Universidad de San Andrés

Departamento de Derecho

Maestría en Propiedad Intelectual e Innovación

“El impacto de la inteligencia artificial en la privacidad de los datos personales en Argentina: Desafíos y propuestas de reforma legal”

Estudiante: Mercedes Rosario Garcia Gomez

D.N.I.: 40.927.657

Director de tesis: Dr. Agustin Allende.

Ciudad Autónoma de Buenos Aires, Septiembre 2025

DEDICATORIA:

A mi abuelo, que soñó este camino antes que yo, y cuya fe en mí sigue acompañándome.

A mis papás, por su amor constante, su fortaleza infinita y por haber hecho posible este trayecto.

INDICE:

CONCLUSIONES

BIBLIOGRAFÍA

INTRODUCCIÓN

El avance vertiginoso de la inteligencia artificial (IA) y el Big Data ha transformado profundamente la forma en que se recopilan, procesan y utilizan los datos personales. Tecnologías que antes eran propias de la ciencia ficción hoy forman parte de nuestra vida cotidiana, y están presentes en sectores tan diversos como la medicina, las finanzas, el comercio electrónico o la seguridad pública. Gracias a ellas, es posible detectar patrones, predecir comportamientos y automatizar decisiones con una precisión inédita.

Esta capacidad, sin embargo, no está exenta de tensiones. La IA no solo analiza datos ya disponibles, sino que puede inferir información nueva, a veces sensible, a partir de datos inicialmente inocuos. Cuando esta práctica se despliega sin supervisión ni salvaguardas jurídicas adecuadas, se amplifican los riesgos para los derechos fundamentales, especialmente el de la privacidad. En este escenario, el Big Data y la IA no solo representan una oportunidad para el desarrollo, sino también un desafío mayúsculo para el derecho.

La relación entre ambas tecnologías es simbiótica: la IA necesita enormes volúmenes de datos para aprender y tomar decisiones, y el Big Data permite alimentar esos sistemas con información constante, diversa y muchas veces invisible para quien la genera. Esta dinámica obliga a repensar de forma urgente los marcos regulatorios existentes, especialmente cuando las decisiones adoptadas por sistemas automatizados afectan la vida de las personas sin que éstas lo adviertan, lo entiendan o puedan oponerse.

En Argentina, la Ley 25.326 de Protección de Datos Personales fue sancionada en el año 2000, en un contexto tecnológico radicalmente distinto al actual. A más de dos décadas de su promulgación, resulta legítimo preguntarse si este marco normativo sigue siendo eficaz frente a las nuevas formas de tratamiento automatizado de datos impulsadas por algoritmos inteligentes. ¿Sigue siendo suficiente? ¿O ha quedado desbordado por una realidad que avanza a ritmo de innovación tecnológica?

En 2003, Argentina obtuvo un reconocimiento clave: fue declarada país con “nivel adecuado de protección” por parte de la Unión Europea, una distinción que habilita el flujo internacional de datos sin restricciones adicionales. revalidó el estatus de “adecuación” para Argentina, lo que permite que el flujo internacional de datos personales desde la UE se realice sin restricciones adicionales (Agencia de Acceso a la Información

Pública, 2024). En su evaluación, la Comisión valoró especialmente la independencia de la Agencia de Acceso a la Información Pública (AAIP) como autoridad de control, la ratificación del Convenio 108 y su protocolo adicional (Convenio 108+) en 2023, y el proyecto de ley de reforma de la Ley 25.326 presentado en junio de 2023, considerado una oportunidad para robustecer el marco normativo argentino. Sin embargo, esta revalidación no implica permanencia automática; la Comisión continuará monitoreando la evolución del sistema y, en particular, la aprobación de dicho proyecto.

Esta tesis se propone analizar en profundidad esa pregunta. El objetivo general es evaluar el impacto de la inteligencia artificial en la protección de los datos personales en el contexto argentino, identificar las limitaciones del régimen vigente y proponer reformas normativas que garanticen una tutela efectiva de los derechos fundamentales. A través de un enfoque jurídico-dogmático y comparado, se explorará cómo otras jurisdicciones han enfrentado desafíos similares, y qué lecciones podrían adaptarse al caso argentino sin caer en imitaciones acríticas.

En definitiva, este trabajo parte de una convicción: regular la inteligencia artificial no implica frenar la innovación, sino encauzarla en un marco democrático, inclusivo y respetuoso de la dignidad humana. Porque el desarrollo tecnológico no puede darse a costa de los derechos, sino al servicio de ellos.

NOTA METODOLOGICA SOBRE EL USO DE HERRAMIENTAS DE INTELIGENCIA ARTIFICIAL

Este trabajo fue realizado íntegramente por la autora en el marco de la Maestría en Propiedad Intelectual e Innovación de la Universidad de San Andrés. Con el fin de facilitar la revisión lingüística, mejorar la organización argumentativa y asegurar la claridad expositiva, se recurrió en forma complementaria al uso de herramientas de asistencia basadas en inteligencia artificial, especialmente procesadores de lenguaje natural.

Estas tecnologías fueron utilizadas exclusivamente como apoyo técnico y editorial, sin delegar en ningún momento la elaboración conceptual, el análisis jurídico ni la construcción crítica del contenido. Todas las ideas, hipótesis, decisiones metodológicas, selección de fuentes y redacción final son resultado del trabajo personal y reflexivo de la autora.

La utilización de estas herramientas se enmarca en prácticas académicas actuales, compatibles con los principios de integridad, originalidad y transparencia que rigen esta producción intelectual.

PLANTEAMIENTO DEL PROBLEMA

El creciente uso de la inteligencia artificial y el Big Data en el procesamiento de datos personales en Argentina plantea un reto significativo para la protección de la privacidad. A medida que tanto organizaciones privadas como públicas adoptan estas tecnologías para tomar decisiones basadas en datos, surgen preocupaciones sobre el uso indebido o no regulado de información personal. Si bien la Ley 25.326 fue pionera en su momento, su contenido no aborda los riesgos que implican el uso de IA y Big Data, lo que genera un vacío normativo que deja a los ciudadanos expuestos a posibles abusos de su privacidad.

El problema central es cómo actualizar el marco legal argentino para garantizar una protección adecuada de los derechos de privacidad en este contexto de uso masivo de IA y Big Data. Es fundamental examinar si la Ley 25.326 ofrece las garantías necesarias o si es imprescindible una reforma que contemple los riesgos específicos de estas tecnologías. Deberíamos identificar las áreas en las que la legislación actual se ha quedado rezagada y explorar cómo adaptarla para enfrentar eficazmente los nuevos desafíos tecnológicos.

OBJETIVO

Esta tesis tiene por objetivo identificar qué ajustes normativos concretos necesita la Ley de Protección de Datos Personales (Ley 25.326) para enfrentar los riesgos que plantea el uso de inteligencia artificial y Big Data en el tratamiento automatizado de datos personales en Argentina. A partir de un análisis crítico del marco normativo vigente y su comparación con modelos internacionales, se propondrán reformas orientadas a garantizar una protección efectiva de la privacidad y los derechos fundamentales de las personas en un entorno digital gobernado por sistemas algorítmicos.

HIPÓTESIS

La hipótesis central de esta tesis es que la Ley 25.326, en su redacción actual, no es suficiente para abordar los desafíos que plantean las tecnologías basadas en inteligencia artificial. Aunque la ley ofrece un marco general para la protección de datos, no

contempla de manera específica los riesgos, complejidades particularidades que conllevan estos nuevos modelos de tratamiento automatizado de información. Por lo tanto, se plantea que es necesaria una reforma normativa que permita dotar al sistema legal argentino de herramientas más eficaces para la tutela de los derechos de privacidad en la era digital.

METODOLOGÍA

La investigación se desarrollará a partir de una metodología de corte cualitativo, con un enfoque jurídico-dogmático y comparativo. En primer lugar, se examinará el marco normativo vigente en Argentina en materia de protección de datos personales, prestando especial atención a sus principios, mecanismos de control y limitaciones frente al uso de tecnologías basadas en IA y Big Data. Luego, se incorporará un análisis comparado con sistemas legales extranjeros en particular, el Reglamento General de Protección de Datos (RGPD) de la Unión Europea, la Ley General de Protección de Datos (LGPD) de Brasil y las normativas sectoriales vigentes en los Estados Unidos a fin de identificar buenas prácticas y criterios reguladores que puedan resultar aplicables al contexto nacional.

La investigación se complementará con el estudio de casos concretos que ilustran situaciones problemáticas generadas por el uso de IA y Big Data en el tratamiento de datos personales. Estas experiencias permitirán visualizar cómo se manifiestan en la práctica los riesgos advertidos y por qué resulta necesario revisar la legislación actual. Finalmente, se elaborarán propuestas normativas específicas que, inspiradas en los modelos analizados y adaptadas a la realidad argentina, procuren garantizar una protección efectiva de los derechos de los titulares de los datos personales.

CAPÍTULO 1: Fundamentos conceptuales y tecnológicos

1.1. Inteligencia Artificial: evolución histórica y aplicaciones actuales

Desde tiempos remotos, la humanidad ha buscado replicar su propia inteligencia en herramientas y artefactos, un deseo que se refleja en mitos, relatos literarios y en la propia evolución de la tecnología. Ejemplos de esto se encuentran en narraciones como Frankenstein de Mary Shelley escrita en el siglo XIX, donde la creación artificial de un científico adquiere no solo autonomía si no también capacidad racional. Otro ejemplo, de otorgar inteligencia a lo creado donde atravesó la filosofía fue con René Descartes, en el siglo XVII, donde él se preguntaba si las máquinas podrían pensar, anticipando un debate que hoy se materializa en el desarrollo (acelerado) de la inteligencia artificial.

La IA, en su concepción actual, nace formalmente en la década de 1950, cuando el matemático Alan Turing formuló su célebre test como criterio para evaluar si una máquina podía comportarse de manera indistinguible de un ser humano. Pero ya años más tarde, por 1956, un matemático llamado John McCarthy, durante la Conferencia de Dartmouth o en inglés "Dartmouth Summer Research Project on Artificial Intelligence" en la cual pretendían explorar si una máquina podía simular la inteligencia humana, fue el que acuñó el término "inteligencia artificial" definiéndola como "la ciencia e ingenio de hacer máquinas inteligentes". Este hito marcó el inicio de una disciplina que, al nombrarla y ponerle objetivos permitía la distinción con otras. Décadas después, se consolidaría como una de las fuerzas transformadoras más poderosas del siglo XXI.

En sus primeras décadas, el desarrollo de la IA estuvo centrado en modelos simbólicos, fundamentados en la lógica matemática y el procesamiento de reglas explícitas. Estos sistemas funcionan como un sistema de reglas, es decir, "si ocurre cierta condición, entonces se obtiene una conclusión", por ejemplo, si una persona estornuda mucho y tiene los ojos que pican, la regla indicará que probablemente se trate de una alergia, y si no corresponde, se pasa a la siguiente regla. Este enfoque permitía guardar el conocimiento humano en reglas claras, como si fueran instrucciones, y así podía usarse en cosas como entender el lenguaje, resolver problemas difíciles o manejar robots. Los llamados "sistemas expertos" fueron un gran avance porque imitaban la forma de pensar de los especialistas: tenían una base de datos con hechos y reglas, y un motor que las usaba para sacar conclusiones.

Uno de los ejemplos más emblemáticos fue el sistema “MYCIN”, desarrollado en la Universidad de Stanford en los años 70. Este programa, fue diseñado para diagnosticar infecciones bacterianas en la sangre y recomendar tratamientos con antibióticos, funcionaba a partir de más de 600 reglas codificadas por médicos. A través de una secuencia de preguntas, MYCIN era capaz de ajustar diagnósticos y proponer tratamientos adaptados a las condiciones del paciente. Aunque nunca llegó a implementarse en entornos hospitalarios por la falta de regulación sobre la responsabilidad médica automatizada, su impacto en el campo de la IA fue decisivo: demostró que una máquina podía tomar decisiones complejas basadas en estructuras lógicas.

Simultáneamente, durante los años 60 y 70, surgieron los primeros modelos de aprendizaje automático, como las redes neuronales, que intentaban imitar procesos cognitivos básicos. Uno de estos experimentos simulaba el comportamiento de un ratón en un laberinto, mostrando que una máquina podía aprender a partir de la experiencia. Sin embargo, las limitaciones tecnológicas de la época, particularmente en capacidad de cómputo y almacenamiento, impidieron un desarrollo más profundo de estos modelos hasta el surgimiento del Big Data y el aumento exponencial de la capacidad computacional en las décadas posteriores.

Llegada la década de 1980 es cuando se consolidaron los sistemas expertos, programas que intentaban imitar el razonamiento de un especialista humano siguiendo una serie de reglas y conocimientos almacenados. Se usaron en campos como la medicina, la química y la ingeniería, y durante un tiempo marcaron un gran avance. Sin embargo, al depender de normas demasiado rígidas, se volvieron poco útiles frente a contextos cambiantes. Fue recién con el avance de Internet, el abaratamiento del hardware y la proliferación de datos que la inteligencia artificial dio un salto cualitativo: surgió el aprendizaje automático moderno, basado en algoritmos capaces de identificar patrones complejos sin intervención humana directa. La IA se volvió capaz no solo de ejecutar instrucciones, sino de optimizar su propio desempeño, transformándose en una tecnología adaptativa.

Actualmente, la IA constituye uno de los pilares de la Cuarta Revolución Industrial. Este proceso global, caracterizado por la convergencia de lo físico, lo digital y lo biológico, está modificando profundamente la economía, el trabajo, la vida cotidiana y

las estructuras institucionales. La inteligencia artificial no solo automatiza tareas, sino que reconfigura los vínculos entre los sujetos y los datos que generan, lo cual plantea interrogantes inéditos para el derecho, particularmente en lo relativo a la privacidad.

Ejemplos como ChatGPT o DALL·E, desarrollados por OpenAI, muestran hasta qué punto los sistemas actuales son capaces de interactuar con el lenguaje natural, generar contenido original y adaptarse a distintos contextos. Esta capacidad plantea dilemas nuevos: ¿cómo garantizar que estos sistemas respeten los derechos de las personas cuando procesan, almacenan o infieren datos personales? ¿Cómo asegurar transparencia, equidad y control en decisiones automatizadas?

En este sentido, la definición de Stuart Russell resulta particularmente útil: la IA es "el estudio de agentes inteligentes que perciben su entorno y ejecutan acciones que maximizan sus posibilidades de éxito" (Russell & Norvig, 2021). Esta definición deja en claro que no se trata solo de automatización, sino de sistemas que aprenden, evalúan y actúan de forma autónoma. Bajo esta lógica, la IA adquiere una dimensión política y jurídica, ya que sus decisiones afectan cada vez más aspectos sensibles de la vida humana.

Por lo tanto, si bien la inteligencia artificial representa una herramienta de enorme potencial, también implica riesgos concretos para los derechos fundamentales. Su expansión en ámbitos como la seguridad, la salud, el crédito o el empleo plantea desafíos urgentes en materia de regulación. La capacidad de estas tecnologías para inferir información personal, incluso sin el consentimiento del titular, tensiona directamente los principios consagrados por el derecho a la privacidad.

A lo largo de esta tesis, se analizará cómo estas transformaciones impactan el ordenamiento jurídico argentino, en especial a través de la Ley 25.326. El objetivo es determinar si dicho marco es adecuado para enfrentar los desafíos que impone esta nueva realidad tecnológica o si, por el contrario, resulta necesario avanzar hacia una reforma integral que contemple los riesgos propios de la era de la inteligencia artificial.

1.1.1. Tipos de inteligencia artificial y tecnologías asociadas (machine learning, deep learning, NLP)

La inteligencia artificial (IA), entendida como la capacidad de las máquinas para ejecutar tareas que tradicionalmente requerían inteligencia humana, puede clasificarse en distintos niveles de sofisticación, de acuerdo con su grado de autonomía y capacidad de

aprendizaje. Esta distinción no solo permite comprender el desarrollo técnico de la IA, sino también advertir los riesgos que conlleva su aplicación al tratamiento de datos personales.

En primer lugar, se distingue la IA débil o limitada, orientada a tareas específicas y basada en instrucciones predeterminadas. Este tipo de IA está presente en asistentes virtuales, filtros antispam, motores de recomendación y chatbots de atención al cliente. Si bien sus decisiones no son autónomas, el uso de grandes volúmenes de datos personales para su funcionamiento ya plantea desafíos importantes en términos de consentimiento, minimización de datos y derecho a la privacidad.

Por otro lado, se encuentra la IA general (AGI), aún en etapa de desarrollo, que aspira a replicar la capacidad cognitiva humana, es decir, comprender, razonar y aprender en contextos diversos. El debate en torno a la AGI no es solo técnico, sino ético y jurídico, ya que implica pensar cómo regular a un agente autónomo que podría tomar decisiones con impacto real en derechos fundamentales.

Finalmente, se plantea la noción de una IA superinteligente, propuesta por Nick Bostrom (2014), que hipotetiza sobre un sistema capaz de superar ampliamente la inteligencia humana. Aunque se trata de una proyección especulativa, su sola posibilidad anticipa preguntas complejas sobre responsabilidad, control y límites legales.

Más allá de su capacidad, la IA también se clasifica por el modo en que aprende de los datos:

- **Aprendizaje supervisado**, que utiliza datos etiquetados para predecir resultados. Es común en sistemas de reconocimiento facial, análisis de crédito o clasificación de riesgo. Su uso intensivo de datos personales exige especial atención sobre la licitud del tratamiento y la transparencia del algoritmo.
- **Aprendizaje no supervisado**, que trabaja con datos no etiquetados, identificando patrones de forma autónoma. Se aplica, por ejemplo, en segmentación de consumidores, aunque conlleva el riesgo de generar perfiles automatizados sin consentimiento informado.
- **Aprendizaje por refuerzo**, basado en la lógica de prueba y error, utilizado especialmente en entornos dinámicos como juegos o navegación

autónoma. Su imprevisibilidad plantea desafíos sobre la explicabilidad y el control de las decisiones automatizadas.

Junto a estos métodos, emergen tecnologías específicas que potencian las capacidades de la IA:

- **Machine learning**, que constituye la base técnica de los sistemas de aprendizaje automático, permite construir modelos que mejoran progresivamente su desempeño al exponerse a nuevos datos. Su uso generalizado en la toma de decisiones automatizadas lo convierte en un punto crítico para el análisis jurídico de la protección de datos.
- **Deep learning**, una subcategoría del machine learning basada en redes neuronales artificiales, permite detectar patrones complejos a partir de grandes volúmenes de datos. Es la tecnología detrás de sistemas de reconocimiento facial, análisis de emociones y traducción automática, todos con alto impacto en la privacidad individual.
- **Procesamiento del lenguaje natural (NLP),** que habilita a las máquinas a comprender, interpretar y generar lenguaje humano. Se utiliza en asistentes conversacionales, sistemas de análisis de texto y modelos de IA generativa como ChatGPT, los cuales operan a partir de grandes bases de datos textuales que pueden contener información personal, muchas veces sin el consentimiento explícito de los titulares.

Como señala Delgado Espinal (2024), la IA no solo analiza datos, sino que "puede predecir y manipular el comportamiento individual", lo que obliga a repensar los límites entre análisis legítimo y vigilancia encubierta. Comprender estas tecnologías no es solo un ejercicio técnico, sino una herramienta indispensable para anticipar riesgos jurídicos concretos y actualizar los marcos normativos vigentes.

1.1.2. Aplicaciones Actuales de la Inteligencia Artificial en la vida cotidiana y en el ámbito jurídico

La inteligencia artificial dejó de ser una promesa futurista para convertirse en una herramienta cotidiana, con presencia activa en múltiples esferas de la vida social, económica y jurídica. Desde la personalización de anuncios en redes sociales hasta la predicción de diagnósticos médicos, su despliegue ya tiene efectos concretos sobre el

tratamiento de datos personales, muchas veces sin que los usuarios sean plenamente conscientes.

En el campo de la salud, la IA se utiliza para analizar estudios clínicos, anticipar enfermedades y personalizar tratamientos. Estas prácticas implican el uso intensivo de datos sensibles, como historiales médicos y patrones genéticos, cuya protección exige un marco normativo claro y robusto, especialmente cuando las decisiones se toman sin intervención humana.

