Grupo 5 - Balbuena - Lopez - Moreno - Villarreal

Trabajo Final – Régimen Jurídico Aplicable para el Uso Responsable de la Inteligencia Artificial

Fecha de entrega: 09/06/2025

Materia: Aspectos legales y normativos

Docentes:

Dra. Josefina Riva Posse

E. Damián Bes

Universidad: Universidad del Gran Rosario (UGR)

Índice

1. Introducción

Como estudiantes de la Tecnicatura Universitaria en Ciberseguridad, reconocemos que el avance de la inteligencia artificial plantea desafíos clave en derechos humanos, privacidad y seguridad digital. Por eso, analizamos el proyecto de ley “Régimen Jurídico Aplicable para el Uso Responsable de la Inteligencia Artificial” con una mirada crítica.
Este trabajo busca identificar sus principales aportes y proponer mejoras en aspectos como la ciberseguridad, la gestión de riesgos, la trazabilidad y la responsabilidad ética y legal de los actores que desarrollan y aplican estas tecnologías.

2. Desarrollo

PROYECTO DE LEY

El Senado y la Honorable Cámara de Diputados sancionan con fuerza de ley

“RÉGIMEN JURIDICO APLICABLE PARA EL USO RESPONSABLE DE LA INTELIGENCIA ARTIFICIAL EN LA REPUBLICA ARGENTINA”

TITULO I

DISPOSICIONES GENERALES

ARTÍCULO 1°: Del régimen jurídico aplicable

1. Por la presente, se establece el régimen jurídico para el uso responsable de la Inteligencia Artificial (IA) introducida, distribuida, utilizada, aplicada o comercializada en el territorio de la República Argentina.
2. Este régimen alcanza tanto a los desarrolladores y proveedores de sistemas de IA como a los usuarios y demás actores intervinientes en cualquiera de sus fases de ciclo de vida.

ARTÍCULO 2°: Objetivo

La presente ley tiene por finalidad regular el uso responsable de la Inteligencia Artificial (IA) mediante un marco jurídico basado en los siguientes principios:
1. Fomentar el desarrollo, la introducción al mercado y la utilización de sistemas de IA en la República Argentina.
2. Promover la aplicación ética de la IA, garantizando el respeto a los derechos humanos y libertades fundamentales.
3. Adoptar normas seguras y confiables que protejan la salud, la seguridad y los derechos fundamentales de las personas frente a los posibles efectos derivados del uso de sistemas de IA.

ARTÍCULO 3°: Ámbito de aplicación

1. La presente ley se aplica a las personas humanas y jurídicas que, en el territorio de la República Argentina, actúen en las siguientes calidades:
a) Proveedores de sistemas de IA.
b) Responsables del despliegue de sistemas de IA.
c) Importadores, distribuidores o fabricantes de productos o servicios basados en IA.
d) Usuarios de sistemas de IA.
2. Quedan comprendidos, además, todos aquellos terceros cuya actividad se relacione directa o indirectamente con el ciclo de vida de sistemas de IA.

ARTÍCULO 4°: Definiciones

A los fines de la presente ley, se entenderá por:

1. Inteligencia Artificial (IA): sistema asistente-técnico fundamentado en técnicas computacionales que automatiza tareas simulando comportamientos inteligentes propios de la inteligencia humana, incluidos el aprendizaje automático, la percepción visual, el procesamiento del lenguaje natural y la toma de decisiones.

2. Sistema de Inteligencia Artificial: sistema que funciona con cierto grado de autonomía y que, con datos de entrada, proporcionados por máquinas o personas, infiere cómo alcanzar objetivos establecidos mediante estrategias de aprendizaje automático o basadas en lógica y conocimiento, generando como salida contenidos, predicciones, recomendaciones o decisiones.

3. Uso responsable de la IA: empleo de sistemas de IA de manera ética y transparente, respetando los derechos humanos, la privacidad, la seguridad y la equidad.

4. Principio ético de uso de la IA: conjunto de acciones y técnicas destinadas a resguardar, la dignidad, la libertad y la privacidad de la persona humana que accede a un sistema de IA.

5.Sistema de IA transparente: aquel cuya operativa es comprensible y explicada de forma clara a los usuarios y partes interesadas.

6. Evaluación de impacto de IA: proceso para identificar, evaluar y abordar los impactos, riesgos y consecuencias éticas, sociales y legales del desarrollo o implementación de sistemas de IA.

