

La inteligencia artificial como aliada para un parlamento abierto más transparente y participativo

Rafael Rubio Núñez

Catedrático de Derecho Constitucional
Universidad Complutense de Madrid
España

ORCID [0000-0001-5074-0371](https://orcid.org/0000-0001-5074-0371)

E-mail: rafa.rubio@der.ucm.es

Miguel Ángel Gonzalo Rozas

Director de Documentación, Biblioteca y Archivo
Congreso de los Diputados
España

ORCID [0000-0002-9735-6497](https://orcid.org/0000-0002-9735-6497)

E-mail: miguel.gonzalo@congreso.es

RECIBIDO: 14 de septiembre de 2025

ACEPTADO: 11 de octubre de 2025

Revista Española de la Transparencia

Núm. 23 (2026). Extra - ISSN 2444-2607

DOI: <https://doi.org/10.51915/ret.421>



La inteligencia artificial como aliada para un parlamento abierto más transparente y participativo

RESUMEN: La acelerada digitalización de la sociedad y el auge de la inteligencia artificial (IA) están transformando profundamente el ecosistema jurídico-político. Se estudia el papel de la IA en un parlamento abierto, describiendo ejemplos en distintos países donde estas herramientas incrementan la transparencia legislativa, la participación ciudadana y la rendición de cuentas institucional. Seguidamente se abordan los desafíos éticos y jurídicos que plantea el uso de IA en el ámbito parlamentario –como la opacidad algorítmica, los sesgos discriminatorios, la automatización excesiva de decisiones políticas, así como los problemas de privacidad y seguridad de los datos– y se proponen principios y directrices para un uso responsable (no discriminación, respeto a derechos fundamentales, supervisión humana, transparencia algorítmica, etcétera). Las conclusiones recalcan la necesidad de equilibrar las oportunidades de la IA para fortalecer el Estado de Derecho con salvaguardias firmes que eviten la erosión de los principios democráticos.

PALABRAS CLAVE: Inteligencia Artificial; Parlamento abierto; Transparencia; Participación Ciudadana; Rendición de Cuentas; Sesgos Algorítmicos; Ética de la IA.

Artificial intelligence as an ally for a more transparent and participatory open parliament

ABSTRACT: The rapid digitalization of society and the rise of artificial intelligence (AI) are profoundly transforming the legal-political ecosystem. We study the role of AI in an Open Parliament, describing examples from different countries where these tools increase legislative transparency, citizen participation, and institutional accountability. We then address the ethical and legal challenges posed by the introduction of AI in the parliamentary and democratic arena –such as algorithmic opacity, discriminatory biases, the over-automation of political decisions, as well as data privacy and security issues– and propose principles and guidelines for its responsible use (non-discrimination, respect for fundamental rights, human oversight, algorithmic transparency, etc.). The conclusions underscore the need to balance AI's opportunities to strengthen the Rule of Law with robust safeguards to prevent the erosion of democratic principles.

KEYWORDS: Artificial Intelligence; Open Parliament; Transparency; Citizen Participation; Accountability; Algorithmic Biases; AI Ethics.

Grupo de investigación Complutense Tecnología y Democracia. Se sigue la estructura de la presentación realizada por los autores en el Curso de Verano sobre *"Digitalización, IA y fuentes del Derecho"* (U. de Zaragoza, Jaca, 2025), ampliando cada apartado con literatura especializada y reflexiones interdisciplinarias.

La inteligencia artificial como aliada para un parlamento abierto más transparente y participativo

Rafael Rubio Núñez

Catedrático de Derecho Constitucional
Universidad Complutense de Madrid
España

Miguel Ángel Gonzalo Rozas

Director de Documentación, Biblioteca y Archivo
Congreso de los Diputados
España

CONTENIDOS: 1.- Introducción. 2.- IA y parlamento abierto. 3.- Desafíos éticos y jurídicos del uso de IA en el ámbito parlamentario. 4.- Principios y directrices para una IA parlamentaria responsable- 5.-Conclusiones. Bibliografía.

1. Introducción

La célebre máxima del pionero informático Ted Nelson en 1974 –“Si te interesa la democracia y su futuro, más vale que entiendas de computadores” (Nelson, 1974)– resume a un tiempo una constatación histórica y una intuición visionaria: el destino de las instituciones democráticas está y seguirá estando íntimamente ligado al desarrollo tecnológico. Medio siglo después, inmersos en la era de la digitalización masiva y la inteligencia artificial (IA), aquella advertencia adquiere plena vigencia. La democracia del siglo XXI se ve atravesada por algoritmos que mediatizan la información pública, por redes digitales que reconfiguran la participación ciudadana, y por sistemas automatizados que prometen optimizar (o sustituir) los procesos políticos que tradicionalmente correspondían a las personas. El diseño de la tecnología impacta y condiciona el diseño de la sociedad, planteando a juristas y politólogos dilemas inéditos sobre cómo preservar los valores democráticos en un entorno crecientemente algorítmico.