En el sector financiero, la IA permite detectar fraudes, calcular riesgos crediticios y automatizar inversiones. Sin embargo, como señala Barona Vilar (2021), los algoritmos que evalúan la solvencia de una persona pueden "replicar estructuras de exclusión que el derecho debería corregir, no legitimar", lo que obliga a repensar el equilibrio entre eficiencia y justicia.

En el ámbito educativo, se implementan sistemas que adaptan contenidos según el perfil del alumno, utilizando información sobre su desempeño, conducta y preferencias. Estas herramientas, si bien valiosas, también pueden generar formas de clasificación que afecten la autonomía del estudiante y la equidad educativa.

En el derecho, la IA ya se emplea para predecir fallos, analizar jurisprudencia, detectar infracciones de propiedad intelectual y automatizar la redacción de contratos. Sin embargo, estas aplicaciones plantean interrogantes sobre la responsabilidad legal en decisiones automatizadas y sobre el derecho a una defensa justa cuando se utilizan herramientas que, por su naturaleza, son opacas o de difícil explicación.

Estas aplicaciones no son neutras ni inevitables. Cada una de ellas redefine el modo en que se recolectan, procesan y valoran los datos personales, y por tanto exige respuestas jurídicas adecuadas. La IA ha traído consigo una nueva lógica de gobernanza algorítmica, donde decisiones que antes eran humanas ahora son delegadas a modelos estadísticos. Como sugiere Determann (2017), la privacidad no debe ser entendida solo como un derecho individual, sino como "una condición estructural para el ejercicio de otros derechos fundamentales". Esta mirada exige incorporar también la noción de privacidad grupal, que reconoce que los sistemas automatizados no solo afectan a personas aisladas, sino que pueden generar formas de discriminación estructural sobre colectivos enteros, al categorizar y actuar sobre perfiles estadísticos. Como sostienen Selinger y Hartzog (2019), la privacidad debe entenderse también como un bien colectivo,

ya que los sistemas automatizados operan sobre grupos y no solo sobre individuos identificados. Así, el impacto de la IA sobre la privacidad no se limita al plano personal, sino que incide en la configuración misma de los vínculos sociales y en la reproducción de desigualdades preexistentes. Regular estos efectos supone asumir que la protección de datos personales es también una cuestión de justicia social, y no solo una garantía individual.

Por eso, resulta urgente incorporar una mirada crítica que no se limite a celebrar la innovación, sino que se pregunte por sus efectos sobre la dignidad, la autonomía y la igualdad. La regulación argentina, anclada en un paradigma pre-digital, debe actualizarse para ofrecer garantías reales frente a una tecnología que ya está moldeando la vida cotidiana y reconfigurando los términos del vínculo entre ciudadanía y poder.

La expansión de la inteligencia artificial en diversas áreas de la vida cotidiana no puede comprenderse de forma aislada. Su funcionamiento y capacidad de aprendizaje dependen, en gran medida, del acceso a enormes volúmenes de información. En este sentido, el desarrollo del Big Data y los procesos de automatización masiva han configurado un nuevo ecosistema digital donde los datos personales se han convertido en un insumo estratégico. Comprender esta dinámica resulta clave para analizar los impactos de la IA desde una perspectiva jurídica, en especial cuando los derechos fundamentales se ven cada vez más condicionados por decisiones automatizadas.

1.2. Big Data, automatización y su impacto en el ecosistema digital

El concepto de Big Data refiere al procesamiento y análisis de grandes volúmenes de información que, por su tamaño, velocidad de generación y variedad, exceden las capacidades de los sistemas tradicionales. En el mundo actual, profundamente atravesado por lo digital, cada clic, transacción, búsqueda o publicación en redes sociales genera datos que pueden ser almacenados, analizados e incluso monetizados. Esta realidad ha situado al Big Data como una herramienta estratégica, tanto para el sector público como privado, y como uno de los pilares de la transformación tecnológica que estamos presenciando.

Las características esenciales del Big Data suelen resumirse en lo que se conoce como las cinco “V”: volumen, velocidad, variedad, veracidad y valor. El volumen remite a la inmensa cantidad de datos generados constantemente, desde historiales clínicos hasta registros de navegación. La velocidad se relaciona con la rapidez con la que esta

información es producida y necesita ser procesada, muchas veces en tiempo real. La variedad expresa la diversidad de formatos en los que se presentan los datos, que pueden ser estructurados como una planilla de Excel, semiestructurados como un correo electrónico o directamente no estructurados como una fotografía o un video. La veracidad apunta a la necesidad de contar con información confiable, ya que los datos erróneos pueden conducir a decisiones igualmente defectuosas. Finalmente, el valor representa la capacidad de extraer conocimiento útil que permita actuar con eficiencia, prevenir riesgos o detectar tendencias.

Sin embargo, lo que hace particularmente complejo el tratamiento de estos datos es que pueden ser reutilizados para múltiples fines distintos de los originalmente previstos, como campañas de marketing, evaluaciones de riesgo, predicciones de conducta o incluso vigilancia estatal. Esta multiplicidad de finalidades plantea serios desafíos para el control individual y la protección de la privacidad, ya que muchas veces el uso posterior de los datos resulta opaco o inesperado para el titular. Como advierte Purtova (2018), en entornos de Big Data el principio de limitación de finalidad se vuelve difícil de aplicar, lo que incrementa la opacidad del tratamiento y debilita las garantías tradicionales del derecho de protección de datos.

1.2.1. Relación entre Big Data e Inteligencia Artificial

La interrelación entre Big Data e inteligencia artificial es íntima y esencial. De hecho, sin el primero, la segunda no habría alcanzado el nivel de sofisticación actual. Los algoritmos de IA, especialmente los de aprendizaje automático, requieren enormes volúmenes de información para poder detectar patrones, ajustar modelos predictivos y optimizar sus resultados. Esta sinergia ha transformado a ambas tecnologías en un binomio inseparable: el Big Data alimenta a la inteligencia artificial, y esta última permite que los datos puedan ser procesados con velocidad, profundidad y escalabilidad.

En este escenario, la IA no solo analiza datos existentes, sino que también puede inferir información nueva, incluyendo datos sensibles no revelados explícitamente por las personas. Esto genera importantes tensiones en términos de protección de la privacidad, ya que se difuminan las fronteras entre lo público y lo íntimo, lo consentido y lo deducido. Así, mientras el Big Data potencia el desarrollo de la IA, también magnifica sus riesgos, exigiendo un replanteo urgente del marco legal vigente.

Un ejemplo cotidiano de esta relación simbiótica puede verse en los sistemas de recomendación de plataformas como Netflix o Spotify, que utilizan la información sobre el comportamiento del usuario para ofrecer contenidos personalizados. Lo mismo ocurre en el ámbito de la salud, donde los sistemas de diagnóstico basados en IA se nutren de grandes volúmenes de datos clínicos para detectar patologías, sugerir tratamientos y predecir la evolución de enfermedades. En materia de ciberseguridad, el análisis en tiempo real de grandes cantidades de tráfico permite identificar amenazas antes de que se materialicen, evidenciando el poder de esta tecnología cuando es correctamente aplicada.

1.2.2. Aplicaciones del Big Data en distintos sectores

El Big Data ha transformado múltiples industrias, permitiendo desde una mayor eficiencia operativa hasta la personalización de servicios. Algunos ejemplos de su aplicación incluyen:

- **Sector financiero:** Los bancos y entidades financieras utilizan Big Data para la detección de fraudes, la evaluación crediticia y la optimización de inversiones mediante el análisis predictivo.
- **Gobiernos y políticas públicas:** La administración pública analiza grandes volúmenes de datos para mejorar la gestión del tráfico, la distribución de recursos y la detección de necesidades sociales.
- **Marketing y publicidad:** Las empresas utilizan el análisis de datos para segmentar a su audiencia y personalizar anuncios basados en el comportamiento de los consumidores en línea.
- **Industria de la salud:** El análisis de datos clínicos y epidemiológicos permite predecir brotes de enfermedades, mejorar tratamientos y diseñar políticas sanitarias más eficaces.

1.2.3. Desafíos y riesgos del Big Data

A pesar de sus innumerables beneficios, el uso intensivo del Big Data plantea una serie de desafíos que no pueden ser ignorados. Uno de los más relevantes es el riesgo de vulneración de la privacidad. La recopilación masiva de información muchas veces sin el conocimiento o consentimiento del titular puede desembocar en usos abusivos o no previstos. A esto se suman los riesgos de sesgos algorítmicos: si los datos utilizados para entrenar modelos de IA están contaminados con prejuicios sociales, los sistemas pueden replicarlos y profundizarlos, generando nuevas formas de discriminación automatizada.

Otro de los desafíos radica en la falta de una regulación adecuada. En muchos países, incluida Argentina, las leyes de protección de datos fueron concebidas en contextos analógicos y no alcanzan a cubrir las complejidades actuales del entorno digital. Además, existe el peligro del uso indebido de la información, ya sea por parte de empresas que buscan monetizarla, o por gobiernos que pueden utilizarla para vigilar a la ciudadanía en lugar de protegerla.

En este sentido, es imperioso que el avance del Big Data vaya acompañado de un marco normativo robusto, actualizado y con enfoque en derechos humanos, que contemple las particularidades de este nuevo paradigma tecnológico. Tal como se explorará en los capítulos siguientes, la legislación argentina aún presenta vacíos frente a este fenómeno, lo que obliga a pensar propuestas de reforma que permitan garantizar el desarrollo de estas tecnologías sin comprometer los derechos fundamentales de las personas.

1.2.4. Datos Personales y Privacidad

En el contexto actual, marcado por la irrupción del Big Data y el desarrollo acelerado de la inteligencia artificial, la protección de los datos personales se ha convertido en una preocupación central. La información ya no se limita a registros estáticos, sino que es constantemente generada, analizada y utilizada con fines diversos, desde la personalización de servicios hasta la toma de decisiones automatizadas. Esta dinámica, si bien representa una enorme oportunidad para la innovación, también plantea una amenaza concreta para el derecho a la privacidad, entendido como la capacidad del individuo de controlar qué datos personales comparte, con quién y para qué.

La noción de datos personales está íntimamente ligada a este derecho. Desde el punto de vista jurídico, los datos personales comprenden toda aquella información que identifica o puede identificar a una persona física, de manera directa o indirecta. Esto incluye no solo datos evidentes como el nombre, el DNI o el domicilio, sino también información biométrica, de geolocalización, comportamiento digital y hábitos de consumo. En un entorno atravesado por tecnologías como la inteligencia artificial, el Big Data y el Internet de las Cosas, los datos personales ya no son simples rastros de una actividad, sino insumos estructurales para sistemas que toman decisiones automatizadas sobre las personas.

Reducir los datos personales a una definición meramente técnica sería insuficiente. Su protección implica una garantía más amplia: el resguardo de la dignidad, la autonomía y la autodeterminación informativa. Este último concepto fue desarrollado por el Tribunal Constitucional Federal Alemán en su sentencia de 15 de diciembre de 1983, en respuesta a la Ley del Censo de Población de 1983. La ley requería a los ciudadanos proporcionar información detallada sobre sus condiciones personales y laborales, lo que generó preocupaciones sobre la posible utilización indebida de estos datos. El Tribunal estableció que "el derecho fundamental garantiza en esta medida la capacidad de los individuos para determinar, en principio, la divulgación y empleo de sus datos personales". Este fallo sentó las bases para reconocer que toda persona debe poder controlar el destino de su información, decidir quién la recopila, cómo se utiliza y con qué finalidad.

A nivel internacional, se han consolidado ciertos principios fundamentales que orientan el tratamiento legítimo de los datos personales. Entre ellos se destacan el consentimiento informado como garantía de autonomía del titular; la finalidad específica que impide usos posteriores distintos a los declarados inicialmente; y la minimización que establece que sólo deben recolectarse los datos estrictamente necesarios para cumplir un propósito determinado y conservarse únicamente durante el tiempo indispensable para ello, evitando almacenamientos innecesarios o prolongados sin justificación legítima. A estos principios se suman la obligación de garantizar la seguridad y confidencialidad de la información, evitando accesos no autorizados, filtraciones o usos indebidos Este conjunto de principios configura un marco normativo que busca equilibrar innovación tecnológica y tutela efectiva de derechos fundamentales.

Tal como advierte Lothar Determann (2017), la privacidad no puede entenderse simplemente como una categoría jurídica neutral. En su análisis, subraya que este derecho es un factor estructural para el ejercicio de libertades esenciales como la libertad de expresión, la participación política, la libertad de culto y la vida democrática. En los modelos europeos, la privacidad ha sido reconocida como un derecho fundamental como lo establece el artículo 8 de la Carta de Derechos Fundamentales de la Unión Europea, mientras que en Estados Unidos su protección ha estado subordinada históricamente a otros principios, como la libertad de empresa o la seguridad nacional. Esta divergencia revela que la privacidad no se concibe del mismo modo en todos los sistemas jurídicos, y que su alcance depende del contexto político, histórico y cultural.

En Argentina, la Ley 25.326 constituye la normativa de base en esta materia. Si bien fue un avance significativo en su momento, resulta evidente que fue concebida para un entorno analógico y hoy no logra dar una respuesta integral a los desafíos planteados por la inteligencia artificial y el tratamiento masivo de datos. El diseño actual de la ley no contempla, por ejemplo, mecanismos efectivos de control sobre algoritmos opacos ni establece regulaciones específicas sobre decisiones automatizadas, lo que genera un vacío preocupante en términos de tutela de derechos. Esta situación resulta especialmente llamativa si se considera que Argentina ha ratificado instrumentos internacionales relevantes como el Convenio 108 del Consejo de Europa (Ley 27.483) y su Protocolo Adicional, conocido como Convenio 108+ (Ley 27.699), que exigen estándares elevados de protección, transparencia y control en el tratamiento de datos personales, incluso en contextos de inteligencia artificial. Sin embargo, esos compromisos aún no se han traducido en una actualización normativa integral a nivel interno.

Hoy más que nunca, frente al avance de tecnologías predictivas y clasificatorias, el derecho a la privacidad adquiere una renovada urgencia. No se trata solo de evitar filtraciones de información o usos indebidos, sino de garantizar que las personas sigan siendo sujetos de derechos y no objetos de análisis algorítmicos. La respuesta dependerá, en parte, de cuán sólido y actualizado sea el marco normativo, pero también de la capacidad de los Estados para comprender que la privacidad no es un obstáculo para el progreso, sino una condición indispensable para una sociedad libre, plural y humana.

1.2.5. Interacción entre IA, Big Data y Datos Personales

La intersección entre inteligencia artificial, Big Data y datos personales configura uno de los mayores desafíos jurídicos y éticos del siglo XXI. La combinación de estas tecnologías permite procesar grandes cantidades de información con una velocidad y precisión inéditas, lo cual potencia enormemente su valor estratégico, pero también agrava los riesgos inherentes al uso indebido de la información personal.

Uno de los problemas más debatidos en este sentido es la falta de transparencia en los sistemas de IA. Muchos de los algoritmos utilizados actualmente funcionan como verdaderas “cajas negras”, ya que ni siquiera sus desarrolladores pueden explicar completamente cómo se llega a una determinada decisión. Esta opacidad atenta contra el principio de explicabilidad, fundamental para poder impugnar decisiones que afectan derechos individuales.

Otro riesgo importante es el sesgo algorítmico. Si los datos utilizados para entrenar una IA contienen prejuicios explícitos o implícitos, el sistema puede no solo replicarlos sino incluso amplificarlos, generando resultados discriminatorios. Esto ha sido observado en casos concretos en todo el mundo; Uno de los más conocidos es el del sistema "COMPAS" en Estados Unidos, utilizado para predecir la reincidencia de personas imputadas. Una investigación periodística reveló que este sistema otorgaba puntuaciones de riesgo más altas a personas negras que a blancas con antecedentes similares, evidenciando un sesgo racial estructural (Angwin, Larson, Mattu & Kirchner, 2016). Otro ejemplo relevante es el caso de Amazon, cuya herramienta interna para selección de personal fue abandonada luego de detectarse que desfavorecía sistemáticamente a las mujeres al filtrar currículums, ya que el algoritmo había sido entrenado con datos históricos sesgados por género (Dastin, 2018). Estos casos demuestran que el sesgo algorítmico no es un problema teórico, sino una amenaza real que puede consolidar desigualdades existentes bajo una apariencia de objetividad tecnológica.

La toma de decisiones automatizadas es quizás el terreno más sensible de esta interacción. En sectores como el financiero, el laboral o el sanitario, el uso de IA puede determinar el acceso a un crédito, la contratación de un empleado o la selección de un tratamiento médico. Si estas decisiones se toman sin intervención humana, sin posibilidad de revisión o sin criterios claros de evaluación, se pone en juego no solo el derecho a la privacidad, sino también principios fundamentales como la igualdad ante la ley, la dignidad humana y la autodeterminación informativa.

Esta compleja interacción, que será retomada en los próximos capítulos desde una perspectiva normativa y comparada, evidencia que el avance tecnológico no puede ir desligado del desarrollo jurídico. La innovación, sin regulación adecuada, corre el riesgo de vulnerar derechos en nombre de la eficiencia.

El análisis conceptual realizado hasta aquí sobre la inteligencia artificial, el Big Data y su interacción con los datos personales nos permite comprender no solo la magnitud de las transformaciones tecnológicas en curso, sino también la urgencia de contar con marcos regulatorios adecuados que acompañen este proceso. Estas tecnologías, al incidir de manera directa sobre derechos fundamentales, especialmente el de la privacidad, exigen una respuesta normativa que no puede postergarse.

En este contexto, resulta indispensable examinar el estado actual del marco jurídico argentino en materia de protección de datos personales, evaluando su capacidad para enfrentar los desafíos que plantea el nuevo paradigma tecnológico. Con este objetivo, el próximo capítulo se adentrará en el análisis de la Ley 25.326, sus fundamentos, limitaciones y la necesidad de su actualización frente a los avances de la inteligencia artificial y el uso masivo de datos.

1.3. El tratamiento automatizado de datos personales: una dimensión crítica en la era de la inteligencia artificial

En el contexto del ecosistema digital contemporáneo, no todo tratamiento de datos personales plantea los mismos desafíos ni exige las mismas respuestas normativas. En particular, el tratamiento automatizado esto es, aquel en el que las decisiones se adoptan sin intervención humana significativa presenta riesgos cualitativamente distintos respecto de los mecanismos tradicionales. En estos casos, la inteligencia artificial opera sobre grandes volúmenes de información personal con el fin de predecir comportamientos, clasificar perfiles o tomar decisiones, muchas veces sin que los individuos afectados tengan conocimiento de ello, posibilidad de impugnarlo o incluso de comprenderlo.

Esta automatización, si bien ofrece ventajas en términos de eficiencia y escalabilidad, puede erosionar principios fundamentales como el consentimiento informado, la transparencia y la autodeterminación informativa, pilares de los sistemas jurídicos democráticos. La opacidad algorítmica, la posibilidad de discriminaciones invisibles y la dilución de la rendición de cuentas configuran un nuevo tipo de vulnerabilidad que el derecho aún no ha terminado de conceptualizar ni regular de manera adecuada.

En este marco, el enfoque de esta tesis pone el foco en la protección de los datos personales en el tratamiento automatizado mediante inteligencia artificial, como uno de los principales retos regulatorios de la actualidad. No se trata de ignorar el resto de los desafíos asociados al tratamiento de datos, sino de visibilizar un área crítica donde confluyen avances tecnológicos, impactos sociales y vacíos legales. Esta perspectiva permite evaluar con mayor precisión la suficiencia o insuficiencia del marco normativo argentino y proponer reformas específicas alineadas con los principios internacionales y las experiencias comparadas.

1.3.1. El impacto de la IA en el derecho a la privacidad y la autonomía personal

La inteligencia artificial ha modificado la forma en que entendemos el derecho a la privacidad. Si en el pasado este derecho implicaba el resguardo del ámbito íntimo frente a intromisiones arbitrarias, hoy exige nuevas respuestas frente a algoritmos que analizan, infieren y predicen aspectos de nuestra vida sin que medie una participación consciente. La IA no solo recoge lo que decimos, sino también cómo lo decimos, cuánto tiempo miramos una pantalla o con quiénes interactuamos, reconstruyendo así perfiles extremadamente precisos.