7. Proveedor: persona humana o jurídica, pública o privada, que desarrolla, encarga, ofrece o comercializa un sistema de IA, con o sin retribución.

8. Usuario: persona humana o jurídica, pública o privada, bajo cuya autoridad se utiliza un sistema de IA, sea propio o de un tercero.

9. Grupo de interés afectado: persona humana o jurídica o conjunto de personas cuyos derechos o intereses se vean comprometidos, directa o indirectamente, por la aplicación de sistemas de IA, aun sin interactuar con ellos (por ejemplo, consumidores, trabajadores, investigadores o gobiernos).

ARTÍCULO 5°: Principios Rectores

Son principios rectores del presente régimen jurídico los siguientes:

1. Transparencia: Se deberá garantizar que toda persona que interactúe con un sistema de I.A. sea debidamente informada de dicha interacción. El cumplimiento podrá acreditarse mediante identificaciones visuales y/o auditivas claras que informen que un contenido o interacción ha sido generado total o parcialmente mediante I.A.

Los riesgos asociados al uso de estos sistemas deberán ser informados de forma clara, accesible y comprensible para los usuarios y el público en general.

2. Robustez: Los desarrolladores, operadores y usuarios de sistemas de I.A. deberán garantizar su correcto funcionamiento, velando por el respeto de los derechos humanos y las garantías constitucionales.

Se promoverán mecanismos de evaluación y verificación periódica, así como la capacitación del personal involucrado en su desarrollo y utilización.

3. Equidad y No Discriminación: Durante todo el ciclo de vida de los sistemas de I.A., se evitarán sesgos y prácticas discriminatorias, promoviendo la equidad, la inclusión y la accesibilidad, a fin de garantizar que los beneficios de la tecnología estén disponibles para toda la sociedad.

4. Responsabilidad Proactiva: Los desarrolladores y usuarios deberán adoptar medidas técnicas y organizativas adecuadas para demostrar que sus sistemas de I.A. son éticos, transparentes, seguros, respetuosos de los derechos humanos y de la privacidad.

Esto incluye: protección de datos desde el diseño, análisis de riesgos, evaluaciones de impacto, validación de resultados, monitoreo y revisión periódica de su funcionamiento.

5. Trazabilidad: Debe garantizarse la posibilidad de auditar, comprender y verificar las decisiones, recomendaciones o acciones realizadas por un sistema de I.A. mediante la provisión de información clara, accesible y verificable en todo momento.

6. Privacidad y Seguridad: La privacidad de los datos personales y la seguridad de los sistemas deberán estar protegidas conforme a los más altos

estándares técnicos y legales. Los incidentes de seguridad que pudieran afectar derechos de las personas deberán notificarse sin dilación a la Autoridad de Aplicación, a la Dirección Nacional de Protección de Datos Personales y a los titulares de los datos afectados.

7. Fiabilidad y Reproducibilidad: Los sistemas de I.A. deberán reproducir con fidelidad la realidad captada, especialmente en contenidos audiovisuales, audios o fotografías, garantizando su integridad cuando sean utilizados como evidencia en procesos judiciales o administrativos.

8. Colaboración Internacional: Se promoverá la cooperación con organismos internacionales, académicos y técnicos para enfrentar desafíos éticos, legales y técnicos, mediante el intercambio de buenas prácticas.

ARTÍCULO 6°: Evaluación de Impacto sobre Derechos Humanos

La Autoridad de Aplicación deberá garantizar, además del cumplimiento de los principios establecidos en la presente ley, lo siguiente:

•Requerir la implementación obligatoria de una Evaluación de Impacto en Derechos Humanos (EIDH) para todos los proyectos de I.A.

• Asegurar que la EIDH se realice de forma transparente y participativa, con la intervención de expertos, partes interesadas y organizaciones de la sociedad civil.

• Publicar los resultados de la EIDH, los cuales deberán ser considerados para autorizar, modificar o restringir la implementación de un sistema de I.A.

• Evaluar los riesgos en función de su probabilidad y la magnitud del daño potencial.

• Considerar tanto los impactos positivos como negativos en la evaluación.

• Documentar los riesgos identificados y las medidas adoptadas para mitigarlos.

• Exigir la aplicación de protocolos de prueba, validación y verificación, acordes al tipo y criticidad del sistema desarrollado.

• Promover procesos de mejora continua para prevenir desvíos, fallas o sesgos emergentes posteriores a su implementación.

