de sistemas que impliquen manipulación conductual, explotación de vulnerabilidades (especialmente de grupos específicos); aquellos que impliquen identificación biométrica en tiempo real (ver precedente SRFP); categorización biométrica sensible; evaluación y/o predicción de delitos; elaboración de bases de datos faciales masivas o indiscriminadas mediante raspado no selectivo de fuentes abiertas para

crear o ampliar bases de datos de reconocimiento facial; reconocimiento y monitoreo emocional en espacios laborales; (ver sistemas de riesgo inaceptable EU AI Act).

Observación, fundamentación y/o redacción propuesta:

Art. 16: Se propone que la documentación que se elabore en los términos del art 16 sea pública, atento tratarse de herramientas que deberán ser auditadas en caso de uso, tal como prevé el reglamento, y con la finalidad de garantizar la transparencia y rendición de cuentas.

Art. 17: el listado debe ser taxativo. En cuanto a la anonimización y pseudoanonimización, ambas pueden realizarse mediante automatización, no siendo imprescindible el uso de IA. Para la transcripción automática de audiencias (voz a texto), se debe requerir el consentimiento informado (Ley N°25326), por tratarse de datos sensibles; en este caso, se debe aplicar una política ZDR (cero retención de datos).

En relación a la traducción de textos, la normativa procesal exige que dicha labor sea llevada adelante por traductores oficiales (art. 218, 255, 256 CPPBA), por lo que se debe suprimir dicha actividad del listado.

En cuanto a los chatbots de atención ciudadana, no se indica cómo serán desarrollados, mecanismos de privacidad, anonimización y seguridad (teniendo en cuenta que las personas vuelcan datos personales al interactuar con los mismos), ni se indica plazo de guarda. Se debe prohibir el uso de los registros de chats para entrenamiento de otros modelos, atento que las consultas versarán, en general, sobre asuntos judiciales del consultante. Se debe aplicar política ZDR. Se señala que el uso de estos chats no es útil para las personas que no saben leer ni escribir. En cuanto a las estadísticas y análisis de desempeño actualmente son elaboradas por los sistemas utilizados en la órbita de la SCBA (Augusta) y el MPBA (SIMP). En cuanto a los plazos, el cumplimiento de los mismos es una función del agente judicial, cuyas previsiones están insertas en los Códigos Procesales.

La utilización de softwares de productividad, geolocalización permanente y extracción de datos que permiten elaborar perfiles conductuales debe prohibirse. En caso que se decida avanzar igual sobre la intimidad de los trabajadores, acceder y revisar las comunicaciones electrónicas para monitorear rendimiento, resguardar herramientas y bienes de capital; o con motivo de recopilación de datos, seguridad informática, o de privacidad, se debe garantizar que las restricciones a la esfera de autodeterminación de trabajadores (incluidos los magistrados y funcionarios, peritos, etc), lo sea dentro de la reglamentación, con conocimiento previo y consentimiento del trabajador, conforme los criterios sentados por el Tribunal Europeo de DDHH en “Barbulescu II” (05/09/2017).

En cuanto a la corrección ortográfica y gramatical de documentos, se recomienda continuar utilizando las herramientas provistas por la SCBA a través de los sistemas operativos que ha contratado, teniendo en cuenta que los programas de procesamiento de texto suelen incluir dicha funcionalidad, no siendo necesario incorporar IA para ello.

Se propone agregar un párrafo: “La incorporación de tecnologías, incluidos los sistemas de bajo riesgo, en ningún caso implicará despido ni reducción de persona, debiendo en su caso recalificarse al trabajador y asignar nuevas funciones. Deberá: especificar el nivel de supervisión humana de las tareas modificadas o sustituidas; informar de manera anticipada y consultar a la organización sindical

previa implementación; realizar una evaluación de impacto y gestión de riesgos laborales, garantizar la reconversión profesional en los sectores afectados, proteger los datos personales y prevenir sesgos algorítmicos en los sistemas que se apliquen".

Art. 18: Se debe prohibir la utilización de estos sistemas para funciones críticas de la actividad jurisdiccional, incluyendo interpretación de normas, valoración de pruebas, etc., en consonancia con lo reglado en el art. 26 incs. 1, 2, 5. Los repositorios de sistemas de IA deben ser públicos, y las bases de datos utilizadas, también. Se debe realizar el Plan de monitoreo continuo y revisión periódica, mínimamente, cada seis meses.

Art 19: Se propone que el texto sea reemplazado por "Sistemas de IA prohibidos", por los motivos señalados previamente. A la hora de establecer prohibiciones (por ejemplo, la delegación de función jurisdiccional) debe aplicarse la legislación procesal pertinente. En cuanto al inc. 3, prácticamente todas las herramientas de este tipo reproducen sesgos discriminatorios (ver comentario Bloque 2).

En cuanto al art. 19 incs. 4 y 5, ver Bloques 2 y 8.

En cuanto al art. 19 inc. 7, hasta que no se obtengan las definiciones del art. 5, se debe prohibir también. En caso de autorizarse el uso para elaboración de pericias, debe contemplarse el estándar Daubert.

En relación al art. 19 inc. 8, sistemas como los indicados han sido prohibidos en el marco de la EU IA Act, por ejemplo, por generar, justamente, un riesgo cuya asunción debe ser prohibida.

En todos los casos, los sistemas que se pretendan utilizar deben ser diseñados y desarrollados por la SCBA o bajo su dirección.

BLOQUE 6: Análisis de impacto algorítmico, planes piloto, auditorías y evaluación de impacto

Disposiciones del Anexo I comprendidas: Capítulo VI -arts. 20° al 24°

Observación general X
Propuesta de modificación X
Incorporación de texto X
Supresión de texto X

Artículo / inciso específico sobre el que recae el aporte (si corresponde)

Artículo 20. Análisis de Impacto Algorítmico. Todo sistema de IA categorizado como de alto riesgo requerirá previo a su despliegue, de manera previa e ineludible, la realización de un Análisis de Impacto Algorítmico (AIA). El AIA deberá examinar, como mínimo:
a) El impacto probable del sistema sobre los derechos fundamentales de las partes y de los usuarios del servicio de justicia, con especial atención a los grupos en situación de vulnerabilidad;
b) La presencia de sesgos estructurales en los datos de entrenamiento y en el diseño del algoritmo;
c) Los niveles de precisión, fiabilidad, transparencia y explicabilidad del sistema en el contexto de uso previsto;
d) Los riesgos de seguridad, ciberseguridad y protección de datos personales;

e) La compatibilidad del sistema con el ordenamiento jurídico vigente y con los principios rectores del presente Reglamento.

Art. 20: Todos los sistemas informáticos en general, y aquellos englobados en la disciplina que se pretende regular, requieren, antes de su despliegue (pase a producción) la realización de análisis de impacto algorítmico. Esto incluye a los denominados de bajo riesgo. Incluso, el propio art. 9 inc. f del Reglamento así lo indica.

Artículo 21. Implementación por fases. Planes Pilotos. Todos los sistemas de IA calificados como de alto riesgo será sometido a una implementación por fases, iniciando con un plan piloto en un entorno controlado. La fase piloto permitirá evaluar la funcionalidad, el impacto potencial y los posibles riesgos del sistema antes de su despliegue a gran escala. Los resultados de la prueba piloto, incluyendo retroalimentación de los operadores judiciales participantes, serán documentados y considerados para la decisión de escalamiento.

Art. 21: En cuanto a los planes piloto, todos los sistemas deberían ser probados previo a su implementación, cfe. art. 9 inc. f del Reglamento. No se indica cómo será la implementación de sistemas de alto riesgo por fases, en qué consisten las mismas, ni cómo se establecerá dicho entorno controlado. Los resultados de las pruebas piloto deberían ser públicos.

Artículo 22. Evaluación de impacto algorítmico (EIA) Seguimiento post-despliegue. Una vez que un sistema de IA haya sido puesto en operación, "La Comisión" realizará, con la periodicidad establecida en el artículo siguiente, una Evaluación de Impacto Algorítmico (EIA). La EIA es el proceso que permite evaluar el desempeño efectivo del sistema en producción, detectar si han emergido sesgos no contemplados en el diseño, verificar si los datos utilizados han perdido representatividad, e identificar si cambios normativos o funcionales hacen necesario ajustar su funcionamiento.