Este tipo de vigilancia pasiva a menudo imperceptible debilita la autonomía personal. Cuando las decisiones se toman en base a datos previamente recolectados, sin conocimiento ni consentimiento efectivo, la persona queda reducida a una categoría estadística, desprovista de control sobre su información. El consentimiento, base tradicional del derecho a la privacidad, se vuelve insuficiente frente a estos mecanismos de recolección y procesamiento masivo, en muchos casos automatizados y continuos.

Como sostiene Bonilla Gutiérrez (2024), en el contexto de la vigilancia algorítmica, el consentimiento formal pierde sentido si no va acompañado de mecanismos efectivos de control y de la posibilidad real de intervención humana. Por eso, resulta urgente redefinir el alcance del consentimiento y avanzar hacia modelos normativos que garanticen una verdadera autodeterminación informativa, capaz de resistir el poder cada vez más concentrado de las plataformas tecnológicas.

1.3.2. Riesgos para la igualdad, la no discriminación y la transparencia

Uno de los mayores peligros del tratamiento automatizado de datos personales mediante IA es la reproducción y en ocasiones la amplificación de sesgos sociales preexistentes. Los algoritmos, al ser entrenados con datos históricos que reflejan desigualdades estructurales, pueden generar decisiones discriminatorias, incluso cuando no hay una intención explícita de hacerlo.

Ejemplos concretos no faltan: desde herramientas de selección de personal que penalizan perfiles por género o lugar de residencia, hasta sistemas de predicción criminal que asignan mayores riesgos a determinadas poblaciones por motivos raciales o socioeconómicos. La discriminación algorítmica no solo es más difícil de detectar, sino

que además se reviste de una supuesta objetividad tecnológica que la vuelve aún más peligrosa.

La falta de transparencia es un factor que agrava este fenómeno. Muchos sistemas de IA funcionan como verdaderas "cajas negras", imposibilitando la comprensión del criterio detrás de una decisión. En este escenario, el derecho a la explicación y a la revisión humana adquiere una relevancia crítica. Sin ellos, las personas quedan desprotegidas frente a decisiones que pueden afectar su acceso a derechos, servicios o incluso su libertad.

La regulación, por tanto, no puede limitarse a proteger la privacidad: debe garantizar también la equidad, la transparencia y la posibilidad de impugnación, especialmente en contextos donde los algoritmos definen trayectorias de vida.

1.3.3. Tensiones entre innovación tecnológica y principios democráticos

La inteligencia artificial, en tanto herramienta de poder, plantea desafíos inéditos a los principios democráticos. Si bien su capacidad para optimizar procesos, reducir costos y predecir conductas puede traducirse en beneficios tangibles, también genera riesgos en términos de concentración de poder, vigilancia y pérdida de control ciudadano sobre decisiones que les afectan directamente.

Cuando un sistema automatizado define, sin intervención humana, quién accede a un crédito, un subsidio o una prestación médica, se produce un corrimiento del poder de decisión desde las instituciones democráticamente responsables hacia entidades tecnológicas, muchas veces privadas, que operan con escasa supervisión pública.

En este sentido, la gobernanza de la inteligencia artificial no es solo una cuestión técnica, sino profundamente política. Exige definir quién diseña los sistemas, con qué valores, bajo qué principios y con qué mecanismos de rendición de cuentas. Regular la IA no es oponerse al progreso, sino condicionar su desarrollo a los valores que sustentan un Estado de derecho: la dignidad humana, la equidad, la transparencia y la participación ciudadana.

La protección de los datos personales en contextos de automatización debe ser entendida, entonces, como una cuestión de justicia democrática. No se trata solo de asegurar privacidad, sino de garantizar que el desarrollo tecnológico se inscriba en un proyecto de sociedad inclusiva, justa y respetuosa de los derechos de todos y todas.

1.4. Datos personales y derecho a la privacidad en entornos algorítmicos

En el contexto contemporáneo, donde la inteligencia artificial y el Big Data se combinan para transformar los modos de vida, de trabajo y de gobierno, los datos personales han dejado de ser simples registros para convertirse en el insumo central de una nueva arquitectura social. Su circulación, almacenamiento y análisis no solo tienen consecuencias económicas o técnicas, sino también profundas implicancias en términos de derechos humanos.

El derecho a la privacidad, históricamente concebido como una protección frente a injerencias arbitrarias en la vida personal, ha debido evolucionar hacia una noción más amplia: la autodeterminación informativa. Esta figura, consagrada por el Tribunal Constitucional Federal Alemán en su histórica sentencia sobre el censo de 1983, reconoce el derecho de toda persona a decidir sobre el uso y destino de sus datos, en tanto manifestación de su dignidad y libertad individual.

Sin embargo, en los entornos algorítmicos actuales, esa autodeterminación se ve constantemente desafiada. Los sistemas de inteligencia artificial pueden inferir información personal sin que haya una declaración expresa por parte del titular, lo que diluye el consentimiento como fundamento del tratamiento legítimo de datos. La privacidad, en este nuevo escenario, no puede entenderse como un estado pasivo o un privilegio reservado, sino como un derecho activo que requiere protección constante y mecanismos institucionales eficaces.

El uso masivo de algoritmos que procesan datos personales en tiempo real ya sea para clasificar perfiles de consumidores, asignar puntajes crediticios, detectar patrones de comportamiento o seleccionar candidatos para un puesto laboral plantea interrogantes sobre la legitimidad de esas decisiones y sobre la posibilidad real de ejercer derechos como el acceso, la rectificación o la oposición. En palabras de Lothar Determann (2017), la privacidad no puede limitarse a evitar filtraciones: “es un resguardo estructural frente al uso instrumental de las personas en mercados digitales opacos y desiguales”.

Por otra parte, es necesario destacar que los datos personales son objeto de una creciente apropiación por parte de actores privados, cuyas plataformas tecnológicas desde redes sociales hasta sistemas de IA generativa recogen, procesan y monetizan información sin siempre contar con bases jurídicas claras o mecanismos de transparencia. Esta privatización del espacio informacional desafía el rol tradicional del Estado como

garante de derechos y exige una nueva arquitectura regulatoria que combine principios legales, controles técnicos y participación ciudadana.

Desde una perspectiva crítica, también debe advertirse que el tratamiento automatizado de datos puede reproducir y profundizar desigualdades preexistentes. Cuando los algoritmos se entrenan con información históricamente sesgada, corren el riesgo de consolidar patrones discriminatorios, afectando especialmente a grupos vulnerables. Así, el derecho a la privacidad debe articularse con otros derechos fundamentales, como el de la no discriminación, el debido proceso o la igualdad ante la ley.

Frente a esta complejidad, se impone una visión integral que reconozca a la privacidad como un derecho habilitante, es decir, como una condición indispensable para el ejercicio de otras libertades esenciales en una sociedad democrática. Tal como ha señalado la Oficina del Alto Comisionado de las Naciones Unidas para los Derechos Humanos, "el derecho a la privacidad es una base esencial para el disfrute de otros derechos, incluidos la libertad de expresión, la libertad de asociación y el derecho a no ser discriminado" (OHCHR, 2022). En la misma línea, la UNESCO (2021) ha sostenido que la privacidad es un componente esencial para el ejercicio de la libertad de pensamiento, expresión y asociación, pilares fundamentales de una sociedad democrática. Regular los entornos algorítmicos no es un obstáculo para la innovación: es una garantía para que dicha innovación se desarrolle en un marco de respeto por la persona humana y sus derechos.

1.4.1. Conceptualización jurídica de los datos personales en el siglo XXI

La definición jurídica de dato personal ha evolucionado junto con los avances tecnológicos que permiten su recolección, análisis y uso en múltiples contextos. Tradicionalmente, la legislación -como la Ley 25.326 en Argentina- considera dato personal a "toda información de cualquier tipo referida a personas físicas o de existencia ideal determinadas o determinables". Este concepto incluye nombres, domicilios o documentos de identidad, pero también datos biométricos, geolocalización, hábitos de consumo y comportamiento digital.

Sin embargo, en la actualidad, esta definición resulta insuficiente. Con el desarrollo de sistemas de inteligencia artificial que pueden inferir datos sensibles a partir de información aparentemente neutra como el estado de salud deducido de hábitos de

navegación o la orientación sexual inferida a partir de redes de contacto, la categoría de dato personal se ha vuelto más difusa, pero también más abarcativa. Como advierte Purtova (2021), “los datos personales ya no son meras huellas del pasado, sino insumos para predecir y moldear futuros comportamientos”, lo que exige una reformulación de su conceptualización jurídica. En la misma línea, Zuboff (2019) sostiene que “la recolección pasiva y el procesamiento predictivo de datos personales convierten la privacidad en una cuestión de poder estructural, más que de elección individual”, destacando así la necesidad de marcos legales que no se limiten al consentimiento individual como única garantía.

Esta nueva lógica exige una revisión conceptual que contemple el carácter dinámico, inferencial y no siempre evidente de los datos personales. Los sistemas jurídicos deben considerar no solo lo que el titular revela voluntariamente, sino también lo que los algoritmos pueden deducir sin su conocimiento. En este escenario, el derecho debe actuar preventivamente, reconociendo el potencial lesivo del uso de datos en contextos algorítmicos y estableciendo límites claros a su recopilación y procesamiento.

1.4.2. Autodeterminación informativa y consentimiento en escenarios digitales

El consentimiento ha sido tradicionalmente el pilar sobre el que se sustenta la legitimidad del tratamiento de datos personales. Según la Ley 25.326, este debe ser libre, informado, expreso y otorgado para fines determinados. No obstante, en los ecosistemas digitales actuales, donde los datos se recolectan de forma continua y muchas veces sin intervención consciente del usuario, este modelo muestra sus limitaciones.

Esto se refleja, entre otras cosas, en el cambio de paradigma del consentimiento expreso ("opt in") hacia mecanismos de oposición posterior ("opt out"), en los que se presume el consentimiento salvo manifestación en contrario por parte del titular. Este desplazamiento pone en tensión la noción misma de consentimiento informado, ya que debilita el control efectivo que las personas pueden ejercer sobre sus datos personales (Bonilla Gutiérrez, 2024).

En la normativa argentina, esta problemática se evidencia en la contradicción entre el artículo 27 de la Ley 25.326, que exige consentimiento previo para fines publicitarios, y el artículo 27 del Decreto Reglamentario 1558/2001, que permite presumir el

consentimiento salvo oposición, generando un conflicto interpretativo que ha sido objeto de críticas doctrinarias y jurisprudenciales.

Como plantea Bonilla Gutiérrez (2024), “el consentimiento aislado, desprovisto de un control real sobre el uso posterior de los datos, ya no es suficiente para proteger la autonomía del individuo”. En la misma línea, Basterra (2004) sostiene que “el consentimiento debe ser no solo expreso, sino también verificable, renovable y fácilmente revocable, especialmente cuando se trata de entornos digitales donde el flujo de datos es continuo e incontrolado”. Peyrano (2003) también advierte que el consentimiento no puede ser considerado válido si no va acompañado de mecanismos que permitan ejercer un control efectivo sobre los datos a lo largo del tiempo.

Desde la jurisprudencia, la Cámara Nacional de Apelaciones del Trabajo en el caso Lascano Quintana c/ Organización Veraz S.A. resolvió que el tratamiento de datos personales obtenidos del Boletín Oficial sin consentimiento vulneraba el derecho a la autodeterminación informativa, aun cuando se tratara de información pública. El fallo destacó que la utilización de datos por parte de una base privada exige la autorización expresa del titular, conforme lo establecido en la Ley 25.326. Asimismo, en el caso Torres Abad c/ EN – JGM (Expte. 49.482/2016 CA1), se cuestionó la cesión de datos personales recabados por organismos estatales a terceros sin el consentimiento expreso del titular, declarando su ilegalidad. Finalmente, la Procuración del Tesoro de la Nación, en dictamen de diciembre de 2020, se pronunció en contra del uso de datos personales para fines propagandísticos sin autorización previa, subrayando que el Estado no puede presuponer el consentimiento de los ciudadanos para finalidades distintas a las que motivaron la recolección original de sus datos personales. Este dictamen surgió en el marco de una causa impulsada por la Asociación por los Derechos Civiles (ADC) y sentó un precedente relevante en materia de límites al uso estatal de información personal.

Por ello, se impone la necesidad de fortalecer el principio de autodeterminación informativa, entendida no solo como la capacidad de autorizar un uso puntual de los datos, sino como el derecho a ejercer un control activo y continuo sobre ellos. Esto implica implementar mecanismos de consentimiento granular, la posibilidad de revocación sencilla y herramientas tecnológicas que permitan al titular rastrear el uso de su información, algo que la actual legislación argentina aún no garantiza.

1.4.3. La privacidad como derecho habilitante en sociedades gobernadas por datos

En un contexto cada vez más atravesado por algoritmos y grandes flujos de información, la privacidad adquiere una dimensión estratégica que supera su conceptualización tradicional como simple protección del ámbito privado. Ya no se trata únicamente de resguardar al individuo frente a intromisiones puntuales, sino de garantizar que los datos personales no sean utilizados para reducir a las personas a simples objetos de análisis, clasificación y predicción. La privacidad, en este sentido, emerge como un verdadero derecho habilitante, un factor clave para el ejercicio pleno de otros derechos fundamentales como la libertad de expresión, la participación democrática y la autonomía personal.

Tal como sostiene el jurista alemán Lothar Determann (2017), la privacidad no debe concebirse solo desde una óptica jurídica formalista, sino como un elemento estructural esencial que posibilita el desarrollo de una sociedad libre y plural. Este enfoque cobra especial relevancia en sociedades gobernadas por datos, donde la capacidad de controlar el flujo de información personal determina en buena medida la libertad real de las personas. En palabras de Determann, "sin seguridad no puede haber intimidad, pero puede haber seguridad sin ninguna intimidad", lo que implica que una sociedad plenamente vigilada, aunque potencialmente segura, sería incompatible con una vida democrática y autónoma.

Este razonamiento cobra aún mayor importancia al considerar que, actualmente, la inteligencia artificial y el Big Data permiten procesar información personal a gran escala, muchas veces sin un consentimiento real o consciente por parte de los usuarios. En estas condiciones, el consentimiento tradicional, que generalmente se limita a aceptar términos y condiciones de forma mecánica, resulta insuficiente para proteger adecuadamente la autodeterminación informativa. Tal como advierte Bonilla Gutiérrez (2024), "el consentimiento formal, aislado de un verdadero control, ya no alcanza"; por lo tanto, se requiere un replanteo normativo y ético profundo que permita que las personas ejerzan una autonomía efectiva sobre sus datos personales en entornos digitales complejos.

En este contexto, el debate cobra especial relevancia al observar fenómenos recientes en Argentina, como el escándalo del sistema de reconocimiento facial implementado por el

Gobierno de la Ciudad de Buenos Aires. Este sistema, si bien formalmente amparado por un marco normativo, derivó en un tratamiento masivo e indiscriminado de datos biométricos sin garantías adecuadas, lo cual fue judicialmente cuestionado. En la causa "ODIA y otros c/ GCBA s/ amparo", la Justicia porteña determinó que se habían verificado violaciones graves a derechos fundamentales como la privacidad y la presunción de inocencia, al comprobarse que más de siete millones de personas habían sido vigiladas sin causa suficiente ni control judicial previo (Cámara CAyT CABA, Sala I, 2022). Tal como advierte la Agencia de Acceso a la Información Pública, este caso refleja un problema más profundo: "la inteligencia artificial permite en algunos casos hacer tratamientos de datos legales pero poco éticos" (AAIP, 2022, p. 27), lo cual pone de relieve la urgencia de evaluar no solo la legalidad formal de los sistemas automatizados, sino también su legitimidad ética y su impacto estructural sobre los derechos fundamentales.

La privacidad, entendida así como derecho habilitante, resulta crucial también para asegurar otros derechos fundamentales en contextos donde la vigilancia y el control algorítmico pueden erosionar libertades individuales esenciales. Por ejemplo, cuando el procesamiento automatizado de datos personales determina quién accede a créditos, empleos o beneficios sociales sin posibilidad de apelación o intervención humana, no solo se pone en riesgo el derecho a la privacidad, sino también principios fundamentales de equidad, dignidad humana y no discriminación.

Por ello, la legislación argentina debe actualizarse no solo para responder a desafíos técnicos específicos, sino también para resguardar esta dimensión habilitante del derecho a la privacidad. Resulta imprescindible avanzar hacia un marco regulatorio que establezca límites claros, obligaciones de transparencia algorítmica, auditorías efectivas, y una agencia de protección de datos suficientemente fortalecida y autónoma para fiscalizar estos procesos.

En definitiva, concebir la privacidad como un derecho habilitante implica entenderla no como un obstáculo a la innovación tecnológica, sino como una garantía indispensable para que dicha innovación sea realmente inclusiva, democrática y respetuosa de los derechos fundamentales. En sociedades gobernadas por datos, proteger la privacidad equivale a proteger el derecho a ser persona en sentido pleno, y no simplemente un dato más en una cadena de procesamiento algorítmico.

En este marco, se vuelve indispensable examinar si la normativa argentina vigente, en particular la Ley 25.326, resulta suficiente para proteger los derechos fundamentales frente a las nuevas formas de tratamiento automatizado de datos personales. Esta reflexión será abordada en el próximo capítulo, donde se analizará críticamente el marco legal argentino, sus límites actuales y los desafíos regulatorios que impone la era de la inteligencia artificial.

CAPÍTULO 2: El marco legal argentino en materia de protección de datos personales

En los últimos años, la inteligencia artificial dejó de ser una promesa del futuro para convertirse en una tecnología presente en todos los ámbitos de la vida. Hoy, nuestros datos personales no solo se recopilan, se almacenan o se usan para enviarnos publicidad; también se procesan mediante sistemas automatizados que infieren, deciden y actúan, muchas veces sin que lo sepamos o lo entendamos del todo. Este tipo de tratamiento automatizado, especialmente cuando se vale de inteligencia artificial, plantea desafíos que la legislación argentina vigente no previó ni está preparada para enfrentar.

Por eso, antes de adentrarnos en el análisis técnico de la Ley 25.326, vale la pena preguntarse: ¿puede una ley pensada en un contexto analógico, con bases de datos estáticas y tratamientos manuales, responder a los dilemas que plantean los algoritmos, el aprendizaje automático y la toma de decisiones sin intervención humana? ¿Hasta qué punto nuestros derechos están protegidos cuando los sistemas que procesan nuestros datos no son auditables ni explicables?

Este capítulo propone revisar críticamente el marco normativo argentino en materia de protección de datos personales, poniendo el foco en su capacidad o su limitación para regular el tratamiento automatizado que hoy realiza la inteligencia artificial. Para eso, se analizarán los principios centrales de la Ley 25.326, sus vacíos frente al avance tecnológico y las tensiones que se generan cuando los datos se convierten en insumos para modelos que, sin pedir permiso, toman decisiones sobre nosotros.

2.1. Ley 25.326 de Protección de Datos Personales: principios y alcance

En Argentina, la protección de los datos personales se encuentra regulada por la Ley 25.326, sancionada el 4 de octubre de 2000 y reglamentada por el Decreto 1558/2001.

Esta norma se propuso, en su momento, garantizar el derecho a la privacidad de las personas, estableciendo principios rectores como la licitud, la finalidad legítima, la seguridad de los datos y los derechos de acceso, rectificación, actualización y supresión.

Sin embargo, esta legislación fue concebida en un contexto en el que la digitalización aún no tenía la relevancia actual. De hecho, ni siquiera existía Google en ese momento, lo que evidencia la brecha entre la regulación vigente y las tecnologías actuales. La idea de que máquinas serían capaces de inferir comportamientos, tomar decisiones autónomas y clasificar a las personas sin intervención humana no formaba parte del horizonte del legislador argentino a comienzos del siglo XXI. Hoy en día, los modelos de inteligencia artificial (IA) y los algoritmos de aprendizaje automático pueden procesar grandes volúmenes de datos personales de manera automatizada, sin que la legislación contemple adecuadamente los riesgos asociados a este tratamiento masivo y su impacto en los derechos individuales.

