

Defensorías Inteligentes

Roí Corrado

Abogado, Universidad de Buenos Aires, Ministerio Público de la Defensa, Argentina

Resumen

El artículo presenta un proyecto integral para la incorporación estratégica de tecnología e inteligencia artificial en las Defensorías Públicas. A partir de experiencias documentadas como PROMETEA en Argentina, que redujo tiempos de tramitación hasta en un 99%, se demuestra que la automatización de tareas repetitivas libera tiempo profesional para el trabajo que requiere genuino criterio jurídico. El proyecto propone herramientas orientadas tanto a la eficiencia interna institucional (asistentes de redacción, búsqueda jurisprudencial, alertas procesales) como a mejorar el acceso de los asistidos (portales de consulta, traducción a lenguaje claro, notificaciones automáticas). Se enfatiza que la tecnología debe fortalecer el vínculo humano defensor-asistido, no reemplazarlo. El marco conceptual se sostiene sobre tres principios rectores: ética algorítmica, transparencia y centralidad en el defendido. La implementación se estructura en etapas graduales (diagnóstico, piloto, evaluación, escalamiento) con capacitación continua en uso ético de IA. Se identifican riesgos críticos como sesgos algorítmicos, brecha digital, dependencia tecnológica y seguridad de datos, proponiendo salvaguardas específicas. El artículo concluye que las defensorías enfrentan un momento de oportunidad institucional para transformar su servicio, con tecnología madura disponible y experiencias regionales que validan el camino, posicionando la innovación como instrumento de garantía del derecho de defensa efectiva.

Palabras clave: Inteligencia artificial, Defensa pública, Acceso a la justicia, *Legal Tech*, Derechos fundamentales

Sumario

1. Introducción. 2. Beneficios de la tecnología. 3. Posibles riesgos y desafíos. 4. Visión del proyecto. 5. Principios rectores. 6. Pilares del Proyecto 7. Ejemplos de herramientas tecnológicas. 8. Etapas de implementación. 9. Claves del proyecto. 10. Conclusiones.

1. Introducción

1.1. La tecnología en el contexto jurídico

El derecho no ha sido ajeno a la revolución tecnológica que atraviesa todas las esferas de la vida contemporánea. Lo que durante décadas fue un oficio apoyado casi exclusivamente en los libros,

los expediente en papel y la memoria del profesional, se encuentra hoy ante un conjunto de herramientas que redefinen la manera en que se presta y se accede al servicio jurídico. Comprender este fenómeno es el primer paso para que las Defensorías Públicas de la región puedan habitarlo de forma informada y con perspectiva institucional.

En ese marco, la expresión *Legal Tech* -tecnología legal- designa el ecosistema de soluciones digitales orientadas a optimizar la práctica del derecho, desde la elaboración automática de documentos hasta los sistemas de análisis predictivo de jurisprudencia (Solar Cayón, 2021, p. 126). Su desarrollo ha alterado sustancialmente la estructura del mercado legal al poner herramientas de inteligencia artificial al alcance de cualquier persona a través de plataformas digitales (Solar Cayón, 2021, p. 128). Para las instituciones públicas -y particularmente para la Defensa Pública-, ese escenario representa una oportunidad concreta. Democratizar dichas tecnologías de asesoramiento y ponerlas al servicio de quienes más las necesitan.

Dentro de ese ecosistema, la inteligencia artificial ocupa un lugar central. Se trata de sistemas que, mediante el procesamiento de grandes volúmenes de datos y el aprendizaje automático, identifican patrones, anticipan resultados y asisten en la toma de decisiones jurídicas (Corrado, 2025, p. 6). Van desde los asistentes de búsqueda jurisprudencial hasta los grandes modelos de lenguaje capaces de generar y/o reformular textos legales en fracciones del tiempo que demandaría un profesional. No es casual, entonces, que la gran mayoría de los abogados ya considere que la adopción de tecnología en las operaciones legales mejora su rendimiento y fortalece el vínculo con los clientes (Implementando inteligencia artificial generativa en estudios jurídicos y departamentos legales, 2024, Corvalán, 2024, p. 7).

Para las Defensorías Públicas todas estas herramientas tienen un potencial que va más allá de la eficiencia administrativa. Son, en la medida en que se las incorpore con criterio, instrumentos al servicio de la garantía constitucional de defensa efectiva. La pregunta que organiza el presente trabajo es cómo hacerlo de manera que la tecnología fortalezca el vínculo humano que define la labor de la defensa, en lugar de debilitarlo.

2. Beneficios de la tecnología

Hablar de tecnología en el ámbito de la defensa pública no es una promesa abstracta. La experiencia acumulada en distintas instituciones del sistema de justicia argentino permite medir, con números concretos, el tipo de transformación que la incorporación de herramientas tecnológicas produce en el trabajo cotidiano de un organismo público.

El caso más documentado en la región es el de PROMETEA, sistema de inteligencia artificial desarrollado en 2017 por el Ministerio Público Fiscal de la Ciudad Autónoma de Buenos Aires en conjunto con el laboratorio de IA de la Universidad de Buenos Aires. Su objetivo inicial fue la automatización de tareas reiterativas y la elaboración de dictámenes jurídicos basados en precedentes (Estevez, Linares Lejarraga y Fillottrani, 2020, p. 20). Los resultados medidos son elocuentes, en términos globales, si antes de PROMETEA la Fiscalía tardaba hasta tres meses en concluir expedientes con sus respectivos dictámenes, con el sistema ese plazo se redujo a cinco días como máximo, independientemente del tipo de caso (Estevez et al., 2020, p. 21).

Lo que estos datos revelan es que la tecnología libera tiempo profesional para el trabajo que realmente requiere juicio humano. En la Fiscalía, la reducción de tareas repetitivas permitió que el personal calificado dedicara más horas a los casos complejos, mejorando la calidad de sus dictámenes en esos expedientes específicos. Surgieron también, como consecuencia directa de esa ganancia de tiempo, actividades que antes simplemente no ocurrían: capacitación conjunta entre equipos, estudio de buenas prácticas internacionales, planificación estratégica de procesos (Estevez et al., 2020, p. 11). En definitiva, la tecnología reconvirtió de una forma favorable al personal.