Art. 22: A la evaluación de impacto algorítmico debe sumarse, también, la realización de evaluaciones de impacto ambiental.

Artículo 23. Auditorías algorítmicas periódicas. Las auditorías algorítmicas examinarán:

- *Cumplimiento de las normas legales nacionales y los principios establecidos en el presente Reglamento.*
- *Presencia de sesgos, inequidades o efectos discriminatorios en los resultados.*
- *Niveles de precisión, fiabilidad, transparencia y explicabilidad.*
- *Grado de supervisión humana efectiva ejercida sobre los resultados del sistema.*
- *Seguridad técnica y ciberseguridad del sistema.*

Los sistemas de IA en uso serán objeto de auditorías algorítmicas con la siguiente periodicidad mínima:

- *para sistemas de alto riesgo: semestral*
- *para sistemas de bajo riesgo: anual*

Los informes de auditoría serán públicos e incluirán recomendaciones de mejora, suspensión o desmantelamiento del sistema auditado. "La Comisión" adoptará las medidas correspondientes dentro de los treinta días hábiles siguientes a la recepción del informe

Art. 23: En el art. 19 se listan los casos de uso de "sistemas de IA prohibidos o de uso restringido". Siendo éstos los más peligrosos, en el art. 23 "Auditorías algorítmicas periódicas", se trata del único tipo de sistema clasificado al que no se le ha indicado la realización de estas evaluaciones ni el plazo.

Artículo 24. Desmantelamiento de sistemas incompatibles con derechos fundamentales. Cuando las auditorías algorítmicas, las evaluaciones de impacto o cualquier otro mecanismo de control detecten que un sistema de IA viola derechos fundamentales, incumple el presente Reglamento o resulta incompatible con el derecho internacional de los derechos humanos, la Comisión informará de inmediato a la Suprema Corte de Justicia, la que evaluará la suspensión inmediata de su uso y, en caso de corresponder el inicio del proceso de desmantelamiento.

Art. 24: No se indica cómo se llevará adelante el proceso de desmantelamiento, incluyendo las etapas. Nada se menciona sobre el desmantelamiento de las bases de datos, ni se menciona el borrado seguro o destrucción física de los datos en los casos de desmantelamiento. Tampoco, el plazo de retención que podría aplicarse en caso de conservación de datos, ni cuáles serían los parámetros para ello.

Observación, fundamentación y/o redacción propuesta:

Art. 20: Se propone que el análisis de impacto algorítmico se realice sobre la totalidad de los sistemas que se pretenda utilizar, cfe. art. 9 inc. f del Reglamento.

Art. 21: Se recomienda la implementación de planes piloto en la totalidad de los desarrollos que se lleven a cabo, cfe. art. 9 inc. f. Se debe precisar cómo se llevará adelante la implementación por fases en casos de sistemas de alto riesgo. Los informes o documentos que de ello surjan deben ser publicados para acceso irrestricto de la comunidad.

Art. 22: Se propone realizar evaluaciones de riesgos/ impacto en ciberseguridad., y de impacto ambiental, junto con las de impacto algorítmico.

Art. 23: Se debe establecer mecanismos para realizar auditorías mínimas periódicas también en el caso de los sistemas "prohibidos o de uso restringido", atento los señalamientos efectuados en el Bloque 5.

Art. 24: Se debe indicar cómo será el proceso de desmantelamiento, incluyendo las etapas. Se deben desmantelar también las bases de datos. No se indica cómo se garantizará que se realizará borrado seguro o destrucción física de los datos en los casos de desmantelamiento, especialmente, en caso de tratarse de proveedores externos nacionales y, particularmente, extranjeros. Se debe establecer claramente si tras el desmantelamiento habrá plazo de retención de datos o no, indicando tipos de datos, plazo de guarda, y motivos que justifiquen la decisión.

BLOQUE 7: Deberes de los operadores judiciales

Disposiciones del Anexo I comprendidas: Capítulo VII -arts. 25° y 26°

Observación general X
Propuesta de modificación X
Incorporación de texto X
Supresión de texto X

Artículo / inciso específico sobre el que recae el aporte (si corresponde)

Artículo 25. Deberes generales de uso informado. Los sujetos alcanzados por el artículo 2° del presente Reglamento que utilicen herramientas de IA en el ejercicio de sus funciones tienen el deber de:
1. Informarse, con carácter previo a la utilización de cualquier herramienta de IA, acerca de sus funcionalidades, limitaciones técnicas, riesgos conocidos —incluyendo alucinaciones y sesgos — y términos y condiciones de uso publicados por el proveedor;
2. Verificar que la herramienta que se pretende utilizar haya sido autorizada.
3. Abstenerse de utilizar chatbots de uso general en sus versiones de acceso gratuito para el desarrollo de tareas vinculadas a funciones jurisdiccionales o al tratamiento de información judicial;
4. Evaluar, antes de cada uso, si la tarea en cuestión puede ser realizada de manera más fiable o segura con herramientas que no impliquen IA generativa.

Art. 25: En el art. 5 se define al "operador judicial" como aquella persona que en ocasión de sus funciones utiliza estos sistemas, colocando en el agente la responsabilidad directa por el uso y sus consecuencias. La definición pareciera excluir a aquellos que no usan las herramientas propuestas. En cuanto a los deberes colocados en cabeza de los operadores, muchos deben ser garantizados por la organización. Se responsabiliza o se les exige a los usuarios cuestiones complejas (garantizar la fiabilidad de los sistemas, deber de capacitación y del impacto de la tecnología dando cuenta de origen, idoneidad, limitaciones, etc.), de las que probablemente no puedan dar cuenta o no cuenten con los medios necesarios para ello. La fiabilidad o seguridad de la herramienta debe ser evaluada en términos legales y técnicos cfe. Caps. III y IV del Reglamento propuesto. El deber de "informarse" sobre, entre otros aspectos, los TyC del proveedor, y teniendo en cuenta lo que surge de los arts. 10 y 12, implica necesariamente el acceso a los contratos suscriptos por la SCBA con los proveedores. Debe tenerse en cuenta la complejidad y extensión de los contratos, y los cambios en los mismos que introducen los proveedores, usualmente de forma unilateral.

El deber de abstenerse utilizar chatbots de acceso gratuito implica que solamente las personas que cuenten con medios económicos suficientes podrán acceder al uso de estas herramientas.

Respecto de la responsabilidad del trabajador judicial de cualquier jerarquía, el control de lo que realmente ocurre suele estar en manos de quienes proveen la infraestructura, limitando la autonomía del operador a aquello que el sistema le permite hacer -o no-. Incluso, en caso que la decisión del supervisor humano no estuviere contemplada en el espacio de opciones de la máquina, podría producirse un bloqueo operativo por rechazo del comando (la interfaz rechaza el comando

por no coincidir con los parámetros válidos programados), un error de integración o una anulación forzosa; clasificación errónea forzada; problemas y fallas de interpretación de la decisión humana, entre otros riesgos, como el sesgo de automatización, el de confirmación, y las cámaras de eco. A su vez, la rigidez del algoritmo impide al operador ejercer un control real. En caso de procesos donde hay hechos y circunstancias novedosas (edge case) la falta de flexibilidad del sistema podría anular cualquier beneficio de supervisión humana, e incluso condicionar el dictado de nuevos precedentes. A la hora de determinar la atribución de responsabilidad, debe compatibilizarse con la reglamentación vigente en la materia, niveles escalafonarios, responsabilidades funcionales atribuidas por ley, entre otros, con la finalidad de no desvirtuar la jerarquización laboral.