La ley define los datos personales como "toda información de cualquier tipo referida a personas físicas o de existencia ideal determinadas o determinables"(art. 2, Ley 25.326). Esta definición abarca desde datos básicos como el nombre y el Documento Nacional de Identidad (DNI) hasta información sensible, entendida como aquella que "revela origen racial y étnico, opiniones políticas, convicciones religiosas, filosóficas o morales, afiliación sindical e información referente a la salud o a la vida sexual" (art. 2, Ley 25.326). El tratamiento de estos datos está sujeto a restricciones más estrictas y, en principio, prohibido salvo excepciones expresamente previstas por la ley, como cuando "medie consentimiento expreso y escrito del titular", o con fines sanitarios, estadísticos o científicos que garanticen el anonimato (art. 7, inc. 2, Ley 25.326).

Uno de los pilares de la Ley 25.326 es el principio de consentimiento informado. En términos legales, implica que el titular de los datos debe ser debidamente informado sobre la finalidad para la cual se recaban sus datos y prestar su consentimiento previo, libre, expreso e informado para su uso. Pero en un ecosistema digital altamente automatizado, este modelo revela sus límites. Como advierte Bonilla Gutiérrez (2024), el consentimiento aislado ya no garantiza un verdadero control sobre la información: "las nuevas formas de vigilancia algorítmica impiden a los individuos ejercer un control real sobre sus datos", lo que obliga a repensar esta figura central desde una lógica de justicia sustantiva y no meramente formal.

La normativa también impone obligaciones a los responsables de bases de datos, quienes deben garantizar la seguridad y confidencialidad de la información. Asimismo, prohíbe la cesión de datos personales sin autorización del titular y se establecen excepciones limitadas para el acceso por parte de organismos públicos, siempre que se justifique un interés legítimo.

Para garantizar el cumplimiento de la ley, originalmente se creó la Dirección Nacional de Protección de Datos Personales en el ámbito del Ministerio de Justicia. Sin embargo, recién en 2017 más de quince años después de la sanción de la Ley 25.326 se transfirió la competencia en materia de protección de datos personales a la Agencia de Acceso a la Información Pública (AAIP), mediante el Decreto 899/2017, en el marco de la Ley 27.275 sobre el derecho de acceso a la información pública. La AAIP, que fue concebida originalmente con otros fines, adquirió entonces la función de autoridad de control en esta materia. Entre sus atribuciones se encuentran la de supervisar el tratamiento de datos personales, dictar regulaciones complementarias, recibir denuncias y aplicar sanciones.

Como señala Determann (2017), la privacidad no puede limitarse a ser una garantía técnica o legalista. Debe ser entendida como "un factor estructural del ejercicio de derechos fundamentales", en especial cuando los sistemas de IA no solo recolectan información, sino que clasifican, infieren y toman decisiones con impacto real sobre las personas.

Además, la computación en la nube, la circulación global de los datos y la falta de control sobre la jurisdicción donde se alojan los servidores plantean nuevos interrogantes sobre la aplicabilidad de la Ley 25.326. La fragmentación normativa entre países genera tensiones sobre la soberanía digital, la tutela efectiva y los marcos regulatorios aplicables.

Frente a este panorama, organismos como la OCDE, la UNESCO y el Consejo de Europa han comenzado a delinear principios que pueden orientar una eventual reforma legal en Argentina. Entre ellos se destacan la transparencia algorítmica, la supervisión humana, la evaluación de impacto y la rendición de cuentas. En este sentido, el Convenio 108+ modificación modernizada del Convenio 108 del Consejo de Europa al que Argentina adhirió mediante la Ley 27.699, aún no ha entrado en vigor, ya que requiere la ratificación de al menos 38 países para su plena operatividad. Aun así, su incorporación

anticipada ofrece un marco de referencia relevante para armonizar estándares en el plano internacional.

2.2. Debilidades del régimen normativo frente al tratamiento automatizado de datos personales.

A pesar de que la Ley 25.326 posicionó a Argentina como un país con un nivel adecuado de protección de datos, especialmente desde una perspectiva internacional, lo cierto es que su eficacia normativa se encuentra cada vez más cuestionada frente al avance vertiginoso de las nuevas tecnologías. La normativa fue pensada para un ecosistema analógico, donde los datos personales se recolectaban en formularios físicos, los tratamientos eran lineales y los riesgos predecibles. Ese escenario contrasta radicalmente con la realidad contemporánea, en la que algoritmos de inteligencia artificial y modelos predictivos procesan millones de datos de forma automatizada, continua y a una escala difícil de controlar.

Uno de los principales problemas es la centralidad que se otorga al consentimiento informado como fundamento del tratamiento de datos personales. En la práctica, este principio se ha tornado insuficiente para garantizar una protección real. En un entorno digital hiperconectado y automatizado, donde los datos se recolectan y procesan sin intervención consciente del usuario, este modelo deviene insuficiente. La falta de control real por parte de los titulares sobre cómo se recaba, utiliza y comparte su información representa una amenaza para sus derechos fundamentales.

Además, la legislación vigente no contempla de manera específica ni los sistemas de inteligencia artificial ni los algoritmos automatizados que hoy intervienen en decisiones que afectan directamente derechos fundamentales: desde la aprobación de un crédito hasta la selección de un candidato en un proceso laboral. No hay previsiones sobre explicabilidad algorítmica, revisión humana ni rendición de cuentas, lo que impide a los ciudadanos cuestionar o entender cómo y por qué se ha tomado determinada decisión. Este vacío normativo genera lo que se conoce como efecto “caja negra”, donde los procesos son tan opacos que ni siquiera los desarrolladores pueden dar cuenta con precisión del camino que recorrió el sistema para llegar a un resultado. Esto impide establecer criterios claros de supervisión, explicabilidad y transparencia algorítmica, elementos indispensables en un contexto donde las decisiones automatizadas pueden tener consecuencias significativas para la vida de las personas.

Además de las limitaciones normativas, existen problemas de implementación institucional. La Agencia de Acceso a la Información Pública (AAIP), organismo encargado de hacer cumplir la ley, enfrenta serias dificultades para fiscalizar el uso de tecnologías emergentes. Las atribuciones limitadas y los escasos recursos con los que cuenta la AAIP dificultan su capacidad de fiscalizar eficazmente el uso de tecnologías emergentes en el tratamiento de datos personales. Esto genera una brecha cada vez más profunda entre lo que la ley prescribe y lo que efectivamente puede controlar.

El desfase entre ley y realidad fue advertido también por Daniel Monastersky (2019), quien señaló que la normativa argentina fue diseñada en un tiempo en que el procesamiento masivo de información no existía. Esa distancia histórica se traduce hoy en una debilidad estructural: no hay reglas claras sobre entrenamiento de algoritmos, inferencia de datos sensibles, tratamiento de datos por IA generativa ni control de decisiones automatizadas. Como consecuencia, se multiplican los escenarios grises donde los derechos individuales quedan desprotegidos.

A su vez, distintos especialistas han propuesto considerar a la inteligencia artificial como una actividad riesgosa en los términos del artículo 1757 Código Civil y Comercial, lo que permitiría establecer un régimen de responsabilidad ante daños derivados de su uso. Esta interpretación, respaldada por parte de la doctrina, permitiría exigir reparación sin necesidad de probar culpa, dado que se trataría de una actividad peligrosa por su potencial lesivo y nivel de autonomía. Tal como sugiere Peruzzotti (2023), “la IA puede encuadrarse como una actividad riesgosa en la medida en que su despliegue técnico supera el control humano y puede generar daños imprevisibles, aún bajo pautas de diligencia razonable”. Esta vía busca suplir, al menos parcialmente, el vacío normativo actual mediante la aplicación analógica de institutos jurídicos ya vigentes, aunque no exime la necesidad urgente de un marco legal específico que aborde los desafíos estructurales del uso de sistemas automatizados.

Otra problemática creciente es la circulación transfronteriza de datos personales. En la era de la computación en la nube, los datos de los argentinos pueden ser procesados y almacenados en jurisdicciones extranjeras, sujetas a normativas que no siempre garantizan niveles adecuados de protección. Esto debilita la capacidad del Estado argentino para ejercer soberanía digital, y dificulta el acceso a mecanismos efectivos de reparación en caso de abuso.

Finalmente, casos como el de DeepSeek, donde se cuestionó la legalidad y el origen de los datos utilizados para entrenar modelos de IA, ponen en evidencia los vacíos regulatorios más críticos. La recolección opaca de datos, el uso de información sensible sin consentimiento explícito y la falta de mecanismos para auditar estos procesos son síntomas de una normativa que no logra dar respuesta a los dilemas éticos y jurídicos de la inteligencia artificial.

Frente a este escenario, la necesidad de reformar el marco legal argentino ya no puede postergarse. No se trata únicamente de actualizar una norma que ha quedado obsoleta, sino de repensar el sistema de protección de datos desde sus fundamentos frente a tecnologías que tensionan los principios clásicos del derecho. Por ejemplo, el principio de legalidad requiere que todo tratamiento de datos se apoye en una base jurídica clara, pero en muchos casos el uso de información para entrenar algoritmos no se sustenta en ninguna justificación específica ni en el consentimiento informado del titular. El principio de calidad del dato exige exactitud y actualización permanente, algo difícil de garantizar cuando los modelos de IA incorporan información errónea o generan "alucinaciones" que pueden perjudicar a las personas. El principio de finalidad también se ve afectado, ya que los datos son reutilizados para fines distintos a los originales como el entrenamiento de sistemas predictivos sin que se informe ni se autorice expresamente ese nuevo uso. A ello se suma la imposibilidad práctica de ejercer derechos como la rectificación o la supresión, especialmente cuando los datos han sido incorporados a sistemas opacos o diseminados globalmente. Incluso el principio de transparencia, que exige informar al titular sobre el tratamiento, suele limitarse al momento inicial de la recolección, sin que se brinde información posterior sobre el uso, cesión o filtración de datos (data breaches).

Tal como advierte el Comité Europeo de Protección de Datos en su Opinión 28/2024, muchos de estos principios fundacionales se ven desbordados por las lógicas operativas de los sistemas de IA, lo que pone en riesgo la efectividad de las garantías del RGPD en entornos automatizados. Estos desajustes normativos reflejan que no solo faltan normas técnicas para regular la inteligencia artificial, sino que los principios rectores del régimen actual se ven desbordados por el modelo tecnológico dominante. Por eso, repensar la ley implica también resignificar los principios fundantes de la protección de datos personales en clave de derechos humanos y en un entorno cada vez más automatizado.

2.3. Propuestas de actualización legislativa ante los desafíos de la inteligencia artificial.

Frente al diagnóstico crítico sobre las limitaciones de la Ley 25.326, resulta evidente que la normativa argentina necesita una revisión profunda y estructural. No se trata de una simple modernización técnica, sino de adaptar el marco legal a una nueva realidad donde los datos personales ya no son únicamente registros pasivos, sino insumos fundamentales para sistemas de inteligencia artificial que predicen, clasifican y toman decisiones que afectan directamente los derechos de las personas.

Una de las reformas más urgentes es la incorporación del principio de responsabilidad proactiva. Esta noción, ya presente en el RGPD europeo, obliga a quienes procesan datos personales mediante sistemas automatizados a anticiparse a los riesgos, no solo a responder ante ellos. En la práctica, esto supone implementar auditorías periódicas, adoptar medidas de privacidad y seguridad desde el diseño (privacy and security by design) y por defecto, DPO, transferencias internacionales, contratos de tratamiento con encargados y llevar adelante evaluaciones de impacto en la privacidad antes de desplegar tecnologías que puedan afectar derechos fundamentales. Como plantea Baca Rivero (2021), "la incorporación por diseño de los principios de privacidad y transparencia permitiría garantizar el tratamiento legítimo de los datos personales sin necesidad de limitar el desarrollo tecnológico".

En este sentido, también debe consagrarse el derecho a la explicabilidad, entendido como la posibilidad de que una persona comprenda los motivos detrás de una decisión tomada por un sistema automatizado. Es importante diferenciar este concepto de la interpretabilidad: mientras que la explicabilidad apunta a que el sistema pueda brindar razones claras y comprensibles al usuario final, la interpretabilidad se vincula más con la comprensión técnica del funcionamiento interno del modelo algorítmico, algo que suele estar restringido a especialistas. Ambos principios son complementarios, pero el derecho a la explicabilidad resulta indispensable desde una perspectiva ciudadana, ya que fortalece la posibilidad de impugnar decisiones injustas y evita que los algoritmos operen como cajas negras fuera del control democrático.

A su vez, debe garantizarse la intervención humana efectiva ante decisiones automatizadas de alto impacto, recuperando la dimensión ética y deliberativa que caracteriza al Estado de derecho. Este principio está recogido en el Reglamento de IA de

la Unión Europea (Reglamento de IA), aprobado en 2024, el cual establece criterios diferenciados para sistemas de riesgo inaceptable, alto, medio o mínimo, y exige mecanismos de supervisión humana especialmente en áreas sensibles como la justicia, la salud o el empleo.

Otra línea prioritaria es la regulación específica del uso de tecnologías sensibles, como los sistemas de reconocimiento facial o el tratamiento de datos biométricos. La ausencia de reglas claras en esta materia ha permitido prácticas de vigilancia masiva sin control ni rendición de cuentas. Establecer límites concretos, criterios de necesidad y proporcionalidad, y exigir autorizaciones judiciales en contextos de uso estatal son medidas básicas para evitar abusos. En Estados Unidos, por ejemplo, diversos estados han comenzado a dictar leyes específicas sobre inteligencia artificial: la ciudad de Nueva York ha establecido requisitos de auditoría y transparencia para herramientas de IA utilizadas en procesos de contratación laboral, buscando prevenir discriminaciones algorítmicas (NYC Local Law 144/2021).

Por otro lado, se vuelve necesario dotar a la Agencia de Acceso a la Información Pública (AAIP), la cual es la autoridad de aplicación local en lo que concierne a la supervisión de la protección de datos personales, de mayores recursos técnicos, autonomía y capacidad de fiscalización. En un escenario donde las grandes corporaciones tecnológicas concentran poder sobre los datos y los algoritmos, un organismo débil o subfinanciado corre el riesgo de convertirse en un actor meramente simbólico. La AAIP debe transformarse en una autoridad robusta, capaz de auditar sistemas de IA, imponer sanciones y acompañar el desarrollo tecnológico desde una perspectiva de derechos.

A nivel normativo, el debate también debe incluir la posibilidad de establecer una ley general de inteligencia artificial o, alternativamente, avanzar en una regulación sectorial como lo ha hecho Estados Unidos con marcos como la Ley de Colorado sobre sistemas de IA de alto riesgo. Lo importante es que el camino elegido responda a las necesidades del contexto local y no a modelos importados sin una reflexión crítica. En ese sentido, la experiencia del Reglamento de IA europeo ofrece un ejemplo de legislación integral y basada en principios, pero su aplicabilidad debe ser cuidadosamente evaluada en función de las capacidades institucionales argentinas.

Finalmente, cabe destacar que en Argentina se están dando pasos incipientes hacia una regulación más adaptada. La AAIP elaboró en 2023 un proyecto de ley de protección

de datos personales mediante un proceso participativo que contó con la intervención de actores académicos, empresariales y de la sociedad civil, aunque aún no ha sido tratado en profundidad por el Congreso. A su vez, existen múltiples proyectos legislativos sobre inteligencia artificial presentados en la Cámara de Diputados, y en el ámbito de la Comisión de Ciencia y Tecnología se han llevado a cabo audiencias públicas para debatir los desafíos regulatorios de estas tecnologías emergentes. Esta apertura institucional resulta prometedora, aunque todavía incipiente.

Como advierte Bonilla Gutiérrez (2024), "las nuevas formas de vigilancia algorítmica no solo erosionan la privacidad, sino que también impiden a los individuos ejercer un control real sobre sus datos". Frente a ello, la regulación no debe limitarse a lo declarativo. Necesita ser efectiva, operativa y profundamente comprometida con la dignidad humana. Solo así será posible que el desarrollo de la inteligencia artificial en Argentina se inscriba en un horizonte democrático, inclusivo y justo.

CAPÍTULO 3: Análisis comparado de Marcos Regulatorios sobre IA y Protección de Datos

En este apartado se analiza cómo podría adecuarse el marco normativo argentino para hacer frente a los desafíos del tratamiento automatizado de datos personales mediante inteligencia artificial. A partir del estudio comparado de regulaciones internacionales y de los proyectos legislativos locales, se proponen orientaciones para una regulación efectiva y con enfoque en derechos humanos.

3.1. Enfoque comparado en la regulación del tratamiento automatizado de datos personales: una introducción

La regulación del tratamiento automatizado de datos personales mediante inteligencia artificial constituye uno de los desafíos jurídicos más significativos de la era digital. Lejos de tratarse de una problemática exclusivamente local, los efectos de la automatización trascienden las fronteras y requieren respuestas integradas, informadas por las experiencias de otros países y bloques normativos. En este sentido, el análisis comparado emerge como una herramienta indispensable para construir marcos regulatorios eficaces, sensibles a los derechos humanos y adaptados al nuevo ecosistema tecnológico.

Tal como sostiene Mayer-Schönberger (2018), "el análisis comparado permite identificar tanto las mejores prácticas como los errores regulatorios más frecuentes en el tratamiento automatizado de datos personales mediante IA, enriqueciendo el debate local con experiencias internacionales relevantes" (p. 36). Esta mirada no pretende importar soluciones en forma acrítica, sino evaluar qué aspectos podrían ser integrados, adaptados o incluso superados en función de las particularidades del contexto argentino.

Desde esta perspectiva, el presente capítulo se estructura en torno a cuatro modelos jurídicamente relevantes: la Unión Europea, con énfasis en el Reglamento General de Protección de Datos (RGPD), el recientemente aprobado Reglamento de Inteligencia Artificial (Reglamento de IA) y la Opinión 28/2024 del Comité Europeo de Protección de Datos, Brasil a través de su Ley General de Protección de Datos (LGPD), Estados Unidos centrado en el enfoque sectorial y la Ley de IA del estado de Colorado, y Alemania como jurisdicción clave en el desarrollo histórico del derecho a la autodeterminación informativa.

La elección de estos casos se basa tanto en su influencia normativa como en su relevancia doctrinaria y técnica. La Unión Europea ha consolidado un modelo garantista basado en la dignidad humana y el principio de precaución. El RGPD, junto con el Reglamento de IA aprobado en 2024, establece una arquitectura legal integrada para la protección de datos personales y la regulación del desarrollo y uso de sistemas de inteligencia artificial. Este último clasifica los sistemas según el nivel de riesgo y exige requisitos estrictos para aquellos considerados de alto impacto, tales como evaluaciones de conformidad, registro obligatorio, trazabilidad, documentación técnica y supervisión humana (Parlamento Europeo y Consejo de la Unión Europea, 2024).

Brasil, en tanto, ha demostrado cómo adaptar esos estándares a un marco latinoamericano con instituciones en desarrollo. Estados Unidos ofrece un enfoque pragmático, descentralizado y basado en la autorregulación sectorial, con ejemplos recientes de avance como la AI Bill of Rights y la legislación de Colorado. Alemania, por su parte, aporta una base teórica robusta, al haber dado origen a la noción de autodeterminación informativa tras experiencias históricas de vigilancia estatal.

Como advierte Lothar Determann (2017), “el análisis de distintos modelos regulatorios permite comprender mejor cómo la protección de datos puede alinearse con diferentes prioridades sociales, desde la seguridad nacional hasta la defensa activa de la

dignidad humana y la autodeterminación informativa" (p. 23). En su enfoque comparado, subraya que mientras en Europa la privacidad es un derecho fundamental autónomo, en Estados Unidos se encuentra subordinada a valores como la libertad de empresa, la eficiencia y la seguridad nacional, lo que deriva en regulaciones fragmentadas y asimétricas.

A su vez, en los últimos años, organismos como el Comité Europeo de Protección de Datos han comenzado a emitir directrices específicas sobre inteligencia artificial, como la Opinión 28/2024, que exige que los sistemas de IA se diseñen con salvaguardas jurídicas, técnicas y organizativas que garanticen transparencia, explicabilidad y minimización del uso de datos personales. Estas directrices se complementan ahora con el Reglamento de IA, que representa el primer marco normativo integral y vinculante para la IA en el ámbito internacional.