• Implementar mecanismos de supervisión y control, tanto internos como externos, para garantizar la integridad de los sistemas.
• Verificar el cumplimiento de las obligaciones impuestas a desarrolladores, proveedores y usuarios.
• Desarrollar programas de formación ciudadana sobre el uso responsable de la I.A. y la identificación de situaciones de riesgo para los derechos humanos.
•Aplicar sanciones proporcionales a quienes incumplan la presente normativa.

ARTÍCULO 7°: Gestión de riesgos de I.A.

La responsabilidad de los proveedores y usuarios en la implementación y uso de sistemas de Inteligencia Artificial (I.A.) se determinará conforme las siguientes categorías de riesgo:

1. Riesgo inaceptable y prácticas prohibidas:

Quedarán prohibidos los sistemas de I.A. que constituyan una amenaza manifiesta a los derechos fundamentales. Esto incluye:

a) La manipulación cognitiva o conductual de personas, en especial de grupos vulnerables, de forma que impida la toma de decisiones informadas o provoque acciones que no se hubiesen realizado sin dicha manipulación, siempre que generen o puedan generar un daño.

b) Sistemas de puntuación social o clasificación de personas que deriven en un trato desfavorable o discriminatorio, ya sea por su puntaje o pertenencia a determinada categoría.

c) Búsqueda de personas o investigación de delitos graves, en concordancia con la legislación penal vigente, deberá realizarse obligatoriamente una Evaluación de Impacto según el Artículo 6 y notificarse a la Dirección Nacional de Protección de Datos Personales.

2. Riesgo alto:

Sistemas que puedan afectar gravemente la integridad, libertad, salud o derechos fundamentales. Estarán sujetos a:

• Evaluación previa y registro ante la autoridad de aplicación.
• Auditorías periódicas, incluso durante su operación.

• Publicación obligatoria de algoritmos y datasets empleados en su funcionamiento, garantizando trazabilidad y posibilidad de auditoría externa.
• Incluyen, entre otros, sistemas aplicados a infraestructura crítica, justicia, salud, educación, seguridad pública, gestión migratoria y empleo.

3. Riesgo medio:

Sistemas que interactúan de forma limitada con decisiones humanas sin sustituirlas sustancialmente. Requieren inscripción ante la autoridad de aplicación y deben cumplir con los principios del Artículo 5. Serán considerados riesgo medio cuando:

a) Mejoren resultados de actividades humanas sin sustituirlas.
b) Detecten desviaciones de patrones sin accionar directamente.
c) Sean auxiliares de tareas, sin tener autonomía de decisión.
d) Cumplan con todos los requisitos legales y técnicos establecidos por la autoridad de aplicación.

4. Riesgo bajo:

Sistemas que no se encuadren en los niveles anteriores y que presenten mínima incidencia sobre los derechos fundamentales. Deberán:

a) Ajustarse a los principios rectores del Artículo 5.
b) Incorporar mecanismos accesibles de reporte y reclamo para usuarios y afectados.
c) Documentar los datos, fuentes y protocolos utilizados, asegurando la transparencia.

Además, se establece la creación de un organismo técnico independiente con competencias suficientes para ejercer como autoridad de aplicación, fiscalización y sanción, a fin de evitar conflictos de interés y garantizar imparcialidad en la gestión de riesgos.

ARTÍCULO 8°: Protección de Datos y Privacidad

DISPONGASE que toda implementación desarrollo y uso de un sistema de I.A. deberá respetar y garantizar el derecho a la privacidad de las personas humanas que lo utilicen o sean destinatarios del mismo, así como la

protección de sus datos personales, cumpliendo con los principios y reglas establecidas en la ley 25.326, a tal efecto deberán adoptarse medidas técnicas y organizativas apropiadas para garantizar la seguridad, confidencialidad, integridad, disponibilidad y uso legítimo de los datos, evitando su uso indebido, acceso no autorizado y manipulación, o cualquier forma de afectación que pueda comprometer los derechos de los usuarios y la integridad del sistema adoptando medidas de seguridad adecuadas para la protección de los datos personales.

ARTÍCULO 9°: Deberes y Responsabilidades

ESTATUYESE como deberes y responsabilidades de los proveedores y usuarios del sistema de I.A., los siguientes:

1) En todo momento de utilización del I.A., el usuario debe disponer de mecanismos tecnológicos que le permita limitar, restringir o mitigar los efectos de la I.A. en contextos que afecten derechos humanos o grupos vulnerables.

2) El usuario debe disponer de mecanismos tecnológicos de minimización de datos, rectificación, supresión y modificación de datos para asegurar la calidad de los datos utilizados.