Artículo 26. Deberes específicos en la utilización de herramientas de IA. Los sujetos alcanzados por el presente Reglamento que usen herramientas de IA para el ejercicio de sus funciones deberán:
1. Prescindir de herramientas de IA para la valoración de medios probatorios, el escrutinio de hechos, la realización de juicios de valor y la solución de problemas jurídicos de fondo;
2. Prescindir de herramientas de IA para aplicar el ordenamiento jurídico, motivar o adoptar decisiones en un proceso, tomando como único o determinante fundamento las respuestas ofrecidas por el sistema;
3. Abstenerse de introducir, por cualquier medio, datos personales, información sensible, datos de investigaciones en curso o cualquier otro dato confidencial en herramientas de IA generativa de acceso público o comercial cuyos términos de servicio autoricen el uso de dichos datos para reentrenar modelos futuros o permitir el acceso de terceros;
4. Prescindir del uso de herramientas de IA si se advierte que sus resultados generan daños potenciales a los derechos humanos o producen resultados sesgados o discriminatorios;
5. Abstenerse de presentar como de autoría propia el texto o contenido elaborado íntegramente con herramientas de IA generativa, debiendo citar en forma adecuada y transparente los materiales producidos con su asistencia;
6. Verificar, contrastar y validar con fuentes fiables toda información, cita jurisprudencial, referencia normativa o análisis producido por un sistema de IA antes de incorporarlos a cualquier actuación judicial;
7. Reportar de inmediato a la Secretaría de Tecnología Informática cualquier fallo, comportamiento inesperado, resultado sesgado o impacto negativo identificado en un sistema de IA, conforme al procedimiento establecido en el artículo 32.

Art. 26. Inc. 3: la norma es correcta; se debe tener en cuenta que, por ejemplo, OpenAI (ChatGPT) utiliza todos los datos que se introducen para entrenar sus modelos por defecto; Google (Gemini) utiliza la información para entrenamiento, salvo que se trate de información de empresas con reglas estrictas de privacidad; en el caso de Anthropic (Claude) utilizan los datos para entrenamiento, prohibiéndolo solamente en los planes corporativos especiales. Esos datos, obtenidos en el marco de contratación para uso civil, son utilizados para entrenar sistemas que serán utilizados con fines militares. Al respecto, el Departamento de Defensa de EEUU firmó acuerdos con ocho de las principales empresas de IA (SpaceX, OpenAI, Google, NVIDIA, Reflection, Microsoft, AWS, Oracle) para integrar sus tecnologías en redes militares clasificadas.

Art. 26 inc. 4: las herramientas de IA tienen la capacidad de generar daños potenciales a los derechos humanos, producir resultados sesgados o discriminatorios. Incluso, los modelos generales (generativos) tienen la capacidad emergente de generar contenido ilegal.

Observación, fundamentación y/o redacción propuesta:

Art. 25. Se propone que la redacción comience: “Deberes generales de uso”. En cuanto a los deberes generales, se propone que la SCBA mantenga y actualice un repositorio público en línea con información sobre los términos y condiciones de uso del proveedor en los términos de la contratación efectuada, en los mismos términos del art. 30 propuesto en el Reglamento. Ello brindará la posibilidad de garantizar el acceso a la totalidad de los operadores judiciales, a la vez que fortalecerá la transparencia y rendición de cuentas.

En relación al deber de informarse sobre los términos y condiciones, y de abstención de uso de herramientas gratuitas, deberán destinarse fondos suficientes para proveer de acceso a los trabajadores a la herramienta que se les requiere que utilicen, no pudiendo trasladarse los costos operativos al trabajador, sea de la jerarquía que sea, ni a ninguno de los sujetos alcanzados. En cuanto al deber de evaluar si la tarea puede ser realizada de manera más fiable o segura sin usar IAG, para ello debe intervenir el área técnica informática.

En cuanto al deber de verificar que la herramienta haya sido autorizada, se propone también la elaboración por parte de la SCBA de un repositorio público en línea, actualizado, de las herramientas autorizadas, junto con sus versiones, debiendo preferirse los desarrollos propios, y aquellos que sean más compatibles con nuestro ordenamiento constitucional.

Esto se expresa en varios artículos y se reafirma en el Cap. VII sobre los deberes de los operadores judiciales. Cada persona es responsable de informarse antes de usar cualquier herramienta de IA de sus funcionalidades y limitaciones técnicas, así como de los términos y condiciones publicados por el proveedor. Esto implica la abstención del uso de chatbots. No se especifican consecuencias ni tipos de sanción por incumplimiento por lo que habría que especificar si se aplican los términos generales del reglamento disciplinario o lo que en su caso corresponda. Quedan especificadas las prohibiciones (art. 26).

En cuanto a los trabajadores judiciales en general, no se alude a la entrega de herramientas de trabajo (teléfonos oficiales, computadoras para trabajo remoto o fuera de la sede) ni a medidas vinculadas con capacitación. Se debe garantizar zero rating para la totalidad de los sitios web, servicios, aplicaciones y aquellos que en el futuro se implementen, de forma tal que no se trasladen costos operativos a los trabajadores, teniendo en cuenta que internet es esencial para la prestación de la tarea bajo la modalidad de teletrabajo, o en caso de realizar tareas fuera de la sede.

Se deberán tener en cuenta las situaciones donde el uso de la herramienta por parte de los trabajadores sea consecuencia de una decisión de un superior jerárquico.

Art. 26 inc. 5: Se recomienda establecerlo como prohibición, teniendo en cuenta lo reglado en el art. 19 inc. 1.

BLOQUE 8: Protección de datos personales

Disposiciones del Anexo I comprendidas: Capítulo VIII -arts. 27° y 28°

Observación general X
Propuesta de modificación
Incorporación de texto
Supresión de texto

Artículo / inciso específico sobre el que recae el aporte (si corresponde)

Artículo 27. Principios de protección de datos en el uso de IA El uso de sistemas de IA en la Jurisdicción Administración de Justicia deberá observar los siguientes principios en la protección de datos personales, sensibles, confidenciales:
1. Minimización de datos: Los sistemas de IA deberán requerir un mínimo de datos personales para funcionar. Se dará preferencia a sistemas que mejoren la privacidad por diseño.
2. Consentimiento informado: Se elaborarán e implementarán protocolos de consentimiento para el tratamiento de datos personales con herramientas de IA en el ámbito judicial, conforme a la legislación nacional de protección de datos aplicable.
3. Anonimización: Cuando los sistemas de IA procesen datos personales, se emplearán técnicas de anonimización, especialmente en la creación de bases de datos utilizadas para análisis jurídico o estudios de precedentes; salvo en los supuestos comprendidos en el último párrafo del artículo 10.
4. Control institucional: Solo se permitirá que personal debidamente calificado acceda a datos individuales con la competencia y necesidad de hacerlo. Los protocolos de datos especificarán quién puede acceder y bajo qué circunstancias.
5. Protección ante proveedores externos: Cuando el procesamiento de datos judiciales involucre proveedores externos o servicios en la nube, se garantizará que el nivel de protección ofrecido cumpla con los estándares legales locales y los estándares de seguridad que se establezcan.

Se debe garantizar la tutela efectiva de la privacidad y protección de datos personales. Como se indicó al analizar el art. 6, se debe tener en cuenta que hay Estados que no ofrecen los mismos niveles de protección que la República Argentina en materia de derechos humanos y garantías. En tal sentido, si se contrata con proveedores sujetos a la legislación extranjera (en cumplimiento de la ley 19550), los mismos deben cumplir con la legislación nacional. Al respecto, se recomienda tener en cuenta que en algunos países, tales como EEUU, rigen leyes como CALEA, que obligan a las empresas a efectuar modificaciones en sus infraestructuras para facilitar la vigilancia por parte de las fuerzas de seguridad gubernamentales, de forma tal que puedan acceder a la información almacenada por esos operadores sin necesidad de requerirla, lo que en nuestro país no está permitido (ver arts. 153, 153 bis, 157 bis, CP; Ley 27078; Ley 25326; Ley 19798 de Telecomunicaciones; Ley 25250 de Inteligencia, específicamente el art. 5; Ley 24240; entre otros). Cobra especial relevancia conocer las medidas de seguridad que se adoptarán teniendo en cuenta la multiplicidad de registros bajo custodia de la SCBA: de Juicios Universales, Banco de Datos Genéticos (que requieren tutela especial por el tipo de datos almacenados y su variedad); Registro Central de Aspirantes a Guardas con fines de adopción; Registro de Violencia Familiar, entre otros. Debe tenerse en cuenta también que la infraestructura de la SCBA interopera con otras infraestructuras públicas (registro de deudores alimentarios, por ejemplo).