En este contexto, conviene analizar cómo la IA incide tanto en las fuentes formales del Derecho —en particular, la legislación y la jurisprudencia, pilares del Estado de derecho— como en los procesos e instituciones que las

producen, interpretan y aplican. A ello se suma otra intuición que hoy se ha consolidado empíricamente: la tecnología —el “código”— opera como un mecanismo de regulación de conductas. Como resume Lessig, “code is law” (Lessig, 1999, p. 6) y, en consecuencia, el control del código supone un ejercicio del poder y quienes escriben código “son cada vez más legisladores” al fijar por defecto opciones sobre privacidad, acceso o anonimato (Lessig, 1999, p. 60). El código, como la tecnología en general, no es neutral. De ahí la importancia de poder conocer su contenido, e incluso la identidad de quién lo diseña y los objetivos, fines y valores que están detrás. Esta normatividad técnica —visible, por ejemplo, en plataformas que ordenan el discurso público mediante algoritmos opacos— obliga a replantear categorías jurídicas clásicas: ¿puede la IA erosionar los mecanismos democráticos de producción normativa? ¿Se someten los algoritmos a escrutinio y control con garantías equiparables a las de las leyes que aprueban los parlamentos? Estas preguntas guían la investigación que sigue.

En este trabajo, que se inscribe en el debate emergente sobre IA y las instituciones democráticas se examinarán (i) las potencialidades de la IA para promover un parlamento Abierto, esto es, un Poder Legislativo más transparente, participativo y colaborativo con la ciudadanía; (ii) los desafíos éticos y jurídicos que conlleva la introducción de IA en los procesos parlamentarios y democráticos (sesgos, opacidad, responsabilidad, etc.) y (iii) los principios y directrices que deberían orientar un uso responsable de estas tecnologías en instituciones parlamentarias. El objetivo final es brindar un panorama comprensivo —a la vez actualizado y crítico— del estado del arte y las posibilidades del uso de este conjunto de tecnologías en sede parlamentaria identificando tanto las vías en que la IA puede contribuir con el Parlamento en fortalecer el Estado de Derecho (por ejemplo, facilitando el acceso a la información jurídica, aumentando la transparencia gubernamental, optimizando la toma de decisiones con base empírica) como las formas en que podría debilitarlo (v.g., introduciendo un sesgo en el proceso de decisión, concentrando poder en las empresas poseedoras de la tecnología, erosionando garantías fundamentales).

2. IA y parlamento abierto

2.1 El concepto de parlamento abierto en la era digital

El movimiento de parlamento abierto nació como extensión del paradigma de gobierno abierto, aplicando sus principios al poder legislativo (Vela Navarro-Rubio, Rubio, 2017a). Implica promover la transparencia, la

participación ciudadana y la colaboración en la actividad parlamentaria, apoyándose en las nuevas tecnologías para acercar el Parlamento a la sociedad (Rubio et al., 2014). Un parlamento abierto publica información clara sobre su trabajo (agendas, votaciones, iniciativas), rinde cuentas de sus gastos, facilita el acceso de la prensa y la ciudadanía, recibe insumos de la sociedad civil en los debates, e innova en mecanismos de participación (Gonzalo, 2018, p. 225). En esta evolución institucional se transita del parlamento electrónico al parlamento digital "hasta llegar al Parlamento Abierto, entendido como el impulso de la participación y la transparencia en la institución" (Rubio Núñez, 2022, p. 9)

La digitalización de las instituciones parlamentarias ha facilitado enormemente estos objetivos: desde la transmisión en vivo de sesiones hasta la puesta a disposición de la sociedad de bases de datos legislativas online y portales de datos abiertos (Vela Navarro-Rubio, Rubio, 2017b). Sin embargo, a pesar de los avances, la complejidad y volumen de información parlamentaria (centenares de proyectos, miles de enmiendas, millones de palabras en diarios de sesiones) han hecho que la digitalización no sea suficiente planteando el reto de hacer verdaderamente accesible y comprensible la información parlamentaria para el público y convertir esta información en un instrumento de participación. Frente a estos retos la inteligencia artificial ofrece soluciones prometedoras, pues puede procesar automáticamente documentos, detectar conexiones, resumir contenidos y atender consultas que manualmente serían inviables.

Así, un parlamento abierto en el siglo XXI puede valerse de la IA para profundizar su apertura a la sociedad. Pero también enfrenta el desafío de lograr que esa incorporación de IA sea coherente con los valores democráticos (evitando sesgos, opacidad o desigualdad). Muchos parlamentos del mundo están apenas explorando estas posibilidades; otros más avanzados sirven de referencia. En esta labor organizaciones como la Unión Interparlamentaria (IPU) está ejerciendo el liderazgo y, por ejemplo, en 2024 emitió un conjunto de directrices sobre IA en los parlamentos enfatizando que esta debe aumentar –no sustituir– la capacidad humana, y que su adopción requiere estrategias, gobernanza clara y enfoque ético, acompañando estas guías con casos de uso de IA en tareas parlamentarias concretas (IPU, 2024a).