Finalmente, vale señalar que más del 60% de la carga de trabajo de una fiscalía involucra casos reiterativos para los cuales existe una solución jurídica estandarizada (Estevez et al., 2020, p. 21). Si ese dato es razonablemente extrapolable a la estructura de trabajo de las defensorías - algo que requeriría verificación institucional propia, que es precisamente el diagnóstico previo que todo proyecto de este tipo debe contemplar-, entonces el potencial de mejora es sustancial. No porque la tecnología vaya a resolver los casos, sino porque puede encargarse de la arquitectura burocrática que hoy rodea cada uno de ellos.

2.2. Para los asistidos

La discusión sobre tecnología en la defensa pública suele quedarse en los beneficios internos, como si la institución fuera el único destinatario de la mejora. Ese enfoque es válido, pero incompleto. Hay una dimensión que pocas veces se nombra con la claridad que merece, y es la experiencia concreta de la persona asistida al intentar comunicarse con la institución que, por mandato constitucional, existe para defenderla.

Una persona detenida, o un familiar que busca información sobre su ser querido, experimenta a la defensoría pública como una línea telefónica que permanece ocupada. Como una mesa de entradas a la que llega después de horas de espera y donde le dicen que no pueden informarle porque el expediente no está en esa sede. Como también, la incertidumbre de no saber si tiene defensor asignado, quién es, cómo contactarlo y en qué estado está su causa. Esa incertidumbre en muchos casos es el equivalente práctico de no tener defensa, aunque jurídicamente el expediente tenga uno. La persona que desiste de seguir averiguando porque agotó sus llamadas sin respuesta ha sido, en los hechos, desconectada del proceso que la afecta directamente.

Este problema no nace de la negligencia ni de la falta de compromiso de quienes trabajan en las defensorías, nace de la desproporción estructural entre la demanda de información y la capacidad de respuesta de los canales disponibles. Las mesas de entrada y las líneas telefónicas no están diseñadas para absorber el volumen de consultas que genera la cantidad de personas asistidas; ese volumen desborda cualquier sistema que dependa exclusivamente del contacto humano para resolver consultas básicas y repetitivas.

La tecnología puede intervenir en este punto de manera directa. Un sistema de consulta digital permitiría que cualquier persona ingrese un número de causa o un dato mínimo de identificación y obtenga de forma inmediata información sobre el estado procesal de su expediente, el nombre y contacto de su defensor, las próximas audiencias agendadas o las obligaciones procesales vigentes. Algo similar hizo el Consejo de la Magistratura de la Ciudad de Buenos Aires con JustiBot, un chatbot accesible vía WhatsApp que, desde 2021, permite realizar consultas sobre el estado de causas, trámites frecuentes y derechos de los usuarios en lenguaje claro, sin necesidad de concurrir físicamente a ninguna sede (Vazquez, 2024).

Por otro lado hay una dimensión igual de importante que es la comprensión. El lenguaje jurídico es, para la mayoría de las personas asistidas por la defensa pública, un idioma ajeno. Términos como "sobreseimiento", "requerimiento de elevación a juicio", "medida cautelar" o "excarcelación" forman parte del vocabulario de quien trabaja en el sistema, pero son opacos para quien lo transita por primera vez y en condiciones de vulnerabilidad. La AAIP ha señalado que la comunicación con la ciudadanía debe ser "lo más clara y completa posible, utilizando un lenguaje comprensible por una persona no experta" (AAIP, 2023, p. 44). Los sistemas de traducción automática de terminología legal a lenguaje llano, integrados en plataformas de consulta, permiten que una persona entienda no solo qué ocurrió en su causa, sino qué significa lo que ocurrió.

En la misma línea, los sistemas de alertas automatizadas pueden operar como mecanismo de acompañamiento procesal. Una notificación que avise que existe una prohibición de contacto vigente, que la causa pasó a una instancia determinada, o que hay una audiencia programada, permite que el asistido o su entorno familiar no dependan de haber logrado comunicarse con alguien para estar informados. Esa autonomía informativa reduce el riesgo de incumplimientos procesales por desconocimiento, mejora la coordinación entre el asistido y su defensor, y devuelve a la persona una capacidad de seguimiento sobre su propio caso que el sistema, en su estado actual, le niega en la práctica.

3. Posibles riesgos y desafíos

Toda transformación institucional tiene costos y toda herramienta poderosa puede mal usarse. Reconocer los riesgos de la incorporación tecnológica en la defensa pública es un ejercicio para que el proyecto sea serio. Un análisis honesto de lo que puede salir mal es, en definitiva, lo que permite diseñar las salvaguardas necesarias para que no salga mal.

El primero y quizás el más subestimado de los desafíos es la resistencia al cambio por parte del personal. Incorporar nuevas herramientas en una institución que tiene sus propios ritmos, culturas de trabajo y jerarquías informales genera fricciones que ningún manual de implementación puede eliminar por decreto. El personal que lleva años trabajando de una determinada manera tiene razones legítimas para desconfiar de sistemas que no comprende del

todo, y esa desconfianza, si no se gestiona con tiempo y con pedagogía, se convierte en obstáculo activo.

La brecha digital es otro riesgo que merece atención particular en el contexto de la defensa pública. Los asistidos de las defensorías no son un grupo homogéneo, incluyen personas privadas de libertad, adultos mayores, personas en situación de pobreza extrema, individuos con escasa o nula alfabetización digital. Diseñar herramientas pensando solo en el usuario promedio con smartphone y conectividad estable significa dejar fuera precisamente a quienes más dependen del servicio.

Los sesgos algorítmicos representan el riesgo más técnico pero también uno de los más graves en términos de derechos. Un sistema de inteligencia artificial aprende de los datos con los que fue entrenado, y si esos datos reflejan desigualdades históricas -patrones de criminalización diferencial, sobrerrepresentación de ciertos grupos en determinados tipos de causas, disparidades en el acceso previo a la justicia- el sistema puede reproducir y amplificar esas desigualdades sin que nadie lo haya programado explícitamente para hacerlo. En mi tesina señalo que sin controles técnicos y jurídicos, las salidas de los sistemas algorítmicos tienden a reproducir asimetrías que el Derecho busca corregir, e introduzco el concepto de "tiranía del programador" para describir el escenario en que las decisiones de diseño de quienes construyeron el sistema terminan condicionando resultados jurídicos sin ningún tipo de rendición de cuentas (Corrado, 2025, p. 10).