Art. 27 inc. 1: Evaluar, además de la minimización de datos, la implementación de principios como once only (con las limitaciones establecidas por la CSJN en "Torres Abad"), y teniendo en cuenta la existencia concreta de riesgos tales como los concretados en los hechos que dieron lugar al fallo "Halabi" (CSJN) y "Colectivo de Abogados José Alvear Restrepo vs. Colombia" (CIDH).

Art. 27 inc. 2: tener en cuenta que el consentimiento informado debe cumplir con los requisitos de la Ley 25326, y además, se deberá verificar cómo se garantiza en el caso de que la persona que deba prestar consentimiento no cuente con capacidades para comprender lo que se le explica, o carezca de alfabetización. Los grupos vulnerables son los que mayores dificultades pueden tener para comprender el alcance real del consentimiento que prestan.

Se insiste en que la suscripción de acuerdos o tratados que pretendan brindar reconocimiento de país adecuado a Estados que no garantizan los mismos niveles de protección en la transferencia transfronteriza de datos, no pueden ser tenidos como válidos cuando atentan contra normas de jerarquía constitucional tales como los arts. 18, 19 y 43, además de aquellas contenidas en el art. 75 inc. 22. Incluso, se destaca que el principal tratado internacional de cibercriminalidad (Convenio de Budapest) es de jerarquía infraconstitucional, con lo cual incluso en relación a dicho Tratado, deben prevalecer los derechos y garantías consagrados en la Constitución Nacional y los tratados internacionales de DDHH en que la Argentina forma parte.

Artículo 28. Prohibición de compartir datos confidenciales con IA comercial. Los sujetos alcanzados, conforme el artículo 2 del presente Reglamento, no incluirán datos personales, información confidencial de las partes, datos de investigaciones en curso ni cualquier otro dato sensible en los prompts o instrucciones dirigidos a herramientas de IA generativa de acceso público o comercial, cuyos términos de servicio autoricen el uso de los datos ingresados para entrenar modelos futuros o permitir el acceso de terceros.

El art. 28 establece la prohibición de inserción de datos personales, información confidencial de las partes, datos de investigaciones en curso, ni cualquier otro dato sensible en los sistemas de IA generativa de acceso público o comercial cuando implique el uso de los datos para entrenamiento de modelos futuros. Para cumplir con ello, será necesario el desarrollo de sistemas y herramientas propios, lo que puede hacerse a través de laboratorios de informática propios, o bien en colaboración con el complejo científico-tecnológico y universitario provincial o nacional.

Observación, fundamentación y/o redacción propuesta:

Se debe dar estricto cumplimiento a la Ley 25326 y Ley 27699 observando además las normas indicadas previamente, por ser aquellas que regulan las tecnologías. Téngase en cuenta que tanto la Ley 25250 (art. 5), la, Ley 27078 (art. 5), Ley 19798 (arts. 14, 18, 19, 20, 21) y el art. 153 CP reglan la inviolabilidad de las comunicaciones (además de la tutela de los tratados internacionales del art. 75 inc. 22 CN, y los arts. 18 y 19 CN).

La responsabilidad primaria en materia de protección de datos en la órbita Administración de Justicia, debe ser siempre puesta en cabeza de la SCBA, por ser aquella la que determina las tecnologías que deben usarse. A su vez, esta protección alcanza la totalidad de los datos que

almacene, gestione, administre o trate, incluidos los datos de la totalidad de la masa de trabajadores, de todas las jerarquías.

En cuanto al art. 27 inc. 3, “anonimización”; se reitera lo dicho en relación al art. 10, siendo que no se puede exigir mayores recaudos a los proveedores nacionales, que sí se sujetan a nuestra legislación; que aquellos que se le exige a los proveedores externos, por los motivos mencionados.

En cuanto al art. 27 inc. 4, “Control Institucional”, se recomienda que se establezcan controles de acceso en función de la necesidad de saber.

Respecto del art. 27 inc. 5, “Protección ante proveedores externos”, se remite a lo dicho en el Bloque 2, Bloque 8, Bloque 7 infra, respecto de la incapacidad de los proveedores que están sometidos a legislación extranjera, de ser considerados “adecuados” en términos de privacidad, especialmente cuando no han suscripto tratados internacionales de DDHH, o adherido al Estatuto de Roma de la CPI. También, se destaca que los proveedores de determinados países, como EEUU, no pueden garantizar lo que la SCBA pretende en el reglamento, por los motivos expuestos, teniendo en cuenta que la información que gestiona y administra la administración de justicia es crítica. Debería verificarse que los proveedores, en caso de pertenecer a países miembros de la OTAN, cumplan acabadamente con la legislación vigente en nuestro país, tanto local como el derecho internacional humanitario. Ello, atento que se encuentra abierta una hipótesis de conflicto con uno de los países miembros de dicha organización, y teniendo en cuenta las previsiones que la propia OTAN ha tomado en relación a la guerra cibernética, y los medios y métodos de guerra.

Respecto del art. 28, ·”Prohibiciones de compartir datos confidenciales con IA comercial”, teniendo en cuenta que los desarrollos tecnológicos existentes, en su mayoría, son comerciales o de acceso público, se destaca nuevamente la importancia de desarrollar sistemas propios, lo cual puede realizarse a través de laboratorios de informática propios, lo que implicará la contratación de especialistas técnicos. De esa manera, y sin perjuicio de no insertar datos confidenciales, se debe esclarecer si la SCBA entrenará sus propios sistemas y modelos, entre otros aspectos de seguridad y privacidad (plazo de guarda, anonimización, pseudoanonimización).

BLOQUE 9: Transparencia: deber de informar a las partes y repositorio público de sistemas de IA.

Disposiciones del Anexo I comprendidas: Capítulo IX -arts. 29° y 30°

Observación general X
Propuesta de modificación
Incorporación de texto
Supresión de texto

Artículo / inciso específico sobre el que recae el aporte (si corresponde)

Artículo 29. Transparencia e integridad. Deber de información a las partes. Los operadores judiciales deberán informar expresamente sobre el uso de sistemas de IA generativa para la realización de labores, tareas o actividades institucionales.

En especial para actividades que terminan impactando y reflejándose en los procesos de adopción y emisión de decisiones sustanciales, los funcionarios y empleados harán explícito en el expediente, documento o decisión, el nombre de la herramienta usada, modelo y empresa proveedora; fecha en que fue usada; explicarán para qué fue empleada, el detalle sobre cómo fue usada; referirán la ubicación específica de los productos o resultados reproducidos, transcriptos o incorporados, con comillas, negrillas, letra cursiva o cualquier formato distintivo, para identificar claramente los textos de la decisión que fueron producidos directamente por la herramienta.
A los fines de este artículo, dichas manifestaciones o revelaciones podrán incluirse en el cuerpo principal del expediente o decisión, en notas a pie de página.
Esta obligación de información garantiza el derecho de las partes al debido proceso y a la impugnación efectiva.

Art. 29: En relación al contenido del informe de uso de herramientas del campo de la IA con la finalidad de identificar adecuadamente la herramienta utilizada, es necesario también indicar la versión del producto. Por otro lado, y siguiendo buenas prácticas en materia forense (teniendo en cuenta el derecho a recurrir y a impugnar acordados), y siguiendo el esquema propuesto en la Guía Integral de Empleo de la Informática Forense en el Proceso Penal (aprobada por Res. PG 483/16) deberían proveerse mecanismos que permitan elevar los niveles de confiabilidad, de manera que la utilización sea fundada y que pueda efectuarse un debido control, o en su caso impugnación. Cuanto menos, además de los puntos indicados en el art. 29 párrafo 2, debería consignarse por qué las acciones y métodos utilizados, incluida la elección de la herramienta, son los mejores cursos de acción posibles, o contar con un especialista que valide y verifique el proceso realizado. Se debe determinar una metodología, técnica o proceso adecuado, que permita su auditabilidad. Sin perjuicio de lo anterior, cuando se indica la forma en que deben consignarse "los productos o resultados reproducidos (…) para identificar claramente los textos de la decisión que fueron producidos por la herramienta", colisiona con la prohibición de uso para la elaboración de decisorios, atenta contra el principio republicano, y violenta las normas que establecen la potestad decisoria en cabeza del magistrado o funcionario.