3) El usuario de I.A. deberá contar con protocolos, mecanismos y medidas apropiadas para la detección temprana de fallas o comportamientos inusuales, vulneraciones, ataques, incidentes de seguridad, abusos o riesgos desconocidos a priori, con el fin de suspender, bloquear, desactivar, desconectar, contrarrestar y mitigar los efectos.

4) En caso de detección de fallas, incidentes o errores, que puedan afectar los derechos de una persona humana o grupo de personas humanas, el usuario y proveedor de I.A. están obligados a notificarle de forma inmediata y adecuada la desviación generada a los titulares de datos o personas y terceros potencialmente afectadas, informando las vías disponibles para que el afectado o los afectados puedan ejercer sus derechos, lograr la rectificación de la información o remediación de la decisión tomada por I.A.

5) Los proveedores y usuarios de sistemas de I.A. son responsables de sus acciones y decisiones por los daños y perjuicios producidos a las personas humanas y jurídicas con la utilización del sistema, sea por el mal uso o fallas de los mismos, conforme las disposiciones del Código Civil y Comercial de la Nación y, en su caso, del Código Penal, en tanto y en cuanto resultare aplicable.

Los mecanismos tecnológicos dispuestos en los incisos 1 al 4 del presente artículo, como obligatorios para los proveedores y usuarios, deben ser comunicados a la autoridad de aplicación previa a su implementación.

ARTÍCULO 10° Autoridad de aplicación y fiscalización

El Instituto Nacional de Tecnología Industrial (INTI) o la autoridad pública que en el futuro lo reemplace, es la autoridad de aplicación y de fiscalización de la presente ley, con las siguientes atribuciones:

1) Verificar, auditar y certificar que los sistemas de I.A. cumplan con los principios, requisitos técnicos y legales establecidos en la ley, sus normas complementarias y en los Tratados Internacionales ratificados que la República Argentina adhiere en materia de derechos humanos y tecnología.

2) Dictar las normas administrativas, normas reglamentarias y resoluciones técnicas necesarias para la implementación efectiva de la presente ley.

3) Aplicar las sanciones correspondientes en caso de infracciones a la presente ley.

La autoridad de aplicación coordina su accionar, en lo que respecta a la protección de datos personales, con la Agencia Nacional de Acceso a la Información Pública.

TITULO II

DISPOSICIONES COMPLEMENTARIAS

CAPITULO 1

De las Sanciones y Acciones Reparadoras

ARTÍCULO 11°. Sanciones

LOS proveedores y usuarios que infrinjan las disposiciones de la presente ley son pasibles de las siguientes sanciones:

1) Multa:

a) Por incumplimiento de las obligaciones legales previstas en la presente ley a los infractores del sistema I.A., se aplicará la sanción de multa graduable entre uno (1) a un mil (1000) Argentinos Oro, a ser abonados al precio de su cotización oficial al momento del pago. De acuerdo a los siguientes criterios:

-Gravedad del incumplimiento a la normativa y el daño causado.

-Reincidencia por parte del infractor.

-Potencial del daño inherente al sistema y la posibilidad de que existan otros afectados.

-Impacto social, económico o sobre derechos fundamentales que la infracción puede ocasionar.

2) Suspensión o Cancelación de la autorización:

a) En los supuestos en que los proveedores o usuarios de los sistemas categorizados como de Riesgo Alto o Medio, no cumplan con los requisitos legales, tecnológicos o éticos establecidos para su utilización o se produzcan desvíos de la finalidad para los cuales fueron autorizados.

b) Se detecten desvíos en la finalidad autorizada o afectación directa o indirecta, con la utilización del sistema I.A.

La graduación de esta sanción se realizará conforme la gravedad de la infracción, reiteración, y daños derivados. Podrá aplicarse como sanción accesoria una multa conforme el inciso 1 del presente artículo.

3) Prohibición de uso del sistema de I.A:

Aplicable a proveedores o usuarios de sistemas de bajo riesgo que incumplan reiteradamente los requisitos legales establecidos, conforme los parámetros antes mencionados establecidos en el párrafo último del inciso 2 de este artículo.

El procedimiento sancionatorio deberá garantizar el debido proceso, el derecho de defensa y el respeto a los principios constitucionales consagrados en la Constitución Nacional y el derecho internacional de los derechos humanos.