En cuanto a la seguridad de los datos, una defensoría pública opera con información de alta sensibilidad: causas penales, situaciones de violencia, datos de personas vulnerables, estrategias de defensa. Los sistemas de IA son vulnerables a ataques cibernéticos que pueden comprometer su funcionamiento y resultar en la divulgación no autorizada de datos sensibles o en la manipulación de los resultados del modelo (AAIP, 2023, p. 17). Por eso, la infraestructura tecnológica que soporte cualquier sistema de la defensa pública debe estar alojada en servidores propios o nacionales, con control pleno por parte de la institución. Delegar ese alojamiento en proveedores externos -especialmente extranjeros- implica ceder la soberanía sobre información que pertenece a las personas asistidas y que en ningún caso debería circular fuera del ámbito institucional.

La dependencia tecnológica excesiva es un riesgo que se instala de manera silenciosa y progresiva. Cuando una institución organiza sus procesos en torno a herramientas que no controla ni comprende cabalmente, queda expuesta ante cualquier falla técnica, cambio de proveedor o discontinuación de servicio. Un sistema que funciona bien durante años puede crear la ilusión de que los procesos manuales que reemplazó ya no son necesarios, y esa ilusión se vuelve un problema grave el día que el sistema falla. Por eso la implementación debe ir acompañada siempre de documentación de procesos, capacidad de operación alternativa y auditorías periódicas que garanticen que la institución sigue siendo dueña de su propio funcionamiento.

Los costos de implementación y mantenimiento son una variable concreta que ningún proyecto puede ignorar. Desarrollar software propio requiere inversión inicial significativa y personal técnico sostenido en el tiempo. La alternativa de adquirir soluciones comerciales puede parecer más accesible a corto plazo, pero genera dependencia de terceros, y en el caso de proveedores privados, plantea los problemas de soberanía de datos ya mencionados. La sostenibilidad financiera del proyecto debe pensarse desde el primer día, con presupuesto específico, no como un apéndice de otros rubros institucionales.

4. Visión del proyecto

4.1. El norte del proyecto

Toda institución que emprende un proceso de transformación necesita saber hacia dónde va. Sin esa brújula, los proyectos técnicos se vuelven fines en sí mismos, y la acumulación de herramientas reemplaza a la pregunta más importante que es para qué sirven. La visión que orienta este proyecto es concreta y se puede formular en una sola idea, mejorar sustancialmente la asistencia técnica de los defendidos mediante la incorporación estratégica de tecnología, preservando el vínculo humano que define y da sentido a la labor de defensa.

Esa formulación implica compromisos institucionales concretos que vale la pena desarrollar.

El primero es el de una defensa más eficaz y personalizada. Hoy, la sobrecarga de causas hace que el tiempo disponible para cada asistido sea menor del que su situación requiere. Un defensor que destina horas a tareas administrativas, búsqueda de jurisprudencia o redacción de

escritos estándar tiene menos tiempo para escuchar, para construir una estrategia de defensa genuinamente adaptada al caso concreto y para conocer a la persona que defiende más allá del expediente. La tecnología puede devolver ese tiempo. Cuando las tareas repetitivas son asumidas por sistemas automáticos, el defensor recupera capacidad para ejercer el criterio jurídico al servicio de una persona real, con una historia real y con derechos que merecen una defensa a la altura de su complejidad.

El segundo compromiso es el de mayor transparencia en la gestión de los casos. Para una persona asistida, no saber qué ocurre en su causa genera una angustia que se suma a la que ya produce la situación procesal en sí. Un proyecto que incorpora tecnología con criterio puede hacer que esa información fluya de manera oportuna y comprensible, que el asistido sepa en qué etapa está su proceso, qué decisiones se tomaron y qué viene a continuación.

El tercero es garantizar el acceso igualitario a una defensa de calidad. Las defensorías públicas existen precisamente porque el acceso a la justicia no es igual para todos, y porque el Estado tiene la obligación de compensar esa desigualdad. Sin embargo, dentro del propio sistema de defensa pública pueden reproducirse desigualdades entre quienes tienen acceso a información y quienes no, entre quienes logran comunicarse con su defensor y quienes desisten en el camino, entre quienes entienden lo que ocurre en su causa y quienes lo viven como un proceso opaco que les sucede sin que puedan intervenir. La tecnología bien implementada puede reducir esas brechas internas, asegurando que la calidad del servicio no dependa del azar de qué defensoría tocó, qué capacidad de respuesta tiene esa sede o cuánto insistió la persona en comunicarse.

El cuarto elemento es el fortalecimiento de la institución pública. Una defensoría que incorpora tecnología de manera ordenada y con criterio se vuelve más capaz de cumplir su mandato, más eficiente en el uso de los recursos que la sociedad le confía y más robusta frente a la presión de un sistema judicial que, en toda la región, opera con volúmenes de causas que superan su capacidad estructural. Ese fortalecimiento institucional tiene valor en sí mismo. Una defensoría que demuestra capacidad de innovación y gestión basada en evidencia ocupa un lugar más sólido en el diálogo con los demás actores del sistema de justicia, y puede influir con mayor peso en cómo ese sistema se transforma.

En síntesis, la visión de este proyecto parte de la convicción de que la tecnología es útil en la medida en que sirve a las personas. En el contexto de la defensa pública, esas personas son, ante todo, quienes más necesitan que el Estado cumpla su promesa de protegerlas.

5. Principios rectores

5.1. Ética

El uso responsable de la inteligencia artificial en el ámbito de la defensa pública parte de la premisa que la tecnología no es éticamente neutral. Cada decisión de diseño, cada conjunto de datos utilizado para entrenar un modelo y cada proceso que se delega a un sistema automatizado produce efectos sobre personas reales, y esos efectos pueden ser beneficiosos o perjudiciales dependiendo de cómo se tome cada una de esas decisiones.