Artículo 30. Repositorio público de sistemas de IA La Suprema Corte mantendrá un repositorio público en línea con información clave sobre los sistemas de IA adoptados. El repositorio incluirá, como mínimo, la siguiente información por cada sistema:
● Nombre, proveedor y versión del sistema.
● Propósito y funciones para las que fue adoptado.
● Tipo de datos utilizados para su entrenamiento (cuando sea de conocimiento de la institución). ● Carácter del modelo: propietario, código abierto o desarrollo interno.
● Resultados del Análisis de Impacto Algorítmico y de las auditorías realizadas.
● Indicación sobre si las decisiones adoptadas con apoyo del sistema son impugnables y el mecanismo correspondiente.
● Fecha de incorporación y fecha de la última actualización de la información.
El repositorio se actualizará al menos una vez al año. La información será presentada de forma comprensible para el público general, siguiendo los principios de datos abiertos FAIR: Findable, Accessible, Interoperable and Reusable.

Art. 30: En relación al repositorio público, no se explicitan los parámetros que permitan saber qué información se considera "clave" y cuál no; ello impide conocer los criterios de publicidad de la información, erosionando la confianza en las instituciones y la transparencia y rendición de cuentas. En relación a los tipos de datos de entrenamiento, se indica que será informado "cuando sea de conocimiento de la institución". Se recomienda verificar, fal menos, que los modelos o sistemas no hayan sido entrenados con datos obtenidos ilícitamente.

En cuanto a los mecanismos de impugnación de decisiones tomadas en el marco de un proceso judicial o administrativo, debe tenerse en consideración los mecanismos previstos en la normativa procesal.

Observación, fundamentación y/o redacción propuesta:

Art. 29: se propone incorporar al informe previsto en el 2do. párrafo la indicación de los motivos por los cuales se utiliza la herramienta, de conformidad con las previsiones del art 25 inc. 2 y 4, y art. 26, debiendo acreditarse el consentimiento informado del art. 27 inc. 2 del Reglamento. Para garantizar el debido proceso y la impugnación efectiva, se debe contar con un informe técnico.

Art 30: incorporar a la información que debe publicarse en el Repositorio público los resultados del análisis de impacto algorítmico, de privacidad, de ciberseguridad y ambiental.

Art. 30 último párrafo: "El repositorio se actualizará mensualmente. La información será presentada de forma comprensible para el público general, siguiendo los principios de datos abiertos, garantizando la accesibilidad, en idioma nacional".

Se propone que, dentro del repositorio de herramientas, se desarrollen aquellas que pueden beneficiar la labor judicial, por ejemplo, disminuyendo la exposición de los trabajadores que deben analizar cantidades ingentes de material de abuso y explotación sexual infantil (con las consecuencias psicológicas que implica para los trabajadores).

BLOQUE 10: Seguridad Informática y gestión de riesgos

Disposiciones del Anexo I comprendidas: Capítulo X -arts. 31 y 32°

Observación general X
Propuesta de modificación X
Incorporación de texto X
Supresión de texto

Artículo / inciso específico sobre el que recae el aporte (si corresponde)

Artículo 31. Medidas de seguridad y ciberseguridad previas al despliegue. Antes de desplegar cualquier sistema de IA, la Secretaría de Tecnología Informática Judicial deberá:
● *Poner a prueba la resiliencia del sistema ante ataques adversarios, incluidos ataques de inyección de prompts, extracción de datos, evasión y envenenamiento de datos.*

● *Establecer medidas técnicas, gerenciales y humanas para prevenir, controlar y mitigar riesgos e incidentes de ciberseguridad.*
● *Garantizar que el acceso a servicios en la nube utilizados para sistemas de IA cumpla con los estándares legales locales y los estándares de seguridad institucional.*
● *Implementar un sistema de gestión de riesgos con roles, responsabilidades y procedimientos claros a lo largo de todo el ciclo de vida del sistema.*

Art. 31: Se indica que "antes de desplegar cualquier sistema de IA" la STI "deberá poner a prueba la resiliencia del sistema ante ataques adversarios, incluidos ataques de inyección de prompts, extracción de datos, evasión y envenenamiento de datos", "Establecer medidas técnicas, gerenciales y humanas para prevenir, controlar y mitigar riesgos e incidentes de ciberseguridad"; "garantizar que el acceso a servicios en la nube utilizados para sistemas de IA cumpla con los estándares legales locales y (…) de seguridad institucional"; "implementar un sistema de gestión de riesgos con roles, responsabilidades y procedimientos claros a lo largo de todo el ciclo de vida del sistema".

Para poder considerar la implementación de un proyecto como el propuesto en el reglamento, primero se debe, como bien se indica, establecer una serie de medidas de seguridad y ciberseguridad previas sobre los sistemas a utilizar. Pero antes de eso, debe ponerse a prueba la resiliencia de la infraestructura tecnológica sobre la que operarán esos sistemas, es decir, la infraestructura judicial.

Artículo 32. Reporte y gestión de incidentes. Todo integrante de la organización judicial que identifique fallos, comportamientos inesperados, vulneraciones de seguridad, sesgos, alucinaciones o impactos negativos derivados de sistemas de inteligencia artificial deberá reportarlos de inmediato a la Secretaría de Tecnología Informática. La Secretaría de Tecnología Informática documentará y efectuará el análisis técnico de los incidentes reportados, elevando el correspondiente informe a la Comisión para su evaluación y eventual recomendación de medidas. De acuerdo con la gravedad, naturaleza o impacto del incidente, la Comisión podrá proponer a la Suprema Corte la adopción de medidas preventivas, correctivas, de mitigación, suspensión o desactivación del sistema involucrado. En caso de corresponder, será aplicable el procedimiento previsto en el artículo 24 del presente Reglamento.

ART. 32. Reporte y gestión de incidentes. El artículo es, en principio, adecuado. El problema radica en que, en la actualidad, no pueden reportarse incidentes ni fallas sobre el resto de la infraestructura cibernética del Poder Judicial, ni se cuentan con mecanismos que permitan identificar los criterios, ni tampoco hay un formulario o contacto específico para ello.

En el mes de octubre de 2022, tomó estado público que se encontraban a la venta en el mercado ilegal bases de datos con información sustraída a la SCBA. En ese caso, se informó que se trataba de un lote de información sobre magistrados y funcionarios de la propia SCBA, abarcando 15 mil registros con nombres de usuario, direcciones de correo electrónico, nombre completo, DNI, claves, entre otros.

Hacia el 30 de marzo de este año, hubo una mega filtración de datos de organismos gubernamentales de nuestro país. El día 02/04 en el sitio del MPBA se informó que se identificó "la filtración de un repositorio de información sobre agentes de este Poder Judicial que se encuentra

fuera de la órbita de custodia del Ministerio Público". Ese mismo día, la SCBA confirmó la filtración de datos de agentes judiciales. Es claro el interés de los trabajadores en las condiciones de ciberseguridad.

Observación, fundamentación y/o redacción propuesta:

Art. 31: El trabajo remoto, la deslocalización de los trabajadores y de la oficina judicial y la incorporación intensiva de tecnologías amplió la superficie de ataque, tornándose imprescindible atender la seguridad de las infraestructuras. La Resolución 1523/2019 de Jefatura de Gabinete de Ministros de la Nación aprobó la definición de infraestructuras críticas y de infraestructuras críticas de información estableciendo criterios para su identificación y la determinación de los sectores alcanzados, además del Glosario de términos de ciberseguridad. Según esta norma, el sector Administración de Justicia (y el Estado en general), queda abarcado por ambas definiciones. Se debe tener en cuenta el Decreto 8/2021 del Gobierno de la Provincia de Buenos Aires, que aprueba el Plan integral de ciberseguridad de la provincia de Buenos Aires, al que la SCBA adhirió en términos cuyos alcances no son conocidos, a través de la Res. SC 1649/21 que aprobó el Plan Integral de Seguridad Informática de la Suprema Corte de Justicia, y creó el Comité de Implementación y Seguimiento del Plan, integrada por quienes también participan de la Comisión de Gobernanza y Uso de la IA (arts. 7 y 8 del Reglamento). El Plan Integral aprobado se encuentra en el Anexo I pero no está disponible públicamente, lo que impide conocer su contenido y cómo se gestiona la seguridad informática de una infraestructura crítica, particularmente, un poder del Estado debido a la falta de publicidad.