Este enfoque comparado no solo enriquece el debate académico, sino que constituye una guía práctica para pensar reformas legales en Argentina. Al analizar cómo otras jurisdicciones han abordado el tratamiento automatizado de datos personales qué principios han priorizado, qué mecanismos han utilizado, qué tensiones han debido enfrentar se abren caminos posibles para una regulación más robusta, que combine eficacia tecnológica con protección de derechos fundamentales. En esa línea, la discusión debe enmarcarse explícitamente en clave de derechos fundamentales privacidad y protección de datos, de modo que cualquier reforma respete, como mínimo, los principios de legalidad, finalidad, minimización, transparencia y revisión humana efectiva. En este sentido, resulta pertinente mencionar que en el Congreso argentino existen numerosos proyectos con estado parlamentario que buscan regular la inteligencia artificial; por ejemplo, el Expediente 1937-D-2025, presentado por el diputado Gabriel Felipe Chumpitaz, que propone regular el uso y desarrollo de la IA e incluso la creación de un Ministerio de IA. Si bien ambas iniciativas representan avances en el debate local, aún no abordan de manera integral aspectos clave como la protección de datos personales, la explicabilidad algorítmica o los mecanismos efectivos de rendición de cuentas. En este punto, el reciente informe del Comisionado de Hamburgo para la Protección de Datos y la Libertad de Información (2024) ofrece insumos valiosos para el debate local, ya que alerta sobre riesgos que podrían replicarse en Argentina si la legislación no los contempla expresamente. El documento advierte que el entrenamiento de modelos de lenguaje de gran escala (LLM), como ChatGPT, suele realizarse sin bases legales claras, sin

transparencia suficiente y sin mecanismos efectivos para ejercer derechos como la supresión o la oposición. En el contexto de esta tesina, dicha advertencia resulta especialmente relevante, pues evidencia cómo los fundamentos mismos del régimen de protección de datos, legalidad, finalidad, minimización y transparencia, pueden verse desbordados por la lógica expansiva de la IA generativa, lo que refuerza la urgencia de que los proyectos de ley argentinos incorporen salvaguardas específicas en esta materia.

3.2. Comparación con otros marcos regulatorios: tratamiento automatizado de datos personales mediante inteligencia artificial

La expansión del uso de inteligencia artificial (IA) en la toma de decisiones automatizadas ha obligado a los Estados a revisar sus marcos normativos en materia de protección de datos personales. Sin embargo, los enfoques regulatorios adoptados por distintas jurisdicciones presentan divergencias sustanciales, tanto en su filosofía jurídica como en su arquitectura institucional. En este apartado se analiza comparativamente la respuesta normativa de Brasil, Estados Unidos (con foco en la ley estatal de Colorado), Alemania y la Unión Europea, con el objetivo de identificar modelos y principios que puedan resultar útiles para una eventual reforma legal en Argentina.

En el caso europeo, debe destacarse especialmente la reciente adopción del Reglamento de Inteligencia Artificial (Reglamento de IA) por parte de la Unión Europea, que complementa el marco general del RGPD con una regulación específica para sistemas de IA. Este reglamento clasifica los sistemas de IA según su nivel de riesgo e impone requisitos estrictos para aquellos considerados de alto riesgo, como los utilizados en áreas como recursos humanos, servicios financieros, educación o justicia. Entre sus exigencias, el Reglamento de IA establece la necesidad de realizar evaluaciones de conformidad antes de su comercialización, registrar los sistemas en bases de datos públicas accesibles y garantizar principios de transparencia, trazabilidad y supervisión humana efectiva. Esta herramienta normativa representa un hito en el derecho comparado, al ofrecer un marco legal comprehensivo que conjuga innovación tecnológica con garantías fundamentales, y resulta particularmente relevante como referencia para países como Argentina que aún no cuentan con legislación específica en la materia. Cabe señalar que el Reglamento de IA se aplica “sin perjuicio” del RGPD, por lo que en materia de protección de datos personales este último prevalece en caso de conflicto, dado su carácter de regulación específica de un derecho fundamental (DLA Piper, 2024). Un ejemplo de posible tensión

normativa se presenta en el tratamiento de datos biométricos: mientras el RGPD establece fuertes restricciones para su uso, el Reglamento de IA permite su tratamiento en contextos excepcionales, como para detectar sesgos en sistemas de alto riesgo, siempre que se apliquen salvaguardas adicionales. Este tipo de situaciones podría requerir aclaraciones regulatorias futuras para evitar conflictos de interpretación.

3.2.1. Brasil y la Ley General de Protección de Datos (LGPD)

Brasil constituye un referente en América Latina en materia de protección de datos personales. La Ley General de Protección de Datos (LGPD), sancionada en 2018, fue fuertemente influenciada por el Reglamento General de Protección de Datos (RGPD) europeo, aunque con adaptaciones al contexto regional. Uno de sus principales aportes es el reconocimiento del tratamiento automatizado de datos como un área que requiere especial atención, al establecer una serie de derechos consistentes en la posibilidad de solicitar la revisión de decisiones tomadas exclusivamente por medios automatizados, exigir explicaciones sobre los criterios utilizados y oponerse a determinadas decisiones (art. 20 LGPD).

Una diferencia destacable entre la LGPD y la Ley 25.326 argentina es la noción de consentimiento granular, que permite a los titulares decidir de forma específica qué datos desean compartir y con qué finalidad. Esta posibilidad refuerza el principio de autodeterminación informativa y contrasta con la formulación más genérica presente en la legislación argentina. Además, la LGPD contempla la obligación de ofrecer explicaciones claras sobre los criterios utilizados en decisiones automatizadas (art. 20, inc. 1), lo cual constituye un avance hacia la transparencia algorítmica (Doneda & Monteiro, 2020).[1]

La creación de la Autoridad Nacional de Protección de Datos (ANPD) en Brasil ha sido clave para el monitoreo y fiscalización del cumplimiento normativo, permitiendo una supervisión más eficaz del uso de tecnologías como la IA, en especial en sectores sensibles como salud, crédito y recursos humanos.

[1] Art. 20, LGPD: "El titular de los datos personales tiene derecho a solicitar la revisión de las decisiones tomadas únicamente sobre la base de tratamiento automatizado de datos personales que afecten sus intereses, incluidos los relativos a su perfil profesional, de consumo, de crédito o a los aspectos de su personalidad."

Un caso concreto de aplicación de la LGPD se observa en el Instituto Nacional del Seguro Social (INSS) de Brasil. El INSS ha implementado sistemas automatizados para el reconocimiento de derechos previsionales, como la concesión de beneficios. Sin embargo, estudios han señalado que, aunque existe el derecho a la explicación de decisiones automatizadas, su implementación práctica ha sido deficiente. Esto plantea desafíos significativos para garantizar que los ciudadanos comprendan y puedan impugnar decisiones que afectan directamente sus derechos.

Renato Leite Monteiro ha destacado que, aunque la LGPD ofrece elementos para el reconocimiento de un derecho a la explicación, aún existe incertidumbre respecto al alcance y diseño exacto de este derecho en el ordenamiento brasileño. Subraya la necesidad de una regulación más clara y de jurisprudencia que delimite adecuadamente este derecho.

Por su parte, Danilo Doneda considera que la LGPD es un elemento estructurante del modelo brasileño de protección de datos, proporcionando herramientas para la tutela efectiva de los derechos de los titulares. Sin embargo, enfatiza la importancia de una aplicación eficiente por parte de la Autoridad Nacional de Protección de Datos (ANPD) y del Poder Judicial para garantizar que los principios de la ley se traduzcan en prácticas concretas que protejan a los ciudadanos.

En 2024, un estudio realizado por la Fundación Getulio Vargas reveló que las principales plataformas de inteligencia artificial generativa no están cumpliendo adecuadamente con las disposiciones de la LGPD, especialmente en lo relativo al principio de legalidad, la transparencia en el tratamiento y la posibilidad de ejercer derechos como la rectificación o la supresión. Este informe pone de manifiesto la distancia entre los estándares normativos y su aplicación práctica en un contexto de rápida expansión tecnológica.[2]

En el marco de una posible reforma legislativa en Argentina, la experiencia brasileña ofrece varias lecciones útiles. Entre ellas, se destacan la necesidad de contemplar explícitamente el derecho a la revisión de decisiones automatizadas, exigir explicaciones claras sobre los criterios algorítmicos, incorporar el consentimiento

[2] Fundação Getulio Vargas (2024). "Plataformas de IA não cumprem a LGPD, diz estudo da FGV." Disponible en: https://www.poder360.com.br/poder-tech/plataformas-de-ia-nao-cumprem-a-lgpd-diz-estudo-da-fgv/

granular como expresión de la autodeterminación informativa, y fortalecer el rol de la autoridad de control mediante la creación de una entidad independiente con facultades sancionatorias y técnicas robustas.

3.2.2. Estados Unidos y la Ley de Inteligencia Artificial del Estado de Colorado

El enfoque estadounidense se caracteriza por su fragmentación y fuerte descentralización normativa. A diferencia de la Unión Europea, no existe una legislación federal única en materia de protección de datos personales. En su lugar, coexisten leyes estaduales como la California Consumer Privacy Act (CCPA) y la recientemente aprobada Ley de Inteligencia Artificial del Estado de Colorado (2024), junto con leyes federales sectoriales la Health Insurance Portability and Accountability Act (HIPAA) en el ámbito de la salud. Esta diversidad normativa genera asimetrías en la protección de los derechos según el sector y la jurisdicción.

Según Determann (2017), esta particularidad del modelo estadounidense presenta serias limitaciones: "el enfoque fragmentado de EE.UU. sobre protección de datos genera incertidumbres jurídicas y puede llevar a una protección desigual de los derechos fundamentales según el Estado o el sector involucrado" (p. 45). Esta fragmentación, aunque ofrece flexibilidad regulatoria, también implica desafíos importantes en términos de coherencia normativa y previsibilidad jurídica.

En este contexto, la Ley de Inteligencia Artificial del Estado de Colorado (2024) representa un punto de inflexión significativo. Promulgada en mayo de 2024 y con entrada en vigor prevista para febrero de 2026, esta norma establece por primera vez obligaciones específicas para el uso de sistemas de IA de alto riesgo. Se trata de la primera ley estadounidense que establece obligaciones específicas para el uso de sistemas de inteligencia artificial considerados de alto riesgo. Entre sus disposiciones principales, destacan la exigencia de realizar evaluaciones de impacto en privacidad, la obligación de notificar explícitamente a los usuarios cuando interactúan con sistemas automatizados, y la implementación obligatoria de mecanismos de reporte ante incidentes algorítmicos, todo lo cual marca un avance considerable en términos de responsabilidad y transparencia algorítmica. (Mayer Brown, 2024).

No obstante, Colorado no constituye un caso aislado dentro del mapa regulatorio estadounidense. El Estado de California, históricamente pionero en materia de derechos

digitales, ha adoptado en 2024 una serie de leyes que buscan posicionarlo a la vanguardia de la regulación de la inteligencia artificial. Entre ellas, se destaca la California AI Transparency Act (SB-942), sancionada en septiembre de 2024 y con entrada en vigor prevista para enero de 2026. Esta ley obliga a los proveedores de sistemas de inteligencia artificial generativa con más de un millón de usuarios mensuales a incorporar marcas visibles o latentes en el contenido generado por IA, ofrecer herramientas gratuitas de detección de contenido sintético y publicar reportes sobre los datos utilizados en el entrenamiento de los modelos. Junto con esta ley, California también promulgó normas orientadas a regular los deepfakes, especialmente en contextos sensibles como la educación, las campañas políticas y la protección de menores, consolidando así un enfoque normativo basado en la protección de los derechos fundamentales frente al uso indebido de tecnologías algorítmicas.

Además, el Senado californiano debatió en 2024 el proyecto SB 1047, conocido como Safe and Secure Innovation for Frontier AI Models Act, que, si bien fue finalmente vetado por el gobernador, contenía propuestas innovadoras como la auditoría obligatoria de modelos de frontera, la creación de mecanismos de apagado ("kill switches") y la evaluación obligatoria de riesgos. Este proyecto, aunque no fue sancionado, refleja la intensidad del debate legislativo en torno a la IA en California y la voluntad política de abordar sus implicancias desde una perspectiva preventiva. A nivel federal, se destaca la propuesta conocida como AI Bill of Rights, impulsada por la Casa Blanca en 2023. Esta iniciativa busca establecer principios rectores para el uso de IA, como la transparencia algorítmica, el consentimiento informado y el derecho a impugnar decisiones automatizadas que afecten derechos fundamentales.

Por su parte, el Estado de Maryland creó una Comisión de Inteligencia Artificial Responsable, con el objetivo de evaluar el impacto de estas tecnologías y proponer un marco regulatorio adecuado, lo que da cuenta de una tendencia emergente a nivel estadual hacia una regulación más robusta de la IA.

Este escenario normativo estatal se consolidó como reacción directa al rechazo en el Congreso federal de una propuesta para imponer una moratoria de 10 años que prohibiría a los estados legislar sobre IA. El 2 de julio de 2025, el Senado eliminó esta cláusula por una votación de 99–1, confirmando que los estados mantienen autonomía regulatoria. Esta decisión respalda el creciente fenómeno de 'AI Gold Rush' en más de

45 jurisdicciones estatales, con casi 700 proyectos presentados en 2025, reafirmando el rol central de los estados frente a la ausencia de una ley federal general sobre IA.

A nivel federal, debe mencionarse la propuesta conocida como AI Bill of Rights, impulsada por la Casa Blanca en 2023. Este documento, de carácter programático, busca establecer principios rectores para el desarrollo y uso ético de la inteligencia artificial, como la transparencia algorítmica, el consentimiento informado y el derecho a impugnar decisiones automatizadas que afecten derechos fundamentales. Aunque no tiene fuerza legal vinculante, esta iniciativa federal aporta un marco conceptual valioso para la futura legislación sobre IA en Estados Unidos.

Este enfoque sectorial, aunque pragmático, se alinea con una concepción operativa del riesgo, permitiendo un desarrollo normativo incremental sin la necesidad inmediata de una reforma federal integral. Para el contexto argentino, el modelo regulatorio adoptado en Colorado y California, complementado con otras iniciativas emergentes como el AI Bill of Rights y las leyes estatales de Maryland, demuestra que se puede avanzar en regulaciones concretas sobre inteligencia artificial, incluso sin tener una ley nacional unificada. En lugar de esperar una reforma federal, estos estados empezaron a regular la IA en áreas clave como la salud, la educación o la justicia. Este enfoque muestra que es posible actuar de forma gradual, enfocándose en los sectores más sensibles. Medidas como exigir evaluaciones de impacto, garantizar transparencia sobre cómo funcionan los algoritmos, avisar a los usuarios cuando están frente a un sistema automatizado y crear mecanismos de control institucional pueden servir como guía para pensar cómo regular la IA en Argentina. La clave sería adaptar esas buenas prácticas internacionales a nuestra propia realidad.

3.2.3. Alemania y la tradición europea de protección de datos

Alemania ocupa un lugar fundacional en la construcción del derecho a la protección de datos personales, no solo a nivel europeo sino global. En 1970, el estado federado de Hesse sancionó la primera ley del mundo en esta materia, como respuesta directa a los abusos sistemáticos de vigilancia cometidos durante el nazismo y el régimen de la RDA. Esta experiencia histórica generó una profunda sensibilidad jurídica frente a los riesgos del control estatal y sentó las bases de un enfoque preventivo, centrado en la dignidad humana y la autonomía individual. La noción de autodeterminación informativa, desarrollada por el Tribunal Constitucional alemán a partir del caso del censo poblacional

de 1983, se convirtió en un hito doctrinario que inspiró posteriormente la formulación del derecho a la protección de datos como un derecho fundamental en Europa.

Esa tradición influyó directamente en la Directiva de Protección de Datos que rigió entre el 95 y el 2018 cuando empezó a regir el Reglamento General de Protección de Datos (RGPD) de la Unión Europea, que consolidó una visión proactiva y de base garantista. En su artículo 8, la Carta de Derechos Fundamentales de la Unión Europea consagra el derecho a la protección de datos personales como un derecho autónomo, y el RGPD lo traduce en obligaciones concretas para los responsables del tratamiento. En particular, impone estándares rigurosos en contextos donde intervienen sistemas automatizados, estableciendo:

La obligación de realizar evaluaciones de impacto (art. 35) en casos de tratamientos que puedan entrañar riesgos elevados para los derechos y libertades de las personas físicas.

El derecho a no ser sometido a decisiones basadas únicamente en un tratamiento automatizado, incluida la elaboración de perfiles, salvo ciertas excepciones (art. 22).

La exigencia de transparencia algorítmica y la garantía de una intervención humana significativa, especialmente cuando dichas decisiones puedan producir efectos jurídicos o afecten significativamente a la persona.

En línea con estos principios, el Comité Europeo de Protección de Datos (EDPB) emitió recientemente la Opinión 28/2024, centrada en el tratamiento de datos personales por parte de modelos de inteligencia artificial generativa. En este documento, se enfatiza que los sistemas de IA deben diseñarse y desplegarse respetando los principios de privacidad desde el diseño y por defecto, incorporando salvaguardas jurídicas, técnicas y organizativas que garanticen la minimización de datos, la evitabilidad de decisiones automatizadas opacas, y la explicabilidad de los resultados algorítmicos. La Opinión también subraya la importancia de asegurar que los individuos mantengan control sobre su información, incluso en entornos donde la inferencia y el perfilado automatizado son la norma.

Esta articulación entre tradición jurídica e innovación normativa refleja la capacidad del modelo europeo y en particular, del enfoque alemán, para responder a los desafíos emergentes sin renunciar a sus fundamentos democráticos. Para países como

Argentina, esta experiencia demuestra que es posible avanzar en marcos regulatorios sólidos, respetuosos de los derechos fundamentales y adaptados a las complejidades tecnológicas del presente.

3.3. Adaptaciones al contexto argentino: hacia una regulación efectiva del tratamiento automatizado de datos personales mediante inteligencia artificial

3.3.1. Proyectos legislativos argentinos vinculados a inteligencia artificial y protección de datos personales[3]

El debate parlamentario en torno a la regulación de la inteligencia artificial en Argentina ha comenzado a emerger en los últimos años, impulsado por la creciente preocupación por los impactos sociales, éticos y jurídicos de estas tecnologías. Sin embargo, este proceso aún se encuentra en una etapa incipiente y fragmentada, con propuestas legislativas que, si bien marcan avances conceptuales, no logran articular un marco integral capaz de abordar de forma efectiva el tratamiento automatizado de datos personales mediante inteligencia artificial.

Entre los proyectos que actualmente cuentan con estado parlamentario se destacan dos iniciativas: el presentado por la diputada Graciela Caamaño (Expte. 3420-D-2022) y el del senador Mariano Recalde (Expte. S-2893/22). Ambos coinciden en incorporar la temática de la IA a la agenda legislativa nacional, pero lo hacen desde enfoques limitados y sin anclaje suficiente en el derecho a la protección de los datos personales.

El proyecto de Caamaño propone una "Ley de Inteligencia Artificial Ética", con foco en la promoción del desarrollo federal de la IA, la elaboración de principios orientadores y la creación de una Comisión Nacional de Inteligencia Artificial. No obstante, carece de disposiciones vinculantes en materia de transparencia algorítmica, derechos de los titulares de datos o mecanismos efectivos de rendición de cuentas ante decisiones automatizadas. Tampoco prevé obligaciones específicas en relación con evaluaciones de impacto o sistemas de alto riesgo, ni articula con la Agencia de Acceso a la Información Pública (AAIP) como órgano competente.

Por su parte, el proyecto de Recalde establece lineamientos para una Estrategia Nacional de IA, incluyendo objetivos generales, principios éticos y la creación de un Observatorio de Inteligencia Artificial. Aunque menciona la necesidad de prevenir sesgos

[3] Ver cuadro comparativo de los proyectos de ley presentados en Argentina. Anexo A.

y respetar derechos fundamentales, el texto no incorpora obligaciones normativas claras ni contempla el impacto específico de la IA en el tratamiento de datos personales. Así, la iniciativa se posiciona más como un marco orientativo que como un régimen regulatorio efectivo.

En contraste, el anteproyecto elaborado por la AAIP en 2023, mediante un proceso participativo y con base en buenas prácticas internacionales, constituye un esfuerzo técnico y jurídico más robusto. La propuesta de reforma de la Ley 25.326 contempla expresamente disposiciones sobre tratamiento automatizado de datos, establece la obligación de realizar evaluaciones de impacto en la privacidad, exige transparencia y explicabilidad algorítmica, y prevé la creación de un registro de actividades de tratamiento que incluya sistemas de IA de alto riesgo. Además, fortalece el rol de la AAIP como autoridad de control, asignándole mayores capacidades para supervisar tecnologías complejas.