El respeto por los derechos fundamentales implica que antes de desplegar cualquier herramienta de inteligencia artificial en el trabajo jurídico, la institución debe poder responder con precisión qué derechos de las personas asistidas podrían verse afectados por su uso, y qué salvaguardas concretas están en funcionamiento para protegerlos. En mi tesina advierto que cuando se tratan grandes volúmenes de datos personales en el ámbito de la administración de justicia, los Estados tienen un deber de debida diligencia en derechos humanos a lo largo de todo el ciclo de vida tecnológico, desde el diseño hasta el despliegue y la supervisión continua (Corrado, 2025, p. 23). Ese deber pesa con particular intensidad sobre las defensorías, que trabajan con información de personas en situación de vulnerabilidad frente al poder del Estado.

La prevención de sesgos discriminatorios es, dentro del compromiso ético, el desafío más técnico y al mismo tiempo el más urgente desde el punto de vista de los derechos. Un sistema de inteligencia artificial puede reproducir y amplificar desigualdades históricas sin que nadie lo haya programado explícitamente para hacerlo, simplemente porque los datos con los que fue entrenado reflejan esas desigualdades. La AAIP señala que los sistemas de IA pueden perpetuar o incluso amplificar sesgos y discriminación si no se diseñan, implementan y supervisan adecuadamente, y que las herramientas de evaluación de riesgos en el sistema judicial pueden influir negativamente en decisiones que afectan la libertad de las personas (AAIP, 2023, p. 16). Por eso el principio ético exige auditorías periódicas de los sistemas en uso, participación humana real en las

decisiones que tienen consecuencias jurídicas relevantes, y un compromiso institucional sostenido con la revisión de los resultados que la tecnología produce.

5.2. Transparencia

La transparencia algorítmica es la condición que permite que el principio ético sea verificable. Una institución puede declarar que usa la inteligencia artificial de manera responsable, pero esa declaración solo tiene sustancia cuando existe la capacidad de explicar, con claridad y sin tecnicismos innecesarios, cómo funciona cada herramienta, qué datos procesa y cómo llega a sus sugerencias o resultados. La AAIP define la transparencia algorítmica como la capacidad de la organización para proporcionar explicaciones claras y comprensibles sobre cómo llega un modelo a sus predicciones y decisiones específicas, de modo que las personas puedan comprender los resultados y tengan la oportunidad de pedir explicaciones e información a la entidad responsable (AAIP, 2023, p. 36).

En el contexto de la defensa pública, esa obligación de explicabilidad tiene dos destinatarios. El primero es el propio equipo institucional, que debe ser capaz de entender qué hace cada herramienta que utiliza y de detectar cuándo sus resultados merecen ser cuestionados. El segundo es la persona asistida, que tiene derecho a saber cuándo un sistema automatizado participó en el procesamiento de información sobre su causa y a recibir una explicación comprensible de qué función cumplió ese sistema. Este derecho se desprende directamente del derecho de defensa, que exige poder comprender y eventualmente cuestionar los elementos que intervinieron en el proceso.

La rendición de cuentas institucional cierra este principio. Una defensoría que incorpora tecnología asume también la responsabilidad de comunicar, de manera regular y accesible, qué herramientas utiliza, con qué finalidad, bajo qué condiciones y con qué resultados. Esa rendición de cuentas fortalece la confianza de las personas asistidas en la institución y genera los incentivos correctos para que el uso de la tecnología se mantenga dentro de los límites que los principios éticos establecen.

5.3. Centralidad en el defendido

Si los dos principios anteriores establecen el marco ético y la condición de verificabilidad, este tercero define el propósito al que todo lo demás debe orientarse. La tecnología que se incorpore en las defensorías públicas existe para mejorar la defensa que recibe cada persona asistida. Cuando una herramienta no contribuye a ese objetivo, su presencia en la institución requiere una justificación muy sólida que, en la mayoría de los casos, no existirá.

Que la tecnología sea un medio y no un fin significa, en la práctica, que ninguna decisión de implementación puede tomarse a partir de la lógica de la novedad tecnológica o del prestigio institucional que puede otorgar decir que se usa inteligencia artificial. Cada herramienta debe poder responder a una pregunta concreta: ¿en qué mejora la situación de la persona asistida? Si esa pregunta no tiene una respuesta clara, la herramienta no tiene lugar en el proyecto.

La prioridad del interés del asistido implica que cuando exista tensión entre la eficiencia institucional y el bienestar de la persona asistida, el segundo prevalece. La tecnología puede hacer que la institución procese más causas en menos tiempo, pero ese aumento de velocidad pierde su valor si se produce a costa de la calidad de atención que recibe cada persona. La eficiencia es un medio para servir mejor, y cuando deja de cumplir esa función, deja de ser un valor.

Finalmente, la accesibilidad universal exige que ninguna herramienta tecnológica produzca exclusiones. Las personas asistidas por las defensorías públicas son, en su gran mayoría, personas que ya enfrentan barreras significativas para acceder al sistema de justicia. Incorporar tecnología que solo funciona para quienes tienen conectividad estable, alfabetización digital o dispositivos adecuados significa reproducir dentro de la institución las mismas desigualdades que la institución existe para corregir. Cada herramienta debe diseñarse o adaptarse de modo que sea accesible para las personas más alejadas del sistema, y cuando eso no sea posible, debe garantizarse siempre una alternativa humana real (AAIP, 2023, p. 44).

6. Pilares del proyecto

El proyecto se sostiene sobre cuatro pilares interdependientes. La eficacia interna potencia el acceso de los asistidos, la capacitación hace posible que ambos funcionen bien, y el cambio cultural permite que los otros tres se sostengan en el tiempo. El primer pilar –la eficacia interna–

agrupa herramientas orientadas a mejorar la gestión de las defensorías para liberar capacidad profesional: sistemas de búsqueda y análisis de jurisprudencia que reducen de horas a minutos la identificación de antecedentes relevantes, asistentes de redacción que generan borradores de escritos estándar, alertas automáticas de vencimientos procesales y flujos integrados de comunicación entre defensores, peritos y equipos de apoyo. La eficacia interna no es un fin administrativo sino la condición que hace posible una defensa de mayor calidad para cada persona asistida.