A nivel nacional, la principal norma de referencia es la Decisión Administrativa nro. 641/21 de la Jefatura de Gabinete de Ministros, que establece los Requisitos Mínimos de Seguridad de la Información para el Sector Público Nacional, que también son de aplicación para los proveedores que contraten con las jurisdicciones alcanzadas. La JuFeJus fue la primera organización del país en adherir a dicha norma. Chaco lo hizo después del ataque de ransomware en enero de 2022.

Se debería, como mínimo, contar con una política de seguridad de la información aprobada por las máximas autoridades, notificada y difundida a todo el personal y a todos aquellos terceros involucrados; ser cumplida por la totalidad de los sujetos alcanzados, revisada anualmente, y utilizada como base para establecer todo el andamiaje que acompañará la plataforma tecnológica.

Se debe contar con mecanismos de autenticación, autorización y control de acceso robustos; uso de herramientas criptográficas (cifrado en tránsito y en reposo), seguridad física y ambiental; seguridad en las comunicaciones, gestión de incidentes de seguridad; gestión de activos informáticos, entre los que se encuentran las herramientas de trabajo (computadoras y teléfonos celulares); y capacitación y concientización continua.

Se propone incorporar un CERT, pudiendo seguir el modelo de CERT.ar o del formado en la Provincia de Buenos Aires.

Art. 32: Se propone la implementación de una Guía de notificación y gestión de incidentes de ciberseguridad, con base en la Disposición 3/2023 de la ex Dirección Nacional de Ciberseguridad de la República Argentina.

Se propone que la AJB, en su rol de veedor de las condiciones de salud y seguridad en las que se desarrolla el trabajo judicial, y teniendo en cuenta las circunstancias reseñadas, realice de forma

periódica, lo que en el ámbito corporativo y estatal se conoce como bug bounty, mediando notificación previa, con la finalidad de mejorar la seguridad informática en diferentes niveles, siempre en el marco de la legalidad y la ética. Se propone que esta tarea sea llevada a cabo con Universidades, facultades de ingeniería, y otros actores relevantes. Una experiencia que merece ser destacada es la llevada a cabo por el gobierno de Bolivia, cuyo Centro de gestión de incidentes fomenta la participación ciudadana mediante estas actividades. Empresas como Google, Apple, Meta, Intel, cuentan con programas de estas características.

En el caso de la AJB, brindaría posibilidades de participar en la construcción de capacidades cibernéticas, a la vez que permite a los trabajadores involucrarse activamente y conocer el estado de la seguridad de su entorno laboral (virtual) y de sus propios datos personales, y permite una construcción democrática. Una vez finalizada la actividad, se elevaría un informe con la totalidad de los hallazgos al responsable que la SCBA determine. Se recomienda, también, contar con mecanismos de divulgación responsable de fallas y vulnerabilidades, sin criminalizar al reportante que, en definitiva, está contribuyendo a la higiene del entorno cibernético.

BLOQUE 11: Disposiciones complementarias: actualización periódica del Reglamento.

Disposiciones del Anexo I comprendidas: Capítulo XI -art. 33°

X Observación general
X Propuesta de modificación
X Incorporación de texto
Supresión de texto

Artículo / inciso específico sobre el que recae el aporte (si corresponde)

Artículo 33. Actualización periódica del Reglamento. El presente Reglamento será objeto de revisión y actualización periódica, a los fines de reflejar cambios significativos en el estado del arte tecnológico, el marco normativo aplicable o los hallazgos de las auditorías y evaluaciones de impacto así lo aconsejen. La Comisión elevará al Tribunal las propuestas de modificación debidamente fundamentadas.

Art. 33. La actualización periódica del Reglamento no prevé la participación de los actores involucrados o la cadena de suministro en esta fase del proceso, quedando en manos de la Comisión y del Tribunal Superior la facultad de realizar cualquier modificación futura de manera inconsulta.

Por otra parte, no especifica cada cuánto tiempo se realizará la revisión y actualización. Tomando en cuenta los plazos estipulados para la realización de auditorías y evaluaciones de impacto (Bloque 6), debería realizarse como mínimo de manera semestral y como máximo por el plazo de un año.

Observación, fundamentación y/o redacción propuesta:

Se propone agregar como segundo párrafo: “Con una periodicidad mínima semestral o máxima anual, la Comisión convocará a los actores que integran la cadena de suministro (operadores,

proveedores, etc.) a participar del proceso de revisión y análisis de la implementación de sistemas de IA, su funcionamiento y el cumplimiento de los principios y postulados establecidos en el Reglamento, así como también analizarán los cambios en el estado del arte tecnológico en la medida que resulten significativos para su aplicación inmediata en el sistema de administración de justicia".

Modificar el tercer párrafo, agregando que la Comisión presentará los comentarios resultantes del proceso participativo al Tribunal: "la Comisión elevará los comentarios resultantes del proceso participativo al Tribunal, indicando las propuestas de modificación debidamente fundamentadas".

BLOQUE 12: Consideraciones generales sobre el Proyecto y otros aspectos no comprendidos en los bloques anteriores

Observaciones de carácter general, aspectos omitidos que se estime conveniente incorporar, o consideraciones de técnica legislativa.

Observación, fundamentación y/o redacción propuesta:

La Alta Comisionado de la ONU para los DDHH en el informe "El derecho a la privacidad en la era digital" (A/HRC/48/31) ha indicado que debe respetarse el derecho internacional humanitario, como así también, ha dado recomendaciones para la tutela de derechos en el ámbito digital, reconociéndose la plena aplicabilidad de la Carta de Naciones Unidas y demás tratados al àmbito digital, encomendando a "los Estados que prohíban las aplicaciones de IA que no puedan utilizarse con arreglo a la legislación sobre derechos humanos, al menos hasta que se establezcan garantías adecuadas y hasta el momento en que eso suceda". La introducción de modelos de caja negra o de tecnologías que no puedan ser sometidas a auditoría propicia que se vulnere la garantía de imparcialidad y la posibilidad de conocer los fundamentos de las decisiones.

Se debe evitar que la justicia sea tecnológicamente mediada y, por tanto, deshumanizada. El proceso de descentralización física del Poder Judicial y el Ministerio Público obedece a la obligación del Estado de garantizar el acceso a la justicia, lo que se traduce en facilitar que el justiciable pueda sortear tiempos y distancias. El acceso a la justicia mediado por tecnologías depende de factores como conectividad, capacidades cognitivas y de lectocomprensión de la persona, hardware adecuado para el acceso y utilización de los servicios y herramientas, entre otros. Y seguridad informática, junto con capacitación y formación continua de todos los trabajadores, desde los magistrados hasta los funcionarios y trabajadores de todas las áreas. Hasta que mínimamente tales condiciones no estén cumplidas, se debe precaver el uso de automatización o sistemas decisionales que pongan en riesgo la tutela judicial efectiva, teniendo en cuenta los compromisos, deberes y obligaciones asumidos por el Estado argentino frente a la Comunidad Internacional. En ese sentido, se estima pertinente no avanzar sobre aspectos regulatorios que se encuentran en cabeza del Poder Legislativo y que puedan afectar la seguridad jurídica de manera alguna.

En cuanto a su aplicación al ámbito administrativo, y teniendo en cuenta que la adopción de tecnologías incidirá en la organización, distribución y asignación del trabajo, y en la reglamentación que se aplicará, incluida la sancionatoria, se torna necesaria la participación de los trabajadores a través de sus representaciones sindicales, como así también de aquellos sectores que pudieren verse afectados de cualquier forma,, lo que propiciaría el ámbito adecuado para arribar a consensos garantizando la participación de todas las partes interesadas.