Este proyecto fue retomado parcialmente por el Poder Ejecutivo Nacional en su "Versión junio 2023" del proyecto oficial de reforma de la Ley 25.326. En particular, su artículo 28 establece que los titulares de datos tienen derecho a no ser sometidos a decisiones exclusivamente automatizadas que produzcan efectos jurídicos o significativamente similares, salvo consentimiento explícito o habilitación legal. También se incorpora el deber de proporcionar información clara sobre la lógica aplicada, la importancia y las consecuencias previstas del tratamiento automatizado, en línea con el artículo 22 del Reglamento General de Protección de Datos de la Unión Europea (RGPD).

Sin embargo, este proyecto aún no ha sido tratado formalmente en el Congreso ni articulado con las otras iniciativas sobre inteligencia artificial. Esta desconexión revela una falta de coordinación legislativa que impide una visión sistémica sobre el impacto de la IA en los derechos fundamentales. Mientras los proyectos sobre IA no incorporan exigencias de protección de datos, el proyecto de reforma de la Ley 25.326 incluye menciones relevantes sobre IA, pero sin integrar un régimen específico que contemple su complejidad técnica y regulatoria.

Tampoco se han presentado hasta la fecha proyectos que contemplen de manera articulada la creación de una autoridad especializada en IA, la clasificación de sistemas por niveles de riesgo, o la exigencia de registros públicos de algoritmos como propone el

Reglamento de IA europeo. Este vacío normativo representa una oportunidad, aún desaprovechada, para diseñar un esquema de gobernanza que combine innovación tecnológica con garantías efectivas de protección de derechos.

En suma, la revisión de los proyectos legislativos presentados en Argentina hasta septiembre de 2024 muestra un escenario normativo disperso, con avances desiguales y sin un abordaje integral del tratamiento automatizado de datos personales mediante inteligencia artificial. La ausencia de articulación entre los proyectos de regulación general de IA y la reforma de la Ley de Protección de Datos Personales pone en evidencia la necesidad urgente de construir un marco normativo coordinado, técnicamente informado y alineado con los estándares internacionales, pero adaptado a la realidad institucional y tecnológica del país.

3.3.2. Propuesta normativa para una regulación efectiva del tratamiento automatizado de datos personales

El análisis comparado de los marcos regulatorios de protección de datos vinculados al uso de inteligencia artificial demuestra la urgencia de actualizar el marco normativo argentino. La Ley 25.326, concebida en un entorno analógico, no ofrece respuestas adecuadas a los desafíos que plantea el tratamiento automatizado de datos personales en contextos cada vez más complejos y digitalizados. La falta de mecanismos específicos para regular la toma de decisiones algorítmicas, la escasa exigencia de transparencia y la debilidad institucional de los organismos de control conforman un escenario de alta vulnerabilidad para los derechos individuales.

El Reglamento General de Protección de Datos (RGPD) de la Unión Europea, al efectivizar que la protección de datos se refleje en la categoría de derecho fundamental ofrece una estructura normativa robusta que impone a los responsables del tratamiento obligaciones claras, como la realización de evaluaciones de impacto, la adopción de principios como la privacidad desde el diseño y la obligación de explicabilidad en decisiones automatizadas. Estos mecanismos no solo anticipan posibles afectaciones a los derechos, sino que promueven un modelo de responsabilidad activa y de rendición de cuentas por parte de quienes desarrollan y operan sistemas de inteligencia artificial.

Brasil, mediante su Ley General de Protección de Datos (LGPD), ha adaptado muchas de estas exigencias al contexto latinoamericano. La posibilidad de intervención humana en decisiones automatizadas, el consentimiento granular y la creación de una

Autoridad Nacional de Protección de Datos (ANPD) que fiscaliza y sanciona incumplimientos normativos, constituyen avances significativos. En contraste, Argentina aún carece de estas figuras clave, lo que limita la efectividad del control institucional sobre el uso de IA.

En el caso de Estados Unidos, el enfoque sectorial y descentralizado genera importantes asimetrías en la protección de datos. No obstante, la reciente aprobación de la Ley de Inteligencia Artificial del Estado de Colorado en 2024 representa un avance considerable, al establecer criterios de evaluación de impacto, transparencia y supervisión para sistemas de alto riesgo. Este modelo ofrece una alternativa regulatoria progresiva que Argentina podría considerar, permitiendo una regulación más ágil en sectores clave como salud, educación, seguridad y justicia, sin depender exclusivamente de una ley general.

Por su parte, la Opinión 28/2024 del Comité Europeo de Protección de Datos (EDPB) enfatiza que el tratamiento de datos mediante IA requiere salvaguardas específicas, incluyendo la supervisión humana efectiva, la explicación accesible de decisiones automatizadas, el respeto al principio de minimización de datos y la existencia de mecanismos para impugnar decisiones. Estas recomendaciones resultan especialmente pertinentes para el diseño de una nueva legislación argentina, en la medida en que permiten armonizar el desarrollo tecnológico con los estándares internacionales de derechos humanos.

A su vez, la doctrina de Lothar Determann sostiene que la protección de datos no debe limitarse a prevenir filtraciones, sino que debe concebirse como un resguardo estructural frente a poderes públicos y privados capaces de ejercer formas de vigilancia algorítmica a gran escala. En esa línea, sugiere que el derecho debe ser proactivo, anticipando riesgos y garantizando que la innovación no se imponga a expensas de la dignidad humana. Esta visión se complementa con los aportes del documento “El derecho de protección de datos personales en tiempos de IA” (2022), que advierte que, en la era digital, los esfuerzos estatales tienden a diluirse si no se construyen normativas propias con base en la realidad local, sin caer en la reproducción acrítica de modelos extranjeros.

Frente a este panorama, Argentina podría avanzar hacia una arquitectura regulatoria que contemple, entre otras medidas, la exigencia de evaluaciones de impacto en la privacidad como requisito previo a la implementación de sistemas automatizados,

así como la creación de un registro público y obligatorio de algoritmos de alto riesgo. Este registro, administrado por la Agencia de Acceso a la Información Pública (AAIP), no pretende reemplazar el actual trámite de registro de bases de datos previsto en la Ley 25.326, sino complementarlo mediante una herramienta más idónea para supervisar tecnologías complejas. Su finalidad sería permitir la trazabilidad, transparencia y control público de los sistemas algorítmicos que toman decisiones con impacto significativo sobre derechos individuales.

Esta propuesta encuentra sustento en experiencias regulatorias internacionales como el Reglamento de IA europeo, que obliga a los desarrolladores de sistemas de IA de alto riesgo a registrarlos en una base centralizada, accesible y supervisada por autoridades nacionales, con el objetivo de garantizar estándares de transparencia, supervisión técnica y rendición de cuentas. En esa línea, también la Ley de Inteligencia Artificial del Estado de Colorado (2024) establece que las entidades que implementen algoritmos de alto impacto deben documentar sus funcionalidades, objetivos y metodologías, e informar públicamente sobre su uso.

Contar con un registro de este tipo permitiría no solo a la AAIP, sino también a investigadores, periodistas, organismos de control y la ciudadanía en general, acceder a información clave sobre qué sistemas se utilizan, con qué fines y bajo qué criterios. Este enfoque no solo mejora la capacidad institucional de auditoría, sino que habilita un control democrático del poder algorítmico, permitiendo prevenir abusos y fomentar la confianza pública en la tecnología. La existencia de este registro facilitaría, además, la detección temprana de sesgos, errores o impactos desproporcionados, contribuyendo a una regulación más dinámica, preventiva y técnicamente informada.

El camino hacia una regulación efectiva en Argentina requiere, por tanto, algo más que una modernización técnica del marco normativo: exige una redefinición del rol del derecho como límite, guía y garantía frente al poder algorítmico. Regular la inteligencia artificial no implica frenar el desarrollo, sino asegurar que ese desarrollo se inscriba en valores democráticos, respete la dignidad humana y fortalezca los derechos fundamentales. La protección de los datos personales debe concebirse como un derecho habilitante que permite el ejercicio de otros derechos, y no como un obstáculo a la innovación. En definitiva, se trata de construir un modelo de gobernanza tecnológica que

no quede capturado por lógicas opacas, sino que esté orientado al servicio de las personas y del interés público.

En este sentido, cabe preguntarse si los proyectos de ley sobre inteligencia artificial actualmente en debate en el Congreso argentino recogen estas exigencias. Si bien inicialmente se destacaban las iniciativas legislativas del senador Mariano Recalde y la diputada Graciela Caamaño, una revisión actualizada de los registros del Honorable Congreso de la Nación revela al menos ocho proyectos relevantes que abordan, desde distintos enfoques, aspectos vinculados al desarrollo y la regulación de la inteligencia artificial. Entre ellos se encuentran el Expediente 3003-D-2024 (Juan Brügge), que establece principios para el uso responsable de IA; el 6156-D-2024 (Micaela Morán), que propone un Registro Nacional de Sistemas de IA; el 3900-D-2024 (Silvana Ginocchio), que impulsa un Observatorio Federal de IA; el 1937-D-2025 (Gabriel Chumpitaz), que propone la creación de un Ministerio de Inteligencia Artificial; el 2130-D-2025 (Daniel Gollán), que incorpora modificaciones normativas de alcance transversal; el 0120-D-2024 (Eduardo Fernández), que propone una ley marco para regular el desarrollo y uso ético de la IA; y el 2139-S-2023 (Graciela Caamaño), orientado a principios generales y derechos frente a sistemas inteligentes. Asimismo, debe destacarse el proyecto 2363-S-2023 (Mariano Recalde), que busca incorporar derechos digitales y establece lineamientos para la supervisión algorítmica. Aunque estos proyectos no recogen de forma integral todos los recaudos propuestos por los estándares internacionales como evaluaciones de impacto en la privacidad, explicabilidad algorítmica, o la creación de registros públicos obligatorios— evidencian un creciente interés parlamentario por abordar estas temáticas. En conjunto, constituyen un punto de partida que podría enriquecerse mediante la articulación de sus propuestas hacia un modelo coherente y robusto de regulación.

En conjunto, constituyen un punto de partida que podría enriquecerse mediante la articulación de sus propuestas hacia un modelo coherente y robusto de regulación.

Finalmente, cabe aclarar que, además de los proyectos mencionados, existen otras iniciativas con estado parlamentario que abordan aspectos específicos vinculados al desarrollo o uso de la inteligencia artificial. Entre ellas se encuentran los expedientes 4436-D-2023, 2505-D-2023, 1472-D-2023, 3422-D-2024, 0805-D-2024, S-1747-2023, S-1368-2024 y S-0992-2024, entre otros. Si bien estas propuestas no son analizadas en

detalle en el presente apartado, han sido consideradas en el cuadro comparativo incluido en este capítulo, a fin de ofrecer una visión integral del estado actual del debate legislativo en la materia.

CAPÍTULO 4: CASOS PRÁCTICOS Y ANÁLISIS DE RIESGOS

4.1. Casos relevantes en Argentina

En el contexto argentino, la irrupción de tecnologías basadas en inteligencia artificial para el tratamiento de datos personales ha puesto en evidencia una preocupante brecha entre el desarrollo técnico y la regulación jurídica. Los casos que se presentan no solo revelan vacíos normativos, sino también la urgencia de una respuesta estatal adecuada frente a los riesgos que estas tecnologías suponen para los derechos fundamentales.

Uno de los ejemplos más paradigmáticos es el sistema de reconocimiento facial implementado por el Gobierno de la Ciudad Autónoma de Buenos Aires. La herramienta, ideada inicialmente para detectar personas con pedidos de captura judicial, terminó recolectando datos biométricos de millones de ciudadanos sin el debido resguardo normativo ni control judicial. La justicia federal ordenó su suspensión, alegando la falta de proporcionalidad, transparencia y supervisión.

Este caso motivó una acción de amparo impulsada por el Observatorio de Derecho Informático Argentino (O.D.I.A.), en la que se cuestionó la constitucionalidad del sistema y se denunció la captura masiva de datos sensibles sin consentimiento ni garantías adecuadas. En el fallo *O.D.I.A. c/ GCBA s/ amparo*, dictado por la Cámara de Apelaciones en lo Contencioso, Administrativo y Tributario de la Ciudad de Buenos Aires (Sala I), el tribunal resolvió a favor de la demanda, destacando la ausencia de una evaluación de impacto en la protección de datos personales y la falta de transparencia respecto del funcionamiento del sistema y sus algoritmos. Este pronunciamiento judicial no solo marcó un precedente clave en materia de protección de datos biométricos, sino que puso de relieve la necesidad urgente de regular la transparencia algorítmica y garantizar el control humano significativo sobre decisiones automatizadas. En este sentido, se trata de un fallo paradigmático que demuestra que, sin un marco legal robusto, la inteligencia artificial puede vulnerar derechos fundamentales de manera masiva, silenciosa y difícilmente reparable (Cámara de Apelaciones en lo Contencioso, Administrativo y Tributario de la CABA, 2021).

Tal como se sostiene en la doctrina, “hoy día, la IA permite en algunos casos hacer tratamiento de datos legales pero poco éticos... este consentimiento no es verdaderamente informado” (Delgado Espinal & Espinoza Suárez, 2024), lo que refuerza la necesidad de avanzar hacia un nuevo modelo de regulación más exigente y preventivo. Otro caso que provocó un fuerte debate ético y jurídico fue el uso de IA generativa para replicar la voz y la imagen de la actriz Silvina Luna tras su fallecimiento. Este chatbot interactuaba con usuarios utilizando su identidad digital sin el consentimiento de sus familiares ni un marco normativo claro que regulara este tipo de simulaciones post mortem. El caso evidenció la falta de protección de los derechos personalísimos en entornos digitales, tales como el derecho a la propia imagen, a la voz y a la memoria, incluso después de la muerte. En ausencia de legislación específica, estos desarrollos tecnológicos se encuentran en una “zona gris” legal que requiere atención inmediata.

Asimismo, se han documentado situaciones de sesgos algorítmicos en procesos de selección laboral, segmentación de clientes y concesión de créditos, donde ciertos algoritmos reproducen e incluso amplifican prejuicios preexistentes. Estos sistemas, entrenados con datos históricos marcados por desigualdades de género, raza o condición socioeconómica, terminan tomando decisiones que refuerzan estructuras de exclusión. En palabras de Barona Vilar (2021), “el algoritmo hereda y amplifica los sesgos de los datos, replicando estructuras de exclusión que el derecho debería corregir, no legitimar” (p. 13).

Estos casos no constituyen hechos aislados, sino síntomas de un problema estructural: el desfase entre la velocidad del avance tecnológico y la capacidad del derecho argentino para ofrecer respuestas eficaces, preventivas y garantistas. La IA, sin regulación, puede transformarse en una herramienta que erosiona derechos en lugar de ampliarlos. El desafío no radica en rechazar la innovación, sino en diseñar marcos institucionales capaces de gobernarla con criterios democráticos y respetuosos de la dignidad humana.

4.2. Riesgos para los derechos individuales

El despliegue de sistemas de inteligencia artificial para el tratamiento de datos personales implica una serie de riesgos profundos para los derechos individuales. Estos no son meras conjeturas teóricas, sino consecuencias palpables que afectan la vida cotidiana de las personas y que, en muchos casos, vulneran principios constitucionales básicos.

Uno de los riesgos más significativos es el de la opacidad algorítmica. Numerosos sistemas de IA funcionan como "cajas negras", en las que ni los propios desarrolladores pueden explicar con precisión cómo se toman las decisiones. Esta opacidad vulnera el principio de rendición de cuentas y dificulta el ejercicio efectivo de derechos como el acceso a la información, la rectificación o la impugnación de decisiones automatizadas. Según Barona Vilar (2021), "frente a la complejidad de los sistemas de IA, el Derecho debe volver a ser principio activo de garantía, no mera norma reactiva" (p. 15).

Otro riesgo central es la reproducción y amplificación de sesgos estructurales. La IA, lejos de ser neutral, aprende de los datos que le son proporcionados, los cuales muchas veces reflejan desigualdades preexistentes. En consecuencia, puede replicar y reforzar prejuicios de género, etnia, edad o nivel socioeconómico. Esto no solo afecta la igualdad de oportunidades, sino que perpetúa patrones de discriminación que el derecho debería precisamente erradicar.

La recopilación masiva e indiscriminada de datos personales también representa una amenaza directa a la privacidad y a la autodeterminación informativa. La arquitectura misma de la IA requiere grandes volúmenes de datos, lo que tensiona principios legales como la minimización de datos o la limitación de la finalidad. En este contexto, los derechos ARCO (acceso, rectificación, cancelación y oposición) muchas veces resultan ineficaces ante la complejidad de los sistemas automatizados. Como advierten Delgado Espinal y Espinoza Suarez (2024), "uno de los mayores desafíos que presenta la inteligencia artificial no es solo técnico, sino democrático: su capacidad para predecir y manipular el comportamiento individual en función de datos masivos puede afectar el libre desarrollo de la personalidad" (p. 11142).

Estos riesgos no solo comprometen derechos individuales como la intimidad, la identidad o la libertad de expresión, sino que pueden tener efectos más amplios sobre la salud mental, la participación política y la confianza social. Sin mecanismos de control claros, la inteligencia artificial corre el riesgo de socavar las bases mismas del contrato social y de erosionar la autonomía ciudadana.

4.3. Soluciones tecnológicas y jurídicas

Frente a este escenario, resulta imprescindible promover un enfoque integral que combine herramientas tecnológicas con soluciones jurídicas robustas. La autorregulación tecnológica ha demostrado ser insuficiente, y el derecho debe asumir un rol proactivo que

anticipe, oriente y limite el despliegue de sistemas de IA en función de los derechos fundamentales.

Desde lo técnico, una primera medida es fomentar el uso de tecnologías de protección de la privacidad como la anonimización, la seudonimización y los sistemas de inteligencia artificial explicable (XAI), que permiten entender, auditar y corregir los procesos automatizados. También resulta clave implementar evaluaciones de impacto en la privacidad (Privacy Impact Assessments) antes del desarrollo o adquisición de sistemas de IA, especialmente en el sector público.

Desde el punto de vista jurídico, es urgente una reforma normativa que contemple específicamente el uso de IA en el tratamiento de datos personales. Esta actualización debería incluir el derecho a la información, el derecho a la revisión humana, y el derecho a conocer la lógica del algoritmo que haya intervenido en una decisión significativa. La creación de un registro público de algoritmos utilizados por el Estado también podría contribuir a mejorar la transparencia.

Además, deberían institucionalizarse comités éticos interdisciplinarios que intervengan en el diseño, implementación y control de sistemas automatizados, especialmente en áreas sensibles como salud, justicia o educación. Estos comités pueden garantizar una perspectiva integral, que combine criterios jurídicos, técnicos, éticos y sociales.

Por último, es indispensable promover una educación crítica en torno a la IA, tanto en carreras técnicas como jurídicas. Solo con una ciudadanía informada, un ecosistema institucional sólido y una normativa clara será posible garantizar que el desarrollo de la inteligencia artificial esté al servicio de una sociedad más democrática, inclusiva y respetuosa de los derechos humanos.

4.4. Transformación del marketing digital y la publicidad ante la irrupción de la inteligencia artificial

La irrupción de la inteligencia artificial también ha provocado una transformación profunda en el ecosistema del marketing digital y la publicidad en línea. Herramientas como los motores de búsqueda potenciados por IA generativa están alterando el modo en que las personas acceden a la información, lo que impacta directamente en la arquitectura tradicional de la publicidad basada en buscadores y datos de comportamiento.

El modelo clásico, centrado en motores como Google y basado en estrategias de posicionamiento (Search Engine Optimization o SEO), apuntaba a optimizar el contenido de los sitios web para que aparezcan en los primeros resultados de búsqueda orgánica. Esta lógica implicaba el uso de palabras clave, estructuras técnicas específicas y vínculos internos que buscaban captar el interés del algoritmo del buscador y, así, atraer mayor tráfico de usuarios. Sin embargo, este modelo se ve desplazado por asistentes conversacionales basados en IA generativa que sintetizan información directamente en sus respuestas, reduciendo el número de clics hacia sitios tradicionales y alterando profundamente las métricas clave de visibilidad digital (Swant, 2025). Esta transformación sugiere que, a futuro, los asistentes con IA podrían convertirse en los nuevos intermediarios clave del ecosistema publicitario digital, desplazando el rol dominante que tuvo Google durante dos décadas.