El segundo pilar –acceso de los asistidos- se ocupa de la relación entre la institución y las personas que asiste, con foco en información y comunicación. Incluye canales de consulta digital accesibles desde dispositivos de uso masivo, sistemas de traducción de terminología jurídica a lenguaje comprensible, notificaciones automáticas sobre novedades procesales y portales donde cada asistido puede seguir el estado de su expediente. Su propósito es reducir la distancia entre la persona y la institución que la defiende, para que esa distancia deje de ser obstáculo para el ejercicio efectivo del derecho de defensa.

El tercer pilar -la capacitación- reconoce que son las personas que usan la tecnología quienes determinan si produce los efectos esperados. La formación permanente no es una etapa que se cumple antes de lanzar el proyecto y luego se concluye, sino un proceso continuo que acompaña cada etapa y se actualiza a medida que las herramientas evolucionan. Esa formación abarca tanto el uso técnico como la comprensión de los límites de los sistemas, la capacidad de identificar cuándo un resultado algorítmico merece ser cuestionado y el manejo de los criterios éticos que deben guiar cada decisión. Corvalán y Ferré (2024) identificaron la capacitación continua como uno de los factores más determinantes en el éxito de la implementación de inteligencia artificial en entornos jurídicos, señalando que las organizaciones que invierten en formación sostenida obtienen resultados cualitativamente superiores a las que tratan la capacitación como un trámite inicial.

El cuarto pilar es el más difícil de medir y, posiblemente, el más decisivo para la sostenibilidad del proyecto -el cambio cultural-. Una institución puede adquirir las mejores herramientas disponibles y capacitar a su personal en su uso, y aun así ver cómo la implementación fracasa si la cultura organizacional resiste el cambio de fondo. El cambio

cultural implica que la innovación pase a ser parte de la identidad institucional, que la pregunta sobre cómo mejorar los procesos se instale como una práctica habitual y que el personal vea la tecnología como un recurso que amplía su capacidad de hacer bien su trabajo. Esto requiere liderazgo institucional genuino, reconocimiento de quienes impulsan mejoras, tolerancia al error como parte del aprendizaje y una comunicación interna que explique el sentido del proyecto más allá de sus aspectos técnicos.

7. Ejemplos de herramientas tecnológicas

7.1. Para eficiencia interna

Los ejemplos que siguen son aplicaciones que ya existen, ya funcionan en entornos jurídicos reales y cuya adaptación al contexto específico de una defensoría pública es técnicamente viable con los recursos institucionales disponibles.

El primero es el de los asistentes de redacción de escritos judiciales. Un defensor produce a lo largo de su jornada una cantidad significativa de documentos que comparten estructura, encabezados y fórmulas procesales comunes: apelaciones, incidentes, presentaciones de mero trámite, oficios, informes. Un sistema de inteligencia artificial entrenado con los modelos propios de la defensoría puede generar borradores completos de esos escritos a partir de los datos del expediente, que el defensor revisa, ajusta y firma. La experiencia de PROMETEA mostró que la elaboración de documentos estándar pasó de más de una hora a minutos, y que esa ganancia se traduce directamente en mayor disponibilidad para el trabajo que requiere criterio jurídico real (Estevez et al., 2020, p. 21).

En la misma línea operan los sistemas de búsqueda y análisis de jurisprudencia. Hoy, sin inteligencia artificial, identificar los antecedentes relevantes para una estrategia de defensa puede llevar horas de revisión manual de bases de datos. Un sistema de búsqueda semántica permite ingresar los hechos del caso en lenguaje natural y obtener en segundos los fallos más relevantes, ordenados por pertinencia y con un resumen de sus fundamentos principales.

Los chatbots para consultas internas frecuentes abordan un problema diferente pero igualmente concreto. Dentro de cualquier defensoría circulan diariamente preguntas que tienen respuestas estándar: plazos procesales aplicables a determinado fuero, requisitos para solicitar

una medida cautelar, modelos de escritos para trámites específicos, criterios institucionales sobre determinadas líneas de defensa. Un asistente conversacional entrenado con la normativa interna y la doctrina institucional puede responder esas consultas de manera inmediata, sin que el personal deba interrumpir a un colega o buscar en documentos dispersos.

El sistema de alertas automáticas de vencimientos procesales resuelve uno de los riesgos más simples y más graves de la práctica diaria, el olvido de un plazo. Integrado con el sistema de gestión judicial, este tipo de herramienta notifica con anticipación configurable cada vencimiento relevante de la agenda procesal, tanto al defensor a cargo como a quien lo reemplaza en su ausencia. La sincronización con el calendario institucional permite además que esas alertas se articulen con las agendas de audiencias, las intervenciones del Cuerpo de Peritos y Consultores Técnicos y las coordinaciones con equipos interdisciplinarios, que en la actualidad suelen gestionarse por canales separados sin integración automática.

El análisis de riesgos procesales mediante inteligencia artificial es quizás la herramienta más sofisticada de este grupo. A partir de los datos de un expediente y de patrones identificados en causas anteriores similares, un sistema puede estimar la probabilidad de distintos resultados procesales, identificar los argumentos que históricamente resultaron más eficaces en casos análogos y señalar los puntos débiles de la estrategia de defensa en curso. Esta herramienta no reemplaza el criterio del defensor, sino que lo informa con una base empírica que sería imposible construir manualmente dado el volumen de causas.

7.2. Para asistidos

Las herramientas orientadas a los asistidos parten de un diagnóstico que dice que la principal barrera que enfrentan las personas asistidas no suele ser la falta de voluntad institucional de atenderlas, sino la imposibilidad práctica de procesar el volumen de consultas que generan con los canales disponibles. Las herramientas de este grupo apuntan a descomprimir esa tensión estructural.

El portal de consulta del estado de la causa es la más inmediata. Una persona asistida debería poder ingresar un número de expediente o un dato básico de identificación en una plataforma accesible desde cualquier dispositivo con conexión y obtener en segundos la

información sobre en qué etapa procesal se encuentra su causa, qué ocurrió en la última audiencia, cuál es el nombre y contacto de su defensor y cuándo está agendada la próxima instancia. Ese canal, disponible las veinticuatro horas, absorbe la mayor parte de las consultas que hoy saturan las líneas telefónicas y las mesas de entrada, dejando esos canales disponibles para las situaciones que genuinamente requieren interacción humana.