Se propone comenzar por la resolución de mejoras edilicias que permitan, a la par, la generación y fortalecimiento de capacidades cibernéticas, tanto a nivel de infraestructura, mediante la elaboración de un plan de infraestructura estratégica que contemple mejoras en las condiciones de trabajo y espacios suficientes que propicien la adquisición y desarrollo de hardware y software, puesta en funcionamiento de laboratorios de informática forense para garantizar el acceso a la justicia, la igualdad de armas y el derecho de defensa, y a la vez de generar los espacios para el desarrollo de nuevas herramientas que permitan mejorar significativamente la labor pericial; capacitación contínua de la totalidad de los agentes y también abierta a la comunidad; participación del ciudadano de a pie, la sociedad civil, la representación sindical legalmente constituida, la academia y el sector científico-tecnológico. De esta manera, se generarán capacidades soberanas que permitirán mejores condiciones para garantizar la plena operatividad de los DDHH, especialmente los derechos de los trabajadores y justiciables y, eventualmente, avanzar en la incorporación de aquellas herramientas que probadamente contribuyan de forma beneficiosa al propósito de afianzar la justicia, sin poner en juego la soberanía.

Referencias

- **Bibliográficas**

Asamblea General de las Naciones Unidas. (21 de marzo de 2024). *Aprovechar las oportunidades de sistemas de inteligencia artificial seguros, protegidos y fiables para el desarrollo sostenible* (A/RES/78/265). Organización de las Naciones Unidas. https://docs.un.org/es/A/RES/78/265

Asociación Argentina de Derecho del Trabajo y la Seguridad Social (2025), "Vigilancia digital, intimidad en el ámbito laboral y derecho a la desconexión: hacia una tutela efectiva de la persona trabajadora en la era de la gubernamentalidad técnica", presentación de ponencia para el Concurso de ponencias "Héctor Pedro Recalde - José Daniel Machado". XXV Congreso Nacional de DT y de la Seguridad Social de la Asociación Argentina de DT y de la Seguridad Social (5, 6 y 7 de noviembre de 2025).
https://www.aadtyss.org.ar/files/documentos/4664/Opus%20iustitiae%20pax%20-%20Vigilancia%20digital,%20intimidad%20en%20el%20ámbito%20laboral....pdf

Cambridge University Press (2013), *Manual de Tallin 2.0 sobre Derecho Internacional aplicable a las operaciones cibernéticas de OTAN*
https://www.cambridge.org/core/books/tallinn-manual-20-on-the-international-law-applicable-to-cyber-operations/E4FFD83EA790D7C4C3C28FC9CA2FB6C9

CEJA (2025), Inteligencia Artificial en los Poderes Judiciales. Reflexiones y lineamientos para las Américas.
https://cejamericas.org/wp-content/uploads/2025/12/Inteligencia-Artificial-en-los-Poderes-Judiciales-de-las-Americas_.pdf

CIPPEC (2026), Inteligencia artificial en el sistema judicial argentino: aprendizajes internacionales para una adopción responsable, Documentos de trabajo n° 230
https://www.cippec.org/wp-content/uploads/2026/04/DT-230-EyG-IA-en-el-sistema-judicial.pdf

Federación Judicial Argentina (2025), Inteligencia artificial y digitalización aplicada al ámbito de trabajo en el Poder Judicial

García Gómez, Mercedes Rosario (2025). El impacto de la inteligencia artificial en la privacidad de los datos personales en Argentina: desafíos y propuestas de reforma legal. [Tesis de maestría, Universidad de San Andrés. Departamento de Derecho]. Repositorio Digital San Andrés. https://dspaceapi.live.udesa.edu.ar/server/api/core/bitstreams/54356502-4e0e-4dbf-95a8-18f69b718fe4/content

Lazzarini, Carlos et. al (2022) Inteligencia artificial y política: los desafíos de una tecnología acelerada en las instituciones contemporáneas. https://www4.hcdn.gob.ar/icap/archivos/Inteligencia-artificial-y-politica-1668028317.pdf

Di Iorio, Ana Haydée [et al.]. (2019) Guía técnica para el diseño, implementación y gestión de laboratorios de informática forense. Info-Lab, Universidad FASTA. https://info-lab.org.ar/wp-content/uploads/2026/04/Guia-GT-LIF.pdf

OCDE, (2025), Gobernar con la inteligencia artificial: Panorama actual y hoja de ruta en las funciones centrales de gobierno, OECD Publishing, Paris, https://doi.org/10.1787/dc00e56a-es

Oficina Internacional del Trabajo (2025), Revolución de la seguridad y salud: Papel de la IA y la digitalización en el trabajo, Ginebra. https://www.ilo.org/sites/default/files/2025-04/ILO_Safeday25_Report_ES_r3%2B%281%29.pdf

ONU. Oficina del Alto Comisionado para los Derechos Humanos (ACNUDH) (2011). *Principios Rectores sobre las empresas y los derechos humanos: puesta en práctica del marco de las Naciones Unidas para "proteger, respetar y remediar"*. https://www.ohchr.org/sites/default/files/documents/publications/guidingprinciplesbusinesshr_sp.pdf

ONU, Consejo de Derechos Humanos (2011, 16 de junio). *Derechos humanos y empresas transnacionales y otras empresas* (Resolución A/HRC/RES/17/4). https://ap.ohchr.org/documents/dpage_e.aspx?si=A/HRC/RES/17/4

ONU, Consejo de Derechos Humanos (2011). *Informe del Representante Especial del Secretario General sobre la cuestión de los derechos humanos y las empresas transnacionales y otras empresas comerciales, John Ruggie. Principios Rectores sobre las empresas y los derechos humanos: puesta en práctica del marco de las Naciones Unidas para «proteger, respetar y remediar»* (Documento A/HRC/17/31). https://digitallibrary.un.org/record/705860?v=pdf

ONU. Asamblea General (2013). *El derecho a la privacidad en la era digital.* (Acuerdo A/C.3/68/L.45/). https://digitallibrary.un.org/record/761158?ln=es&v=pdf

ONU, Consejo de Derechos Humanos (2021). *El derecho a la privacidad en la era digital: Informe del Alto Comisionado de las Naciones Unidas para los Derechos Humanos* (A/HRC/48/31). https://docs.un.org/es/A/HRC/48/31

ONU (2025), *Informe de la Relatora Especial sobre la independencia de los magistrados y abogados,* Satterthwaite, Margaret. *La inteligencia artificial en los sistemas judiciales: promesas y escollos.* Naciones Unidas. A/80/169. https://docs.un.org/es/A/80/169

UNESCO (2024), *Directrices de la UNESCO para el uso de sistemas de inteligencia artificial en juzgados y tribunales* https://unesdoc.unesco.org/ark:/48223/pf0000390781_spa.locale=es

UNESCO (2026), *Directrices para el uso de sistemas de IA en Cortes y Tribunales*. https://unesdoc.unesco.org/ark:/48223/pf0000397770/PDF/397770spa.pdf.multi

Reglamento (UE) 2024/1689 del Parlamento Europeo y del Consejo, de 13 de junio de 2024, por el que se establecen normas armonizadas sobre inteligencia artificial (Ley de Inteligencia Artificial). *Diario Oficial de la Unión Europea*, L 2024/1689. https://eur-lex.europa.eu/eli/reg/2024/1689/oj/eng

Wolberg, Mario (2025) Desafíos y Recomendaciones para el Uso Responsable de la Inteligencia Artificial en el Sistema Judicial Argentino en Cuadernos Argentinos de Ciencias Forenses, Año 3, N° 2, citada en Revista de Pensamiento Penal https://www.pensamientopenal.com.ar/doctrina/91846-desafios-y-recomendaciones-uso-responsable-inteligencia-artificial-sistema-judicial

- **Normativas**

Convención de Viena sobre Derecho de los Tratados, arts. 27 y 31.