En consecuencia, el rediseño de la publicidad digital mediada por inteligencia artificial exige un replanteo integral de la arquitectura regulatoria, tanto en materia de protección de datos personales como en lo relativo al derecho del consumidor y a la propiedad intelectual. Para el caso argentino, este nuevo escenario impone el desafío de incorporar principios como la explicabilidad algorítmica, la transparencia publicitaria y el consentimiento explícito, dentro de un entorno digital donde los sistemas de recomendación ya moldean la economía de la atención, el comportamiento de consumo y la configuración de preferencias sociales. En definitiva, no se trata solo de nuevas tecnologías, sino de nuevas lógicas de poder que requieren marcos normativos acordes a su impacto.

Además, la utilización de prompts que pueden incluir nombres de productos, marcas o servicios dentro de las consultas conversacionales plantea nuevos desafíos respecto a los datos utilizados en el entrenamiento de los modelos y la eventual aparición de resultados asociados a determinadas marcas sin control comercial o consentimiento (Anconitano & Vitari, 2025). Estas asociaciones, aunque no siempre intencionales, pueden tener consecuencias tanto desde el punto de vista reputacional como legal, especialmente en lo relativo a la protección marcaria, el uso no autorizado de signos distintivos y la competencia desleal.

Desde la perspectiva de los datos personales, estas transformaciones intensifican el problema de la trazabilidad y del consentimiento informado. Los nuevos modelos

publicitarios se nutren de perfiles cada vez más detallados, generados mediante inferencias automatizadas, lo que dificulta aún más el control del usuario sobre su información personal. Como afirman Delgado Espinal y Espinoza Suárez (2024), el cambio no es sólo técnico, sino político: “la IA permite modelar el deseo y orientar la atención, con impactos profundos en la autonomía individual” (p. 11143).

A su vez, los algoritmos de recomendación potenciados por IA, optimizados para maximizar clics y tiempo de permanencia, pueden derivar en burbujas informativas, polarización o amplificación de desinformación, especialmente si no se implementan salvaguardas éticas y regulatorias. Estos riesgos, aunque usualmente abordados desde la ética de la comunicación, tienen derivaciones directas en términos de derechos del consumidor y derecho a la información veraz.

En este contexto, también surgen nuevos debates sobre el uso de datos protegidos por derechos de autor para entrenar modelos de inteligencia artificial. Un fallo reciente en los Estados Unidos, emitido por el juez William Alsup en 2024, marcó un hito al distinguir entre el uso legítimo de obras para entrenar modelos, bajo la doctrina del fair use, y la obtención ilícita de esas obras, como sucedió con la incorporación de millones de libros pirateados por la empresa Anthropic. El tribunal sostuvo que el uso transformador puede estar permitido, pero el acceso no autorizado a los contenidos originales constituye una violación legal independiente (Alsup, 2024).

Esta tensión entre innovación tecnológica y protección de los derechos de autor ha seguido desarrollándose en la justicia estadounidense. En 2025, el mismo tribunal (United States District Court, Northern District of California) analizó el caso Bartz, Graeber y Johnson v. Anthropic PBC (No. C 24-05417 WHA), donde se volvió a discutir si entrenar modelos de IA con obras protegidas por copyright constituye un uso justo. El juez Alsup sostuvo que el entrenamiento podría considerarse transformador, y por ende uso justo, si el modelo no replica ni suplanta los textos originales, sino que crea algo nuevo: “like any reader aspiring to be a writer, Anthropic's LLMs trained upon works not to race ahead and replicate or supplant them – but to turn a hard corner and create something different” (United States District Court, 2025, p. 9). Sin embargo, el fallo también advirtió que la adquisición no autorizada de más de siete millones de libros

pirateados no puede considerarse legítima, y esa parte fue enviada a juicio para la eventual determinación de daños por hasta USD 150.000 por obra.

Poco tiempo después, en el caso Kadrey et al. v. Meta Platforms, Inc., el juez Vince Chhabria adoptó una postura convergente. Si bien también se trataba del uso de obras literarias protegidas para entrenar un modelo de lenguaje (LLaMA), el tribunal entendió que no se había demostrado un perjuicio económico concreto para los autores y que el entrenamiento podía considerarse un uso transformador, siempre que no reprodujera ni sustituyera el contenido original. Aunque Meta también habría utilizado libros extraídos de bases pirateadas, el tribunal no avanzó en sanciones, al considerar que no se había probado un daño directo.

Estos precedentes, aunque favorables a las empresas tecnológicas en algunos aspectos, reafirman la necesidad urgente de contar con marcos normativos claros sobre el uso de obras protegidas en el entrenamiento de sistemas de inteligencia artificial. Para países como Argentina, donde aún no existe regulación específica sobre esta materia, los casos de Anthropic y Meta funcionan como advertencias sobre la importancia de regular no solo el uso de los datos, sino también su forma de adquisición, almacenamiento y tratamiento, en equilibrio con los derechos de autores y titulares de propiedad intelectual.

En definitiva, los casos analizados en este capítulo evidencian que el impacto de la inteligencia artificial sobre la privacidad no es meramente abstracto o teórico, sino que se manifiesta en prácticas concretas que afectan derechos fundamentales en ámbitos sensibles como el marketing, la publicidad, la gestión pública o el sector laboral. La falta de previsión normativa frente a estas transformaciones incrementa los riesgos de opacidad, discriminación y vulneración de derechos. Esta situación exige pasar del diagnóstico al diseño de herramientas jurídicas efectivas que, sin frenar el desarrollo tecnológico, aseguren una protección adecuada de los datos personales en el contexto argentino. A continuación, se presentan propuestas de reforma normativa orientadas a construir un marco legal más robusto, moderno y coherente con los desafíos que plantea el tratamiento automatizado de datos mediante inteligencia artificial.

CAPÍTULO 5: PROPUESTAS DE REFORMA PARA LA LEGISLACIÓN ARGENTINA

La irrupción de la inteligencia artificial en múltiples esferas de la vida social, económica y estatal impone un replanteo profundo del marco normativo vigente en Argentina. La Ley 25.326, aunque pionera en la región, ya no logra abarcar los desafíos concretos que plantea el procesamiento masivo y automatizado de datos personales, ni establece directrices suficientes frente al uso de algoritmos opacos y sistemas de toma de decisiones automatizada. Esta situación deja a los titulares de datos en una posición vulnerable y al Estado con herramientas limitadas para ejercer un control efectivo.

Lejos de limitarse a una simple actualización técnica, las reformas necesarias deben apuntar a construir una arquitectura jurídica integral, con foco en la transparencia, la supervisión, la equidad y la protección efectiva de los derechos fundamentales en un entorno digital cada vez más complejo. Como sostiene Baca Rivero (2021), implementar algoritmos que "incorporen por diseño los principios de privacidad y transparencia permitiría garantizar el tratamiento legítimo de los datos personales sin necesidad de limitar el desarrollo tecnológico" (p. 87).

5.1. Recomendaciones normativas

Una primera línea de acción consiste en reformar la Ley 25.326 para incorporar definiciones modernas sobre algoritmos, tratamiento automatizado, decisiones significativas y sistemas de alto riesgo. La inclusión de principios como la minimización de datos, la limitación del propósito, la responsabilidad algorítmica y la explicabilidad ya no puede postergarse. Asimismo, se debería exigir, como plantea el Reglamento de IA europeo, que todo sistema de IA en sectores críticos esté sometido a una evaluación de impacto en la privacidad (EIP) previa a su implementación, asegurando así una protección preventiva de los derechos individuales.

Inspirándose en modelos como el registro de sistemas de IA de alto riesgo promovido por la Unión Europea, Argentina podría desarrollar su propio Registro Nacional de IA, supervisado por una Agencia de Acceso a la Información Pública (AAIP) fortalecida técnica, financiera y jurídicamente. Esta institución debería tener la facultad de auditar algoritmos, aplicar sanciones efectivas y emitir lineamientos técnicos obligatorios para las entidades que utilicen inteligencia artificial.

En paralelo, puede contemplarse una regulación sectorial gradual, comenzando por ámbitos como la salud, la seguridad, el crédito o el empleo público, donde el uso de IA ya es una realidad. Este enfoque flexible, influenciado por la experiencia de la Ley de Colorado, permite adecuar la intensidad regulatoria al nivel de riesgo de cada caso, sin frenar la innovación en áreas de menor sensibilidad.

5.2. Derechos de los titulares de los datos

En un contexto donde las decisiones automatizadas pueden incidir profundamente en la vida cotidiana de las personas, no alcanza con que dichas decisiones sean técnicamente correctas: también deben ser comprensibles. Uno de los principios fundamentales que deben guiar el diseño y la regulación de los sistemas de inteligencia artificial es la explicabilidad, entendida, siguiendo la definición propuesta en el Proyecto de Ley 3540-D-2025, como la capacidad de un sistema automatizado para ofrecer información comprensible, verificable y significativa sobre su funcionamiento, su lógica interna y los criterios utilizados para generar resultados o decisiones. Este concepto se distingue de la interpretabilidad, que alude a la comprensión técnica del modelo por parte de especialistas, abordando su estructura, parámetros y procesos internos, pero sin garantizar necesariamente que un usuario no técnico pueda entender las razones de una decisión concreta. Tanto el Reglamento de IA de la Unión Europea como las Directrices de la OCDE sobre Inteligencia Artificial subrayan la importancia de que los sistemas algorítmicos operen de manera transparente y bajo supervisión humana significativa, permitiendo a los individuos entender, cuestionar y, en su caso, oponerse a decisiones automatizadas que los afecten. Esta accesibilidad del conocimiento técnico es clave para que los derechos de las personas puedan ser ejercidos en la práctica, y no queden relegados a una protección meramente formal (OCDE, 2019; Parlamento Europeo y Consejo, 2024).

En esta misma línea, el Proyecto de Ley impulsado por la diputada Silvana Giudici en 2025 propone reformar la Ley 25.326 de Protección de Datos Personales para incorporar principios de transparencia algorítmica, derecho a la explicación, mecanismos de auditoría y revisión humana sustantiva en los procesos automatizados que produzcan efectos jurídicos o impactos significativos en la vida de las personas. La iniciativa establece, entre otros puntos, la obligación de que el diseño de estos sistemas contemple criterios de comprensibilidad, trazabilidad y robustez desde su concepción, así como la

posibilidad de auditorías técnicas y éticas independientes. Esta propuesta refleja una tendencia global a fortalecer la tutela de los derechos de los titulares de datos frente a sistemas automatizados opacos, asegurando que la innovación tecnológica se desarrolle dentro de un marco que combine eficacia con respeto irrestricto por los derechos fundamentales.

La actualización del marco legal debe ir de la mano con un robustecimiento de los derechos de las personas frente a las nuevas formas de tratamiento automatizado. El derecho a la explicación resulta central: toda persona debe saber si una decisión que la afecta fue tomada por una máquina, cómo opera el algoritmo en cuestión y qué criterios fueron aplicados. Este derecho, que el RGPD europeo ya contempla, debe ser incorporado expresamente en la legislación argentina.

Junto con ello, debe garantizarse el derecho a la intervención humana en aquellas decisiones automatizadas que tengan un impacto significativo sobre la vida de los ciudadanos. Esta revisión debe ser efectiva y no meramente formal, evitando que las decisiones algorítmicas se transformen en mecanismos de exclusión sin posibilidad de defensa.

Otra garantía fundamental es el derecho a no ser perfilado injustamente. Los sistemas de IA no pueden utilizar inferencias automatizadas para discriminar o excluir a personas sin que exista una base legal clara ni la posibilidad de control humano. Como destaca Bonilla Gutiérrez (2024), la autodeterminación informativa exige actualizar sus mecanismos frente a la lógica opaca de los sistemas automatizados, que erosionan la capacidad de los individuos para ejercer control real sobre sus datos.

Estas propuestas se enmarcan en la necesidad de pensar nuevas modalidades del derecho a la protección de datos, como el derecho a no ser identificado, a no ser perfilado automáticamente y a reclamar contra decisiones automatizadas, tal como proponen autores como Barona Vilar (2021) y Delgado Espinal y Espinoza Suarez (2024).

5.3. Implicaciones éticas y sociales

La regulación no puede centrarse solo en lo jurídico. Debe incorporar una mirada ética y social sobre los impactos de la inteligencia artificial. Como bien señala Barona Vilar (2021), “frente a la complejidad de los sistemas de IA, el Derecho debe volver a ser

principio activo de garantía, no mera norma reactiva" (p. 15). La regulación anticipatoria es hoy una exigencia democrática y no una opción.

La proliferación de tecnologías de vigilancia masiva, el uso de algoritmos en el sector público sin control social, y la concentración de poder informacional en pocas manos obligan a abrir el debate sobre qué tipo de sociedad queremos construir. La legislación debe promover la transparencia tecnológica, exigir una rendición de cuentas adecuada y garantizar que el desarrollo de IA esté guiado por criterios de equidad, inclusión y justicia.

En esta línea, se propone crear comités éticos interdisciplinarios, con participación de juristas, científicos, académicos y representantes de la sociedad civil, que evalúen el impacto social y cultural de cada implementación de IA. Además, sería deseable que Argentina lidere un espacio de articulación regional para desarrollar un modelo latinoamericano de gobernanza algorítmica, respetuoso de los derechos humanos y sensible a las realidades sociales y económicas de la región.

CONCLUSIONES

La inteligencia artificial ha transformado el tratamiento de los datos personales de manera estructural. Estas tecnologías, lejos de ser meras herramientas de eficiencia, han modificado estructuralmente la relación entre las personas, el Estado y el mercado, instalando nuevos dilemas éticos y jurídicos que desafían la capacidad del derecho para proteger los derechos fundamentales en entornos altamente automatizados.

Ya no se trata solo de almacenar información, sino de predecir, clasificar, decidir y hasta intervenir sobre las personas en función de esos datos, muchas veces sin que ellas lo sepan, sin que puedan objetarlo ni comprender el proceso. Esta lógica algorítmica, que actúa con velocidad y alcance global, desafía los principios clásicos del derecho, especialmente en materia de privacidad, debido proceso y autonomía.

Argentina, con su Ley 25.326, fue pionera en América Latina en establecer un marco de protección de datos personales. Sin embargo, este cuerpo normativo, concebido en una era pre-digital, no contempla la complejidad de los procesos actuales de tratamiento algorítmico, ni los impactos que estos tienen sobre la intimidad, la autonomía y la equidad social. Como sostiene Daniel Monastersky (2019), esta ley fue pensada en

un contexto analógico, y hoy resulta estructuralmente insuficiente para contener los riesgos del ecosistema digital actual.

Al igual que otros países, Argentina, se encuentra ante el desafío urgente de revisar su marco normativo en materia de protección de datos personales. Sin embargo, la urgencia no debe confundirse con precipitación. Regular la inteligencia artificial no puede ser un acto reflejo, ni una carrera por demostrar modernidad, porque el riesgo es terminar construyendo un derecho que aparenta control, pero que no garantiza justicia, ya que la inteligencia artificial, al operar sobre grandes volúmenes de datos, puede no solo reproducir desigualdades, sino consolidarlas bajo una apariencia de neutralidad algorítmica.

Los modelos internacionales ya sea la rigidez del sistema europeo o la flexibilidad fragmentada de Estados Unidos muestran que no hay soluciones universales. Detrás de cada sistema jurídico hay una historia, una cultura política y una visión del poder, que define cómo se ponderan la intimidad, la seguridad, la innovación y los derechos colectivos. Como señala Lothar Determann, la privacidad no se protege del mismo modo cuando se la concibe como un derecho fundamental que cuando se la subordina a la libertad de empresa o a la seguridad nacional.

Frente a esta encrucijada, el derecho argentino no puede limitarse a importar modelos ajenos sin una mirada crítica. Debe construirse desde sus propias bases constitucionales, reconociendo la centralidad de los derechos humanos y la necesidad de asegurar condiciones de equidad tecnológica en una sociedad atravesada por desigualdades estructurales. Como sostienen diversos autores, la regulación debe incluir principios como el de justicia algorítmica, la prevención del sesgo y la participación ciudadana en el diseño de las políticas digitales (Barona Vilar, 2021; Bonilla Gutiérrez, 2024).

Por eso, esta tesis sostiene que la respuesta no está solo en actualizar una ley, sino en repensar el lugar del derecho en un ecosistema gobernado por el dato. Un derecho que acompañe el desarrollo tecnológico sin quedar atrapado por sus lógicas. Un derecho que no sea meramente reactivo, sino que se atreva a anticipar, a poner límites razonables, y a garantizar que el progreso no sea a costa de la dignidad humana.

Porque regular no es solo redactar leyes: es decidir qué valores queremos proteger en un mundo cada vez más automatizado. Y si hay algo que la inteligencia artificial aún

no puede reemplazar, es nuestra capacidad de deliberar, de responsabilizarnos y de defender el derecho a seguir siendo personas, no simplemente perfiles.

En este contexto, la hipótesis de esta tesis se confirma: la Ley 25.326, en su estado actual, no resulta adecuada para enfrentar los riesgos que plantea la inteligencia artificial en el tratamiento de datos personales. La actualización del marco normativo no puede seguir postergándose. Es necesario incorporar principios como la privacidad desde el diseño, la rendición de cuentas algorítmica, la intervención humana efectiva, el derecho a la explicación y evaluaciones de impacto como condiciones mínimas para la legitimidad del tratamiento automatizado de datos.

Pero además del cambio normativo, resulta indispensable repensar la concepción misma del derecho a la privacidad. Como plantea Bonilla Gutiérrez (2024), la autodeterminación informativa debe actualizarse para proteger al individuo en un ecosistema de vigilancia algorítmica que amenaza con diluir el control personal sobre los datos. El consentimiento formal, aislado de un verdadero control, ya no alcanza. La regulación debe asegurar no solo la legalidad, sino también la justicia del uso de los datos personales.

A pesar de la globalidad de Internet y la concentración de poder en grandes corporaciones transnacionales, la regulación local sigue siendo fundamental. No se trata de renunciar a la cooperación internacional, sino de construir normas propias, sensibles a la cultura jurídica, institucional y económica del país, que permitan ejercer soberanía digital y proteger a los ciudadanos con herramientas adecuadas. Como bien advierte Determann (2017), no existe un único modelo posible, y la eficacia de la protección de datos depende de cómo se articula la privacidad con otros valores sociales, como la seguridad, la innovación o la libertad.

Regular la inteligencia artificial no es una cuestión del futuro, sino una necesidad urgente del presente. No se trata de frenar el progreso, sino de garantizar que el desarrollo tecnológico se inscriba en un marco democrático, donde la persona humana siga siendo el centro, y no un dato más dentro de una cadena de procesamiento.

Por todo esto, la reforma de la legislación argentina debe ir más allá de un ajuste técnico. Debe constituir una apuesta política, ética y jurídica por un modelo de inteligencia artificial al servicio de la dignidad humana, capaz de generar confianza, proteger derechos y fomentar una innovación responsable, inclusiva y justa.