La traducción automática de terminología jurídica a lenguaje claro complementa ese acceso con comprensión. Saber que la causa está en etapa de "requerimiento de elevación a juicio" es diferente de entender qué significa eso en términos concretos para la situación de la persona. Un sistema de traducción integrado en el portal puede ofrecer, junto a cada novedad procesal, una explicación en lenguaje accesible de qué implica esa novedad y qué pasos siguen a continuación.

El sistema de alertas sobre prohibiciones de contacto responde a una necesidad específica y urgente en causas que involucran violencia. Cuando existe una prohibición de acercamiento o de contacto vigente, tanto el imputado como su entorno familiar inmediato muchas veces desconocen el alcance exacto de esa restricción o no reciben aviso cuando sus condiciones cambian. Una notificación automática cada vez que se modifica el estado de esa medida cautelar reduce el riesgo de incumplimientos involuntarios que pueden tener consecuencias procesales graves para el asistido.

En la misma lógica operan las notificaciones sobre rebeldías y paraderos. Hay asistidos que pierden contacto con su defensoría sin ser conscientes de las consecuencias que eso genera para su causa. Un sistema que detecta automáticamente la situación de rebeldía declarada y activa un canal de notificación hacia los datos de contacto registrados puede recuperar ese vínculo antes de que el perjuicio procesal se consolide.

Finalmente, la visualización de la cronología del caso en formato amigable permite que la persona asistida entienda su proceso como una secuencia de hechos conectados, y no como una serie de novedades aisladas cuyo sentido se pierde sin contexto. Una línea de tiempo visual, con lenguaje claro y con la posibilidad de acceder a una explicación de cada hito, convierte la historia de la causa en algo legible para quien lo protagoniza.

8. Etapas de implementación

Es imposible pensar que un proyecto de estas características se construye de una sola vez. La experiencia en implementaciones similares dentro del sistema de justicia argentino muestra que los proyectos que intentan transformar todo simultáneamente tienden a colapsar, mientras que los que avanzan por etapas bien delimitadas logran aprender, corregir y consolidar antes de escalar.

La etapa de diagnóstico implica recorrer las defensorías del país, conversar con defensores, secretarios, personal administrativo y equipos de apoyo interdisciplinario, y escuchar con genuina atención qué funciona, qué no funciona y dónde están los puntos de mayor presión cotidiana. Esas conversaciones tienen el objetivo concreto de construir un mapa preciso de las necesidades reales antes de proponer soluciones. El riesgo de saltar este paso es diseñar herramientas que resuelven problemas inexistentes y dejan sin respuesta los que sí existen. La experiencia de PROMETEA fue elocuente. Su implementación exitosa dependió de haber hecho primero un diagnóstico detallado de procesos, gobernanza de datos y reingeniería organizacional antes de desarrollar cualquier aplicación tecnológica (Estevez et al., 2020, p. 21).

A partir de ese diagnóstico, el equipo interdisciplinario debe construir la arquitectura del plan: qué herramientas se desarrollarán primero, con qué criterios se seleccionará la defensoría piloto, qué indicadores se medirán para evaluar resultados y qué condiciones mínimas debe cumplir una sede para participar en la fase siguiente. La defensoría piloto debe reunir condiciones adecuadas para que el aprendizaje sea representativo y transferible, con volumen de causas suficiente para datos significativos, equipo con disposición a participar activamente e infraestructura tecnológica básica que permita la implementación sin inversiones previas de gran escala.

Una vez seleccionada, la implementación se realiza de manera controlada, introduciendo las herramientas gradualmente y con acompañamiento permanente del equipo técnico. La capacitación del equipo piloto es intensiva porque cumple doble función, asegura que las herramientas se usen correctamente desde el inicio y convierte a ese equipo en los primeros referentes internos del proyecto, personas que luego acompañarán la expansión hacia otras sedes desde la autoridad que da la experiencia directa. El monitoreo es continuo y sistemático,

registrando qué funciona según lo previsto, qué produce resultados distintos a los esperados y qué genera resistencias o dificultades que el diseño no anticipó. Esa información es el insumo más valioso porque es la única manera de saber si las herramientas producen en condiciones reales los efectos prometidos en condiciones de diseño.

Concluida la fase piloto, el proyecto hace una pausa deliberada para procesar lo aprendido. Un error identificado aquí, antes del escalamiento, cuesta infinitamente menos que el mismo error detectado cuando ya está replicado en decenas de sedes. El análisis de resultados compara los indicadores relevados durante el piloto con los objetivos establecidos en el diagnóstico, identifica dónde se alcanzaron los resultados esperados, dónde no y por qué, qué problemas surgieron imprevistos y qué herramientas funcionaron mejor de lo anticipado. A partir de ese análisis se realizan los ajustes necesarios, tanto en las herramientas como en los procesos de implementación y capacitación, y se prepara la documentación que guiará la expansión hacia las demás sedes.

El escalamiento no es una réplica mecánica del piloto sino una expansión que incorpora lo aprendido en cada paso previo. Las defensorías se suman progresivamente, siguiendo un orden que puede responder a criterios de tamaño, volumen de causas, disponibilidad de infraestructura o disposición institucional, según lo que el diagnóstico haya revelado sobre las condiciones de cada sede. La capacitación adopta un formato más amplio pero mantiene la misma profundidad que en la fase piloto. Los referentes formados durante el piloto juegan un rol activo, acompañando a sus colegas de otras sedes desde el conocimiento práctico acumulado. El soporte técnico continuo garantiza que ninguna defensoría quede sola frente a los problemas que inevitablemente surgen, y la evaluación permanente de resultados asegura que el proyecto no pierda su capacidad de autocorrección a medida que crece.

A lo largo de todas las etapas, sin excepción, corre un hilo que no puede interrumpirse ni relegarse a un momento específico del proceso. La formación en inteligencia artificial y en ética algorítmica es un proceso continuo que acompaña cada nueva herramienta, cada nuevo grupo de personas que se incorpora al proyecto y cada cambio en las condiciones tecnológicas del entorno. Esa formación abarca la comprensión básica de cómo funcionan los sistemas de inteligencia artificial que se están usando, la capacidad de identificar cuándo un resultado merece ser

cuestionado, el manejo de los criterios éticos que deben guiar cada decisión de uso y el conocimiento de los derechos de las personas asistidas en relación con el uso de tecnología en su causa. La AAIP señala que la diversidad de conocimientos en los equipos es fundamental para comprender las implicaciones sociales del uso de IA, evitar sesgos y discriminación, y priorizar soluciones centradas en el usuario (AAIP, 2023, p. 36).