ARTÍCULO 12° – Acción Judicial Resarcitoria

Este artículo reconoce el derecho de toda persona a reclamar judicialmente cuando sus derechos hayan sido vulnerados por el uso indebido de sistemas de IA. Se establece un régimen de responsabilidad objetiva, no será necesario probar culpa o negligencia para acceder a una indemnización. El monto puede oscilar entre 1 y 1000 “Argentinos Oro”, y se establece un criterio orientador para su graduación: gravedad del daño, reincidencia, impacto social, entre otros. Esta disposición fortalece el enfoque preventivo y el principio de rendición de cuentas, busca garantizar la reparación integral ante los riesgos de sistemas autónomos que pueden afectar a las personas sin intervención humana directa.

ARTÍCULO 13° – Consejo Asesor en I.A.

Se crea un organismo consultivo, interdisciplinario e independiente, encargado de asistir en el análisis ético, social, técnico y jurídico del desarrollo y uso de IA en el país. Estará conformado por especialistas provenientes de diversos sectores: público, privado, académico y de la sociedad civil. Su principal finalidad es asegurar que las decisiones sobre IA incluyan una mirada crítica sobre el impacto en los derechos humanos, la equidad y la inclusión.

ARTÍCULO 14° – Funciones del Consejo Asesor

El artículo establece las funciones del Consejo Asesor, entre las que se destacan: revisar proyectos de IA con impacto significativo, evaluar riesgos éticos, promover la participación ciudadana, asesorar técnicamente a autoridades y empresas, emitir informes públicos y colaborar en la educación sobre el uso responsable de IA. Esta disposición otorga un marco institucional

para que el desarrollo de IA sea acompañado por mecanismos de control social y ético.

ARTÍCULO 15° – Cooperación Internacional

La ley reconoce que los desafíos vinculados a la IA trascienden fronteras, y por ello establece que el Poder Ejecutivo debe fomentar la cooperación internacional. Se prevé la participación en organismos multilaterales, el intercambio de información, la adopción de buenas prácticas y la colaboración para el desarrollo conjunto de estándares regulatorios.

ARTÍCULO 16° – Vigencia

Este artículo establece que la ley entrará en vigencia desde su publicación en el Boletín Oficial, activando su fuerza legal de manera inmediata. A partir de ese momento, todas sus disposiciones serán exigibles, tanto por los ciudadanos como por la autoridad de aplicación.

ARTÍCULO 17° – De forma

Finalmente, se habilita al Poder Ejecutivo a reglamentar la ley, permitiéndole dictar las normas complementarias necesarias para su efectiva aplicación. Este paso es clave para que los principios y artículos de la ley se traduzcan en acciones, procesos y controles concretos. Al facultar al Ejecutivo, se garantiza que la norma no quede en un plano declarativo, sino que pueda operativizarse en el corto plazo, asignando funciones, creando organismos y detallando procedimientos específicos.

FUNDAMENTOS

Este trabajo se elaboró a partir del análisis crítico de un proyecto de ley base sobre el uso responsable de la inteligencia artificial (IA), provisto por la cátedra. Como estudiantes de segundo año de la Tecnicatura Universitaria en Ciberseguridad, propusimos mejoras en redacción, contenido y estructura, con el objetivo de fortalecer su aplicabilidad técnica y jurídica.

Buscamos contribuir a un marco normativo que regule el desarrollo, implementación y uso de sistemas de IA en Argentina, considerando tanto sus beneficios como sus riesgos éticos, técnicos y sociales. Las modificaciones a los artículos 1° al 17° se enfocaron en: mayor precisión legal y técnica, incorporación de principios alineados con estándares internacionales, y promoción de mecanismos de control, auditoría, trazabilidad y reparación.

Se ajustaron definiciones, objetivos y alcances para lograr un lenguaje claro y coherente. Se reforzaron conceptos como evaluación de impacto, transparencia algorítmica y supervisión ética. En los capítulos sobre riesgos, privacidad y responsabilidad, se promovió el rol activo del Estado y la protección de derechos mediante herramientas de ciberseguridad.

También se conservaron artículos estratégicos como los que crean el Consejo Asesor, regulan la cooperación internacional y definen la vigencia de la norma.

Este proceso fortaleció nuestras habilidades en derecho digital y gobernanza tecnológica, así como el trabajo colaborativo. Utilizamos modelos de lenguaje (LLM) para apoyar la redacción y validación técnica, manteniendo criterio propio y autonomía.

El análisis partió de un documento base proporcionado por la cátedra, enriquecido con definiciones adaptadas de fuentes técnicas internacionales como la Unión Europea, UNESCO y OCDE.