ANEXO A

Número de expediente	Título o temática principal	Autor/a	Camara de origen	Contempla evaluación impacto	Contempla registro público	Contempla explicabilidad	Contempla autoridad control especializada	Otros elementos relevantes
4079-D-2024	Presupuestos Mínimos para la Promoción del Desarrollo de la Inteligencia Artificial en la República Argentina	Silvana Giudici & co-firmantes (PRO)	Diputados	No	Sí (definido)	Sí	Consejo Jefatura de Gabinete de Ministros	Principios, etiqueta para contenido realista
3900-D-2024	Creación del Observatorio Federal de Inteligencia Artificial	Silvia Ginocchi (Unión por la Patria)	Diputados	No	No	No	Sí (Observatorio)	Informe público y coordinación HCDN-HSN
3003-D-2024	Régimen Jurídico Aplicable para el Uso Responsable de la Inteligencia Artificial en Argentina	Juan Brügge (Demócrata Cristiano)	Diputados	Sí	Sí	Sí	Instituto Nacional de Tecnología Industrial	Sanciones, trazabilidad, certificación
4436-D-2023	Imágenes Sexuales de Menores Elaboradas mediante Sistemas de IA (modificación artículo 128 CP)	Silvia Ginocchi (Unión por la Patria)	Diputados	No	No	No	Modificación Código Penal	Regula penalmente el uso de IA para generar imágenes sexuales falsas de menores (deepfakes), a través de la modificación del artículo 128 del Código Penal. Enfoque penal, no

								regulatorio integral de IA.
4411-D-2023	Imágenes Sexuales de Menores Elaboradas mediante Sistemas de IA (Milman)	Gerardo Milman (PRO / Juntos por el Cambio)	Diputados	No	No	No	Modificación Código Penal	
4329-D-2023	Proyecto de Ley sobre Regulación y Uso de la Inteligencia Artificial	Anahí Costa (Frente de Todos / Unión por la Patria)	Diputados	Sí	Sí	Sí	Autoridad designada por el PEN	Registro de proveedores, evaluación previa
2505-D-2023	Marco Legal para la Regulación del Desarrollo y Uso de la Inteligencia Artificial	Victoria Morales Gorleri (PRO / Juntos por el Cambio)	Diputados	Sí	Sí	Sí	Autoridad designada por el PEN	Seguridad, responsabilidad, seguro civil
1472-D-2023	Modificación de la Ley Nacional 25.467 (Sistema Nacional de Ciencia, Tecnología e Innovación)	Jimena Latorre - UCR / Juntos por el Cambio (Mendoza)	Diputados	No	Sí	No	Agencia GACTEC	Poder de suspensión de investigación
3955-D-2024	Modificación del Código Penal para Incorporar Delitos Relacionados con Deepfake	Juan Brügge (Demócrata Cristiano)	Diputados	No	No	No	Modificación Código Penal	Nuevas figuras delictivas deepfake

3422-D-2024	Sistemas de Entornos Regulatorios Experimentales (SERE) “Sandbox regulatorios”	Martín Yeza (PRO / Juntos por el Cambio)	Diputados	No	Sí	No	Agencia I+D+I	SERE, entorno controlado
0805-D-2024	Responsabilidad Algorítmica y Promoción de la Robótica, Algoritmos Verdes e Inteligencia Artificial	Maximiliano Ferraro (Coalición Cívica)	Diputados	Sí	Sí	Sí	Sí (Consejo asesor)	Certificaciones, registro de riesgos, algoritmos verdes
S-1747-2023 PL	Proyecto de Ley Estableciendo Controles y Principios Rectores para el Desarrollo, Implementación y Utilización de Sistemas Basados en Inteligencia Artificial	Juan C. Romero (PRO / Juntos por el Cambio)	Senado	Sí	Sí	Sí	MINCyT (PEN) + Registro	Todo el ciclo de IA, auditoría anual ante HCD-HSN
S-2469-2023 PL	Proyecto de Ley de Modificación del Artículo 128 del Código Penal para Incluir Material Pornográfico Infantil Real o Simulado	Juan C. Romero (PRO / Juntos por el Cambio)	Senado	No	No	No	Modificación Código Penal	Penalización específica
S-1370-2024 PL	Proyecto de Ley Regulación de la IA en Educación	Beatriz Avila (Partido por la Justicia Social)	Senado	No	No	Sí	Ministerio de Educación	Ajustes curriculares, evaluación local
S-1368-2024 PL	Proyecto de Ley Marco Legal para la Investigación, Desarrollo, Uso y Regulación de la IA	Beatriz Ávila (Partido por la Justicia Social)	Senado	Sí	Sí	Sí	Autoridad designada por el PEN	Gestión de riesgos, verificación y certificación

S-0992-2024 PL	Proyecto de Ley Incorporación al Código Penal de Delitos con Intervención de IA	María Huala (Frente de Todos)	Senado	No	No	No	Código Penal	Delito “deep porn”
S-0959-2024 PL	Proyecto de Ley Obligación de Sello de Agua en Contenidos Audiovisuales Generados o Manipulados con IA	María Huala (Frente de Todos)	Senado	No	No	No	ENACOM	Informe al Congreso, sellado obligatorio

Fuente: Elaboración Propia.

BIBLIOGRAFIA

Legislación y normativa

Argentina. (2000). Ley 25.326 de Protección de los Datos Personales. Boletín Oficial de la república Argentina.

Brasil. (2018). Lei Geral de Proteção de Dados Pessoais (LGPD), Lei n.º 13.709. Diário Oficial da União.

Estados Unidos. (2018). California Consumer Privacy Act (CCPA). California Civil Code § 1798.100–1798.199.

Unión Europea. (2016). Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos (RGPD). Diario Oficial de la Unión Europea. https://eur-lex.europa.eu/eli/reg/2016/679/oj

Unión Europea. (2024). Reglamento de IA: Reglamento del Parlamento Europeo y del Consejo por el que se establecen normas armonizadas en materia de inteligencia artificial (Propuesta). https://artificialintelligenceact.eu/

Estados Unidos. (2023). Executive Order on the Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence. The White House. https://www.whitehouse.gov/

Consejo de Europa. (1981). Convenio 108 para la Protección de las Personas con respecto al Tratamiento Automatizado de Datos de Carácter Personal.

Congreso de la Nación Argentina. (2019). *Ley 27.483: Aprueba el Convenio para la Protección de las Personas con respecto al Tratamiento Automatizado de Datos de Carácter Personal (Convenio 108)*. Boletín Oficial de la República Argentina. Congreso de la Nación Argentina. (2023). *Ley 27.699: Aprueba el Protocolo de Enmienda al Convenio 108 (Convenio 108+)*. Boletín Oficial de la República Argentina.

Ley 25.326. Protección de los Datos Personales. Art. 27, inc. 3.

Decreto 1558/2001. Reglamentario de la Ley 25.326. Art. 27, inc. 3

Parlamento Europeo y Consejo de la Unión Europea. (2024). Reglamento (UE) 2024/XXXX del Parlamento Europeo y del Consejo por el que se establecen normas

armonizadas en materia de inteligencia artificial (Ley de Inteligencia Artificial). Diario Oficial de la Unión Europea. (en prensa).

City of New York. (2021). Local Law 144 of 2021: Automated Employment Decision Tools Law. New York City Council. Disponible en: https://www.nyc.gov

Agencia de Acceso a la Información Pública. (2022). Anteproyecto de Ley de Protección de Datos Personales. Disponible en: https://www.argentina.gob.ar/aaip

Honorable Cámara de Diputados de la Nación. (2023). Audiencias Públicas en la Comisión de Ciencia, Tecnología e Innovación Productiva – Inteligencia Artificial. HCDN. Disponible en: https://www.hcdn.gob.ar

Organismos e informes internacionales

OCDE. (2019). Principles on Artificial Intelligence. https://www.oecd.org/going-digital/ai/principles/

Organización para la Cooperación y el Desarrollo Económicos (OCDE). (2019). Principios de la OCDE sobre Inteligencia Artificial. Recuperado de https://www.oecd.org/going-digital/ai/principios/

Parlamento Europeo y Consejo. (2024). Reglamento (UE) del Parlamento Europeo y del Consejo por el que se establecen normas armonizadas en materia de inteligencia artificial (Ley de Inteligencia Artificial). Diario Oficial de la Unión Europea. Recuperado de https://eur-lex.europa.eu/

OCDE. (2020). Data Governance and the Role of Artificial Intelligence in the Protection of Personal Data.

OCDE. (2024). Artificial Intelligence and Data Privacy: A Global Framework.

UNESCO. (2021). Recomendación sobre la Ética de la Inteligencia Artificial. https://unesdoc.unesco.org

Naciones Unidas. (2024). Artificial Intelligence and Human Rights: A Global Perspective.

Comisión de Ética de Datos de Alemania (Datenethikkommission). (2019). Opinion of the Data Ethics Commission: Executive Summary. https://www.bmj.de

Future of Life Institute. (2017). Principios de Asilomar sobre Inteligencia Artificial.

Declaración de Montevideo. (2021). IA y Derechos Humanos en América Latina.

UNESCO. (2021). Recomendación sobre la Ética de la Inteligencia Artificial. París: Organización de las Naciones Unidas para la Educación, la Ciencia y la Cultura. https://unesdoc.unesco.org/ark:/48223/pf0000380455_spa

Organización de las Naciones Unidas (ONU). (2018). Informe del Relator Especial sobre el derecho a la privacidad. A/HRC/37/62. Recuperado de https://undocs.org/A/HRC/37/62

UNESCO. (2021). Recomendación sobre la Ética de la Inteligencia Artificial. Recuperado de https://unesdoc.unesco.org/ark:/48223/pf0000381137

OHCHR. (2022). Right to privacy in the digital age. United Nations Human Rights Office of the High Commissioner. https://www.ohchr.org/en/documents/thematic-reports/a77287-right-privacy-digital-age

Agencia de Acceso a la Información Pública (AAIP). (2022). El derecho de protección de datos personales en tiempos de IA. Recuperado de https://www.argentina.gob.ar/sites/default/files/ia_datos_personales_aaip_2022.pdf

Doctrina y artículos académicos

Baca Rivero, F. (2021). Un enfoque de la inteligencia artificial para la protección de datos personales sustentado en la base legal. Revista de Derecho de Alta Tecnología, 3(2), 75–89.

Binns, R. (2018). On the Role and Impact of Data Protection Laws in the Age of Artificial Intelligence. Journal of Information Law & Technology, 24(2).

Bonilla Gutiérrez, J. C. (2024). IA y Privacidad: Protegiendo la Autodeterminación Informativa en la Era Digital. Revista de la Facultad de Derecho de México, 74(290), 125–148. https://doi.org/10.22201/fder.24488933e.2024.290.89719

Cohen, J. E. (2013). Configuring the Networked Self: Law, Code, and the Play of Everyday Practice. Yale University Press.

Doneda, D., & Monteiro, F. (2020). Proteção de Dados Pessoais no Brasil: Comentários à Lei 13.709/2018. São Paulo: Revista dos Tribunais.

González Fuster, G. (2016). The Emergence of Personal Data Protection as a Fundamental Right of the EU. Springer.

López, M. A. (2020). Protección de Datos Personales: Un análisis crítico de la Ley 25.326 en el contexto digital. Editorial LexisNexis.

Monastersky, D. (2019). Privacidad digital y regulación algorítmica. Citado en entrevistas y columnas especializadas.

Russell, S., & Norvig, P. (2021). Artificial Intelligence: A Modern Approach (4.ª ed.). Pearson.

Solove, D. J. (2021). The Concept of Privacy. Stanford Law Review, 53(5), 1104–1151.

Tufekci, Z. (2018). Twitter and Tear Gas: The Power and Fragility of Networked Protest. Yale University Press.

Wachter, S., Mittelstadt, B., & Floridi, L. (2017). Why a Right to Explanation of Automated Decision-Making Does Not Exist in the General Data Protection Regulation. International Data Privacy Law, 7(2), 76–99.

Barona Vilar, S. (2021). Inteligencia artificial o la algoritmización de la vida y de la justicia. Tirant lo Blanch.

Peyrano, G., & Melo, V. (2023). Desafíos regulatorios de la IA en Argentina. Revista de Derecho Digital.

Anconitano, V., & Vitari, W. (2025). What is AI SEO? How artificial intelligence is changing search optimization. Search Engine Land. https://searchengineland.com/guide/what-is-ai-seo

Swant, M. (2025, May 5). In Graphic Detail: How AI is changing search and advertising. Digiday. https://digiday.com/marketing/in-graphic-detail-how-ai-is-changing-search-and-advertising/

United States District Court, Northern District of California. (2025). Andrea Bartz, Charles Graeber, and Kirk Wallace Johnson v. Anthropic PBC (No. C 24-05417

WHA).
https://fingfx.thomsonreuters.com/gfx/legaldocs/jnvwbgqlzpw/ANTHROPIC%20fair%20use.pdf

Basterra, M. I. (2004). El consentimiento del afectado en el proceso de tratamiento de datos personales. Disponible en: https://marcelabasterra.com.ar/wp-content/uploads/2016/11/HD.-El-consentimiento-del-afectado-en-el-proceso-de-tratamiento-de-datos-personales.pdf

Peyrano, G. (2003). La validez del consentimiento como manifestación de voluntad en el tratamiento de datos personales, Revista de Derecho Informático, UCA.

Casos y estudios prácticos

Caso reconocimiento facial en la Ciudad de Buenos Aires (2022).

Caso chatbot de Silvina Luna y derechos personalísimos en IA (2023).

Estudios sobre sesgos algorítmicos en sistemas de selección de personal (2021–2023).

Cámara de Apelaciones en lo Contencioso, Administrativo y Tributario de la Ciudad Autónoma de Buenos Aires, Sala I. (2021). Observatorio de Derecho Informático Argentino (O.D.I.A.) c/ GCBA s/ amparo. Expediente N° 182908/2020.

Tribunal Constitucional Federal Alemán. (1983). Sentencia de 15 de diciembre de 1983 (BVerfGE 65, 1)

Cámara de Apelaciones en lo Contencioso Administrativo y Tributario y de Relaciones de Consumo de la Ciudad Autónoma de Buenos Aires, Sala I. (2022). ODIA y otros c/ GCBA s/ amparo. Causa 26745/2022-0.

Lascano Quintana c/ Organización Veraz S.A., Cámara Nacional de Apelaciones del Trabajo. Comentado por Basterra (2004), disponible en: https://marcelabasterra.com.ar/...

Torres Abad c/ EN – JGM, Expte. 49.482/2016 CA1. Acceso al fallo en: https://www.eldial.com/nuevo/nuevo_diseno/v2/fallo4.asp?base=14&id=47758

Procuración del Tesoro de la Nación (2020). Dictamen sobre el uso de datos personales con fines de propaganda. Disponible en: https://palabrasdelderecho.com.ar/articulo/2076/

Caso Bartz, Graeber y Johnson v. Anthropic PBC (Estados Unidos): United States District Court, Northern District of California. (2025). Andrea Bartz, Charles Graeber, and Kirk Wallace Johnson v. Anthropic PBC, No. C 24-05417 WHA.

Caso The New York Times Company v. Microsoft Corporation et al. (META): United States District Court, Southern District of New York. (2024). The New York Times Company v. Microsoft Corporation and OpenAI Inc., No. 1:23-cv-11195.

Giudici, S. (2025). Proyecto de Ley 3540-D-2025: Modificación de la Ley 25.326 de Protección de Datos Personales para incorporar principios de transparencia algorítmica, derecho a la explicación, auditoría y revisión humana. Honorable Cámara de Diputados de la Nación Argentina.

Guías y manuales técnicos

Determann, L. (2017). Determann's Field Guide to Data Privacy Law (3.ª ed.). Berkeley Technology Law Journal.

Determann, L., & Guttenberg, K. T. zu. (2014). On war and peace in cyberspace: Security, privacy, jurisdiction. Hastings Constitutional Law Quarterly, 41(4), 901–930.

William Fry LLP. (2024). AI Guide: Legal Frameworks for Artificial Intelligence. https://www.williamfry.com/wp-content/uploads/2024/12/WF-AI-guide-Dec24-3.pdf

Latham & Watkins LLP. (2024). EU AI Act: Navigating a Brave New World. https://www.lw.com/en/admin/upload/SiteAttachments/EU-AI-Act-Navigating-a-Brave-New-World.pdf

Agencia de Acceso a la Información Pública. (2000). Ley 25.326 de Protección de Datos Personales. Argentina.

Agencia de Acceso a la Información Pública. (2021). Proyecto de modificación de la Ley 25.326. https://www.argentina.gob.ar/sites/default/files/proyecto_de_modificacion_ley_25326.pdf

Baca Rivero, F. (2021). Protección de datos personales e inteligencia artificial: una aproximación crítica desde la perspectiva latinoamericana. Revista Chilena de Derecho y Tecnología, 10(2), 25-46.

Bonilla Gutiérrez, J. (2024). Vigilancia algorítmica y derecho a la privacidad: desafíos para América Latina. Editorial Jurídica Panamericana.

Bostrom, N. (2014). Superintelligence: Paths, Dangers, Strategies. Oxford University Press.

Charter of Fundamental Rights of the European Union. (2000). Official Journal of the European Communities, C 364/1.

Comité Europeo de Protección de Datos (EDPB). (2024). Opinion 28/2024 sobre el tratamiento de datos personales en sistemas de IA. https://edpb.europa.eu

Determann, L. (2017). Determann's Field Guide to Data Privacy Law: International Corporate Compliance. IAPP Publications.

Doneda, D., & Monteiro, R. L. (2020). Brazil's General Data Protection Law: A Detailed Overview. Global Privacy Law Review, 1(1), 10–19.

European Parliament and Council. (2016). Regulation (EU) 2016/679 (General Data Protection Regulation – GDPR).

Gobierno del Estado de Colorado. (2024). Colorado Artificial Intelligence Act. Colorado General Assembly.

Instituto Nacional de Tecnología Industrial (INTI). (2023). IA y privacidad: impacto en Argentina. Documento técnico.

Monastersky, D. (2019). Protección de datos personales y el desafío de la inteligencia artificial. Editorial Astrea.

Organización de las Naciones Unidas para la Educación, la Ciencia y la Cultura (UNESCO). (2024). Consulta Mundial sobre Regulación de la IA: Enfoques Emergentes. https://unesdoc.unesco.org

Russell, S., & Norvig, P. (2021). Artificial Intelligence: A Modern Approach (4ª ed.). Pearson.

Tribunal Constitucional Federal Alemán. (1983). Sentencia sobre el Censo (Volkszählungsurteil).

Selinger, E., & Hartzog, W. (2019). *The Inescapable Collective*. In J. van den Hoven, B.-J. Koops & L. Leenes (Eds.), **Group Privacy: New Challenges of Data Technologies** (pp. 51–66). Springer. https://doi.org/10.1007/978-3-030-15759-5_3

Purtova, N. (2018). The Law of Everything. Broad Concept of Personal Data and Future of EU Data Protection Law. *Law, Innovation and Technology*, 10(1), 40–81. https://doi.org/10.1080/17579961.2018.1452176

Angwin, J., Larson, J., Mattu, S., & Kirchner, L. (2016). *Machine Bias: There's software used across the country to predict future criminals. And it's biased against blacks.* ProPublica. https://www.propublica.org/article/machine-bias-risk-assessments-in-criminal-sentencing

Dastin, J. (2018). *Amazon scraps secret AI recruiting tool that showed bias against women.* Reuters. https://www.reuters.com/article/us-amazon-com-jobs-automation-insight-idUSKCN1MK08G

Purtova, N. (2021). *The law of everything. Broad concept of personal data and future of EU data protection law*. Law, Innovation and Technology, 3(1), 40–81.

Zuboff, S. (2019). *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power*. New York: PublicAffairs.

Bonilla Gutiérrez, C. (2024). *La crisis del consentimiento en la era digital*. Revista Latinoamericana de Protección de Datos, 10(1), 45–61.

Mayer Brown. (2024, junio). Colorado Governor Signs Comprehensive AI Bill. Recuperado de https://www.mayerbrown.com/en/insights/publications/2024/06/colorado-governor-signs-comprehensive-ai-billSkadden+2Mayer Brown+2Mayer Brown+2

Willkie Farr & Gallagher LLP. (2024, octubre). California Enacts 17 AI Bills in 2024. Recuperado de https://www.willkie.com/publications/2024/10/california-enacts-17-ai-bills-in-2024Willkie Farr & Gallagher

Maryland General Assembly. (2023). Legislation - HB1068. Recuperado de https://mgaleg.maryland.gov/mgawebsite/Legislation/Details/hb1068?ys=2023RS

Determann, L. (2017). *Determann's Field Guide to Data Privacy Law: International Corporate Compliance*. Berkeley: Berkeley Technology Law Journal.

Mayer Brown. (2024, junio). *Colorado Governor Signs Comprehensive AI Bill*. Recuperado de https://www.mayerbrown.com/en/insights/publications/2024/06/colorado-governor-signs-comprehensive-ai-bill

Maryland General Assembly. (2023). *Legislation - HB1068*. Recuperado de https://mgaleg.maryland.gov/mgawebsite/Legislation/Details/hb1068?ys=2023RS

Willkie Farr & Gallagher LLP. (2024, octubre). *California Enacts 17 AI Bills in 2024*. Recuperado de https://www.willkie.com/publications/2024/10/california-enacts-17-ai-bills-in-2024