Esa diversidad se construye con formación sostenida, no con una capacitación inicial que se agota en sí misma. La protección de datos personales forma parte de este hilo desde el primer día. Cada persona que participa del proyecto, en cualquier etapa y función, debe comprender qué datos maneja, bajo qué condiciones puede hacerlo y qué obligaciones tiene frente a la información de las personas asistidas.

9. Claves del proyecto

9.1. Ética algorítmica

La convicción que sostiene este proyecto es que la inteligencia artificial puede generar cambios genuinamente positivos en la defensa pública, siempre que su uso esté anclado en criterios éticos verificables y no solo declarados. Esa convicción reconoce también que la misma tecnología que puede mejorar la calidad de una defensa puede, si se usa sin los controles adecuados, profundizar las desigualdades que el sistema de defensa pública existe para corregir. La ética algorítmica es, en consecuencia, una de las condiciones de funcionamiento del proyecto, presente en cada etapa y en cada decisión de implementación.

La prevención de sesgos algorítmicos requiere una atención que comienza antes del despliegue de cualquier herramienta. Los datos con los que se entrena un sistema de inteligencia artificial reflejan el pasado, y el pasado del sistema de justicia está atravesado por desigualdades estructurales de género, clase y origen étnico que ningún modelo aprende a corregir por sí solo. Se advierte que sin controles técnicos y jurídicos, las salidas de los sistemas algorítmicos tienden a reproducir asimetrías que el Derecho busca corregir, incorporando en la motivación jurídica criterios contrarios al derecho antidiscriminatorio cuando los datos o el diseño del modelo arrastran desigualdades previas (Corrado, 2025, p. 10). Para una defensoría que trabaja

mayoritariamente con personas en situación de vulnerabilidad, ese riesgo merece una vigilancia permanente y metodológica.

Las auditorías regulares de los sistemas en uso son el mecanismo concreto que hace operativa esa vigilancia. Una auditoría algorítmica revisa si los resultados que produce el sistema son consistentes con los valores institucionales, si generan diferencias injustificadas entre grupos de asistidos y si los criterios que el modelo aplica siguen siendo apropiados a medida que cambian las condiciones del entorno jurídico. Esas auditorías deben tener periodicidad establecida, metodología documentada y resultados comunicados con transparencia al interior de la institución.

La participación humana en las decisiones críticas es el límite que ningún nivel de automatización puede cruzar. En el trabajo de una defensoría, las decisiones críticas son aquellas que afectan de manera directa la estrategia de defensa, la relación con el asistido o el ejercicio de un derecho fundamental. En esos puntos, el sistema puede informar, sugerir y asistir, pero la decisión final pertenece al defensor. El juicio humano tiene en el ejercicio de la defensa un rol que ninguna herramienta algorítmica puede asumir, y preservarlo en los momentos que más importan es parte constitutiva del modelo que este proyecto propone.

9.2. Gobernanza de datos

Los sistemas de inteligencia artificial viven de datos. Su calidad, su organización y las reglas que gobiernan su uso determinan, en gran medida, la calidad de los resultados que el sistema produce. Una defensoría que incorpora tecnología sin una estrategia de gobernanza de datos construye sobre una base endeble, las herramientas más sofisticadas producen resultados deficientes si los datos que las alimentan son inconsistentes, incompletos o están mal clasificados.

El análisis de datos para identificar patrones es una de las aplicaciones más valiosas de esta dimensión. Una defensoría que sistematiza la información de sus causas puede identificar, por ejemplo, en qué tipos de proceso se concentran los mayores tiempos de tramitación, qué argumentos de defensa resultaron más eficaces en casos similares ante determinados tribunales, o en qué etapas procesales se producen con mayor frecuencia los errores que perjudican al asistido. Esa información, analizada de manera agregada y con los resguardos de privacidad

correspondientes, permite tomar decisiones institucionales basadas en evidencia en lugar de en intuición.

La mejora continua basada en evidencia exige que los datos generados por el propio funcionamiento del sistema sean utilizados para ajustar y optimizar las herramientas en uso. Un proyecto que se lanza y no mide sus resultados no puede aprender ni corregir. La medición sistemática de indicadores relevantes, con criterios definidos desde el inicio, es la condición para que la implementación tecnológica sea un proceso dinámico.

9.3. Seguridad de software

Una defensoría pública maneja información entre las más sensibles que produce el sistema de justicia: estrategias de defensa, situaciones de personas privadas de libertad, datos de víctimas, condiciones de vulnerabilidad de los asistidos. La seguridad de los sistemas que procesan esa información hace a la integridad de la institución y a la protección de los derechos de las personas asistidas.

El punto de partida es la soberanía sobre los datos. Una defensoría que aloja su información en servidores de proveedores externos, especialmente extranjeros, pierde el control efectivo sobre esa información y queda sujeta a regulaciones, decisiones comerciales y riesgos de seguridad que están fuera de su alcance institucional. El Informe IAs Poder Judicial de Vazquez, señala que mantener cierto grado de autonomía tecnológica es deseable para evitar quedar a merced de decisiones comerciales externas, y que algunas jurisdicciones ya optaron por montar instancias propias o nubes privadas para preservar ese control (Vazquez, 2024). La infraestructura que soporte los sistemas de la defensoría debe estar alojada en servidores propios o nacionales, con control pleno por parte de la institución sobre el acceso, la gestión y el destino de los datos.

La protección contra accesos no autorizados requiere medidas técnicas concretas, sistemas de autenticación robusta para el acceso a los sistemas, registro trazable de todas las operaciones realizadas sobre datos sensibles, y políticas claras sobre qué personas tienen acceso a qué información y bajo qué condiciones. La AAIP señala que la seguridad en el tratamiento de datos personales implica la implementación de medidas técnicas y organizativas adecuadas para

proteger los datos contra el acceso no autorizado, la divulgación, la alteración y la destrucción (AAIP, 2023, p. 33).