Constitución de la Nación Argentina, arts. 18, 19, 43, 75 inc. 22

Código Civil y Comercial de la Nación, art. 1757

Código Penal de la Nación, arts. 153, 153 bis y 157.

Ley N° 19.798, Ley de Telecomunicaciones

Ley N° 19.550, Ley de Sociedades Comerciales, Sección XV.

Ley N° 25.326, Ley de Protección de Datos Personales

Ley N° 25.675, Ley General del Ambiente

Ley N° 27.411, Convenio sobre Ciberdelito del Consejo de Europa (Convenio de Budapest)

Ley N° 27.566, Acuerdo de Escazú

Ley N° 27.078, Argentina Digital

Ley N° 27.499, Ley Micaela de Capacitación Obligatoria en Género para Todas las Personas que Integran los Tres Poderes del Estado, Art. 4

Ley N° 27.699, Ley de Protección de las Personas con respecto al Tratamiento Automatizado de Datos de Carácter Personal

Resolución 1523/2019 de la Jefatura de Gabinete de Ministros, Definición de Infraestructuras Críticas y de Infraestructuras Críticas de Información https://www.boletinoficial.gob.ar/detalleAviso/primera/216860/20190918

Decisión Administrativa 641/2021 de la Jefatura de Gabinete de Ministros, Requisitos Mínimos de Seguridad de la Información para organismos públicos https://www.argentina.gob.ar/normativa/nacional/decisi%C3%B3n_administrativa-641-2021-351345

Disposición 1/2021 de la Jefatura de Gabinete de Ministros, creación del Centro Nacional de Respuesta a Incidentes Informáticos (CERT.ar) https://www.boletinoficial.gob.ar/detalleAviso/primera/241077/20210222

Disposición 20/2022 de la Jefatura de Gabinete de Ministros, Estrategia aplicada al Programa Federal de Transformación Pública Digital https://www.argentina.gob.ar/normativa/nacional/norma-368811/texto

Disposición 3/2023 de la ex Dirección Nacional de Ciberseguridad, Guía de Notificación y Gestión de Incidentes de Ciberseguridad. https://www.argentina.gob.ar/normativa/nacional/disposición-3-2023-386227

Provincia de Buenos Aires

Decreto 8/2021 de la Provincia de Buenos Aires PBA Creación del “Plan Integral de Ciberseguridad” http://normas.gba.gob.ar/documentos/xpzbRYH3.html

Decreto 742/2026, publicado el 14 de julio de 2026 - Marco Provincial para el Desarrollo, Uso y Gobernanza de la Inteligencia Artificial en el sector público. Publicado en Boletín oficial: https://boletinoficial.gba.gob.ar/secciones/14274/ver p. 4 y 5.

Ley N° 11.922, Código Procesal Penal de la Provincia de Buenos Aires https://normas.gba.gob.ar/documentos/V9OGJUPx.html

Ley N° 27.699, Ley Micaela de Capacitación Obligatoria en Género para Todas las Personas que Integran los Tres Poderes del Estado, Art. 4

Resolución 9/2025 PBA - Reglas para el desarrollo, implementación y uso responsable de sistemas de Inteligencia Artificial -IA- para la Administración Pública de la Provincia de Buenos Aires. https://normas.gba.gob.ar/ar-b/resolucion/2025/9/549972; https://normas.gba.gob.ar/documentos/VwRM7Ju5.pdf

Suprema Corte de la Justicia de la provincia de Buenos Aires

Resolución PG 483/16, Guía Integral de Empleo de la Informática Forense

Resolución SC 1649/21, Plan Integral de Seguridad Informática de la Suprema Corte de Justicia elaborado por la Subsecretaría de Tecnología Informática

Resolución SC N° 825/22, obligatoriedad de la formación continua y permanente en materia de género, Art. 3

Resolución SC Nº 1719/26, Reglamento para el desarrollo y uso responsable de la Inteligencia Artificial en el Poder Judicial bonaerense

Resolución RP 747/26, Apertura y Actualización del Plazo del Proceso de Consulta Participativa Sobre el Reglamento de Uso de Inteligencia Artificial en el Poder Judicial

Resolución SC 2020/26, Ratificación de la Resolución RP 747/26

Resolución de Pte. 894/26, Prorroga en el plazo para la presentación de observaciones y aportes al "Reglamento para el desarrollo y uso responsable de la Inteligencia Artificial de la Suprema Corte de Justicia de la provincia de Buenos Aires"

- **Jurisprudencia**

Corte Suprema de Justicia de la Nación, 2009, Fallo "Halabi"

Corte Suprema de Justicia de la Nación, 2026, Fallo "Torres Abad"

Poder Judicial de la Ciudad de Buenos Aires, Amparo por Sistema de Reconocimiento Facial de Prófugos (SRFP) en la Ciudad de Buenos Aires *«Observatorio de Derecho Informático Argentino (ODIA) c/ GCBA s/ amparo»*

Corte Interamericana de Derechos Humanos, 2023, caso Miembros de la Corporación Colectivo de Abogados "José Alvear Restrepo" (CAJAR) Vs. Colombia

Corte Suprema de los Estados Unidos, 1993, fallo Daubert v. Merrell Dow Pharmaceuticals Inc. Plasmado luego en la Regla Federal de Evidencia N°702

Corte Suprema de los Estados Unidos, 2016, Caso COMPAS: State v. Loomis

Observatorio de Derecho Informático Argentino (O.D.I.A.), 2023, Causa N° 182908/2020

Tribunal Europeo de Derechos Humanos (Gran Sala), 2017, Caso Bărbulescu II.

- **Sitios web, referencias a artículos y material audiovisual**

CELS, Declaran inconstitucional el uso del sistema facial en CABA, publicado el 07/09/22, recuperado el 05/08/26 https://www.cels.org.ar/web/2022/09/una-jueza-declaro-inconstitucional-el-uso-del-sistema-de-reconocimiento-facial-en-caba/

Clarín, Ciberdelincuentes subieron datos sensibles de la Suprema Corte bonaerense y los venden online, publicado el 21/07/22, recuperado el 05/08/26

https://www.clarin.com/tecnologia/ciberdelincuentes-subieron-datos-sensibles-suprema-corte-bonaerense-venden-online_0_LmqIo6cy9T.html

Departamento de Guerra de los Estados Unidos, Acuerdos de IA en redes clasificadas, publicado el 01/05/26, recuperado el 05/08/26 https://www.war.gov/News/Releases/Release/Article/4475177/classified-networks-ai-agreements/

Diario judicial, “Promp Injection judicial”, publicada el 13/05/26, recuperado 05/08/26 https://www.diariojudicial.com/news-103427-prompt-injection-judicial

Hackers BO, recuperada 05/08/26 https://hackers.bo/

IBM, ¿Qué es la seguridad del agente de IA? Recuperado el 05/08/26: https://www.ibm.com/mx-es/think/topics/ai-agent-security

Ley de vigilancia de inteligencia extranjera, https://www.intelligence.gov/foreign-intelligence-surveillance-act

Ministerio Público de la provincia de Buenos Aires, Comunicado Incidente de Seguridad Informática, publicado el 02/04/26, recuperado 05/08/26 https://www.mpba.gov.ar/novedad/2635

Red Internacional de Organizaciones de Libertades Civiles (INCLO), documento elaborado por la sociedad civil como aporte a la Oficina del Alto Comisionado para los Derechos Humanos sobre los desafíos que la privacidad en la era digital plantea a los derechos humanos https://www.cels.org.ar/web/wp-content/uploads/2018/07/INCLO-OHCHR.pdf

Red UNIF, Disertación de Eduardo Grutzky Investigador / Desk Officer Grooming Stockholm. Policía de Suecia. "Proteger a los que protegen", publicado 02/10/24, recuperado 05/08/26 https://www.youtube.com/watch?v=Gt_048LkACI

Suprema Corte de Justicia de la provincia de Buenos Aires, Filtración de datos, publicado el 02/04/26, recuperado 05/08/26, https://www.scba.gov.ar/institucional/nota.asp?id=58623&veradjuntos=no

Wassenaar, ¿Qué es el AW? Recuperado el 05/08/26: https://www.wassenaar.org/es/about-us/