3. Prompts utilizados con LLM (ChatGPT)

"Analizamos los artículos 5,6 y 7 de los siguientes artículos, pero queremos mejorar la redacción y profundizar el análisis. ¿Podés ayudarnos a revisarlos sugiriendo mejoras desde una mirada técnica, ética y jurídica, y explicando por qué serían necesarias?"

"Actúa como si fueras un abogado, corrige este texto de proyecto de ley, agregando, eliminando o modificando texto. Ten en cuenta el código penal de argentina"

"Redactá una fundamentación académica que justifique las modificaciones realizadas en los artículos 1 al 4 del proyecto de ley sobre el uso responsable de la inteligencia artificial. Explica qué se cambió, por qué se hizo y qué

beneficios aporta, desde una perspectiva técnica, ética y legal, considerando conceptos como ciberseguridad, trazabilidad, inclusión y alineación con estándares internacionales."

Prompt 1: Se utilizó para revisar y mejorar los artículos 5, 6 y 7 desde una mirada técnica, ética y jurídica. A partir de esto, se ajustó la redacción, se incorporaron auditorías, y se clarificaron conceptos legales.

Prompt 2: Permitió validar el texto según el Código Penal Argentino. Se simplificaron referencias penales y se fortaleció la seguridad jurídica en artículos con contenido sancionatorio.

Prompt 3: Facilitó la redacción de fundamentos para los artículos 1 al 4, incorporando principios de ciberseguridad, trazabilidad y estándares internacionales. Se reflejó en la sección "Fundamentos".

4. Conclusión grupal

Este trabajo nos permitió comprender con mayor profundidad los desafíos actuales que enfrenta nuestro país al intentar regular el uso de la inteligencia artificial. Como estudiantes de segundo año de la carrera de Ciberseguridad, analizamos el proyecto de ley no solo desde lo jurídico, sino también desde una mirada técnica, social y ética, tratando de aportar mejoras concretas que reflejen los riesgos reales que enfrentamos en nuestra disciplina.

Coincidimos en que el proyecto representa un paso importante para establecer un marco legal en un tema que, hasta ahora, viene siendo impulsado más por la tecnología que por la normativa. Sin embargo, también notamos que muchas de sus disposiciones todavía son generales o poco aplicables en el plano técnico. Esto nos llevó a proponer ajustes que busquen hacerlo más operativo, especialmente en cuanto a trazabilidad, supervisión de algoritmos y responsabilidad ante errores o sesgos.

El trabajo en grupo fue clave para poder combinar diferentes enfoques. Cada uno aportó desde su mirada, y tuvimos que ponernos de acuerdo no solo sobre qué modificar, sino también sobre cómo redactarlo, justificando nuestras decisiones con fundamentos sólidos. Esto nos ayudó a desarrollar habilidades colaborativas, y también a darnos cuenta de que regular la IA no es tarea de

una sola disciplina, sino que requiere la participación de especialistas técnicos, legales y sociales.

Uno de los desafíos éticos que más debatimos fue el riesgo de discriminación algorítmica. Nos preocupó especialmente la posibilidad de que sistemas de IA tomen decisiones que afecten a personas sin que haya transparencia ni posibilidad real de reclamo. También vimos la necesidad de que haya una autoridad de aplicación fuerte y con conocimientos técnicos reales, para que la ley no quede solo en el papel.

Usamos el modelo de lenguaje (LLM) como una herramienta de guía para mejorar nuestro trabajo en todos los aspectos: desde la comprensión técnica de algunos conceptos, hasta la organización del contenido, la redacción clara de las modificaciones y la validación ética de nuestras propuestas. No se trató solo de corregir o completar textos, sino de aprovechar el LLM para ordenar ideas, resolver dudas y fortalecer nuestros fundamentos. Esta integración nos permitió desarrollar un análisis más completo y enfocado, sin perder nuestra autonomía como grupo.

En definitiva, esta actividad nos permitió aplicar contenidos de la carrera a un caso real y actual, poniendo en práctica conocimientos de derecho digital, ética profesional y análisis de riesgos tecnológicos. Más allá de la nota, nos llevamos una experiencia que nos hizo pensar en el rol que vamos a tener en el futuro como profesionales que trabajen con y sobre sistemas de IA.

5. Apéndice

Artículos 1 al 4: Dante Balbuena

Artículos 5, 6 y 7: Victoria Lopez

Articulos 8 al 11: Angela Villareal

Artículos 12 al 17: Valentín Moreno