Los planes de contingencia ante incidentes son el reconocimiento realista de que ningún sistema es infalible. Tener definido de antemano qué hacer cuando se produce una falla, una filtración o un ataque reduce el tiempo de respuesta, limita el daño y permite comunicar con transparencia qué ocurrió y qué medidas se tomaron. Finalmente, las auditorías de seguridad periódicas, realizadas por equipos con independencia del área que administra los sistemas, permiten identificar vulnerabilidades antes de que sean explotadas y mantener la infraestructura actualizada frente a un entorno de amenazas que evoluciona permanentemente.

10. Conclusión

A lo largo de este artículo se fue construyendo un argumento que, en su forma más simple, puede formularse así: las defensorías públicas tienen frente a sí una oportunidad concreta de mejorar de manera sustancial la calidad de la defensa que brindan, y esa oportunidad tiene nombre, tiene ejemplos documentados y tiene un camino metodológico trazado. Aprovecharla o dejarla pasar es una decisión institucional que tiene consecuencias directas sobre las personas que el sistema de defensa pública existe para proteger.

La tecnología aplicada al ámbito jurídico demostró, con datos medibles y en condiciones reales, que puede transformar el funcionamiento de las instituciones de justicia. PROMETEA redujo el tiempo de elaboración de dictámenes de 72 a 18 minutos en promedio, acortó los plazos de los amparos habitacionales de 190 a 42 días y permitió que los profesionales que antes dedicaban su jornada a tareas repetitivas pudieran ocupar ese tiempo en los casos que verdaderamente requieren su criterio jurídico. En el Poder Judicial del Chaco, la automatización de documentos en juicios ejecutivos representó un ahorro equivalente a 320 jornadas laborales completas en un solo año. Esos números son tiempo devuelto al trabajo que importa, y en el contexto de una defensoría pública, ese tiempo se traduce en defensas más preparadas, en asistidos mejor informados y en procesos con mayor calidad jurídica.

Pero la importancia de la tecnología para la defensa pública va más allá de la eficiencia interna. El argumento central de este artículo es que la transformación tecnológica bien orientada

es, ante todo, una forma de honrar el compromiso con los defendidos. Una persona que pasa días intentando comunicarse con su defensoría sin obtener respuesta, que desconoce en qué etapa está su causa, que no entiende el lenguaje en que se escribe su propio proceso, está siendo privada en los hechos de una parte del derecho de defensa que el sistema le reconoce en el papel. La tecnología puede cerrar esa brecha, y cuando lo hace en el contexto específico de la defensa pública, produce un efecto que trasciende la gestión institucional y alcanza la dimensión de las garantías fundamentales.

El proyecto que este artículo describe es escalable porque parte de una lógica acumulativa, cada etapa genera aprendizaje que alimenta la siguiente, cada defensoría que se suma al proceso lo hace con el respaldo de la experiencia acumulada en las anteriores, y cada herramienta que se ajusta en función de los resultados medidos se vuelve más eficaz en su siguiente iteración. La visión de largo plazo es la de un sistema de defensa pública que comparte desarrollos, protocolos y lecciones aprendidas entre las distintas jurisdicciones, reduciendo costos, evitando duplicaciones y construyendo una capacidad colectiva que ninguna defensoría podría desarrollar en soledad. Los modelos de colaboración interprovincial que ya se están produciendo en el ámbito del Poder Judicial argentino, como el acuerdo entre Mendoza y San Juan para desarrollar proyectos de innovación conjunta, señalan que esa lógica de trabajo en red es posible y produce resultados concretos (Vazquez, 2024).

Nada de lo que este artículo propone exige esperar condiciones ideales. La experiencia acumulada en la región muestra con claridad que los proyectos de transformación tecnológica en el sistema de justicia que resultaron exitosos no esperaron tener todos los recursos disponibles antes de comenzar. Se comenzó con lo que tenían, aprendieron en el camino y escalaron a partir de la evidencia. Esa disposición a empezar, a medir y a corregir es, en sí misma, parte del cambio cultural que este proyecto requiere.

El llamado a la acción que este artículo formula va dirigido a quienes tienen la responsabilidad institucional de conducir las defensorías públicas del país. La pregunta sobre si la tecnología tiene lugar en la defensa pública ya tiene respuesta. La pregunta que sigue abierta es cuándo y cómo cada institución decide que ese lugar es suyo.

Referencias

1. AAIP (2023). Guía para entidades públicas y privadas en materia de Transparencia y Protección de Datos Personales para una Inteligencia Artificial responsable. Agencia de Acceso a la Información Pública, Argentina.
2. Corrado, R. (2025). Los Derechos Fundamentales ante la Inteligencia Computacional y la Minería de Datos. Trabajo de Investigación. Escuela Judicial — Consejo General del Poder Judicial. Barcelona, España.
https://drive.google.com/file/d/1oMdVfe--6JGYnIb8tI54ob_-Au2EBvh/view?usp=sharing
3. Corvalán, Juan G., implementando inteligencia artificial generativa en estudios jurídicos y departamentos legales: resultados, impacto, guías de uso y directrices / Juan G. Corvalán; Albert Ferre. - 1a ed – Ciudad Autónoma de Buenos Aires: La Ley ; Universidad de Buenos Aires. Facultad de Derecho, 2024.
4. Estevez, E., Linares Lejarraga, S., y Fillottrani, P. (2020). PROMETEA: Transformando la administración de justicia con herramientas de inteligencia artificial.
5. Guía de datos y gobernanza de datos (2024), Reglamento Europeo de Inteligencia Artificial, Sandbox, fecha de versión: 10 de diciembre de 2025.
6. Informe IAs Poder Judicial (2024) Vazquez, G. (2024). La transformación digital del Poder Judicial argentino: resistencias, oportunidades y primeros pasos. Colossus Lab.
7. Minaggia (2023). La inteligencia artificial en el derecho penal: la utilización de algoritmos predictivos. Estudios sobre Jurisprudencia.
8. Solar Cayón, J. I. (2021). Retos de la deontología de la abogacía en la era de la inteligencia artificial jurídica. Derechos y Libertades. Universidad de Cantabria.