En los apartados siguientes, examinaremos cómo la IA se aplica (o puede aplicarse) a las principales funciones de un Parlamento Abierto: (a) la transparencia legislativa (acceso a la información parlamentaria), (b) la participación ciudadana en el proceso legislativo, y (c) la rendición de

cuentas y el control sobre la función parlamentaria. Para cada dimensión, veremos ejemplos reales de iniciativas alrededor del mundo que ilustran el potencial de estas herramientas, así como las precauciones asociadas.

2.2 Transparencia legislativa aumentada por IA

La transparencia y el acceso a la información constituyen el primer eje de un parlamento abierto. Su objetivo es hacer que leyes, debates, votaciones y demás actividades legislativas sean públicas y realmente asequibles, hacia donde se plantea el I Plan de Parlamento Abierto del Congreso (Congreso de los Diputados, 2025). La IA puede potenciar notablemente este eje al automatizar la publicación, la clasificación temática y la búsqueda avanzada de los documentos parlamentarios.

Así lo han entendido un buen número de parlamentos en el marco de la UE. La adopción de la IA es desigual pero sostenida: según los resultados de una encuesta realizada por el ECPRD entre los parlamentos miembros y presentada en el Seminario del Centro en Bruselas en octubre de 2025, la mayoría de las Cámaras ya emplean IA en funciones administrativas (aprox. 30 parlamentos), un número menor en funciones legislativas (13 parlamentos), y alrededor de una cuarta parte combinan ambos ámbitos. Los casos de uso más comunes se concentran en las tecnologías de lenguaje: transcripción y traducción automática de debates o documentos (presentes en 29 parlamentos, ~76% de la muestra). Les siguen aplicaciones de ciberseguridad y desarrollo informático (18 parlamentos), chatbots o asistentes virtuales para apoyo al usuario (13), sistemas de clasificación documental (12), herramientas de participación ciudadana y parlamento abierto (7) y, en último lugar, el uso de IA para redactar borradores legislativos o generar enmiendas (solo 3 parlamentos, evidencia de que esta aplicación aún es incipiente).

En Alemania, el Bundestag, que ha dado un paso relevante al organizar su adopción de IA mediante un marco de gobernanza y mapeo de casos de uso —el *AI Cloverleaf Model*—, ya ha identificado más de 180 aplicaciones potenciales en áreas relacionadas con la transparencia como documentación, biblioteca, traducción y síntesis de información. Este enfoque evita “silos” y alinea la innovación con los principios democráticos, priorizando, entre otros, el análisis de contenidos y la recuperación inteligente de información para el trabajo legislativo y de apoyo. Además, el Bundestag ofrece un amplio catálogo de datos abiertos (plenos, diarios de sesiones, iniciativas y biografías de diputados) en formatos reutilizables (XML, JSON, CSV), y mantiene el sistema DIP de documentación e información parlamentaria, que indexa formal y temáticamente los materiales de

Bundestag y Bundesrat. Estas bases —gobernanza de IA y datos abiertos estructurados— crean condiciones propicias para motores de búsqueda más potentes y la clasificación semántica asistida por IA.

Una de las cámaras más avanzada en este terreno es la italiana que cuenta ya con un sistema de apoyo a la tramitación de enmiendas legislativas, que procesa las enmiendas presentadas a un proyecto de ley, las ordena automáticamente según el reglamento y calcula la similitud entre sus textos, detectando duplicados o propuestas muy similares (esta herramienta, llamada “Minerva”, se basó en un modelo lingüístico de código abierto entrenado en datos legislativos).

Finlandia ofrece un banco de pruebas especialmente fértil. El *watchbot* ciudadano Voitto (Yle News Lab) automatiza el seguimiento de la actividad parlamentaria y genera resúmenes/visualizaciones de votaciones a partir de datos del Parlamento, facilitando alertas personalizadas y productos periodísticos. En paralelo, *Lawradar* (Universidad de Turku) integra fuentes legales y políticas de todo el ciclo legislativo para seguimiento y análisis del avance de los proyectos de ley (Alvesalo-Kuusi, A, 2023). Además, desde 2023 *ParliamentSampo* publica más de un siglo de discursos plenarios del *Eduskunta* como datos enlazados y gráficos de conocimiento, con anotación semántica y clasificación temática mediante técnicas de procesamiento del lenguaje natural (PLN); el portal facilita búsquedas complejas y visualizaciones, abriendo nuevas posibilidades para la rendición de cuentas y la investigación histórica (Hyvönen, E., Sinikallio, L., Leskinen, P., Drobac, S., Leal, R., La Mela, M., Tuominen, J., & Poikkimäki, H., 2024).

Suecia ha impulsado la calidad de las transcripciones con RixVox, un corpus de 5.500 horas de audio de debates del *Riksdag* alimentado con las transcripciones oficiales (*riksdagens protokoll*) y enriquecido con metadatos (género del orador, distrito, etc.) (Rekathati, F. / KBLab, 2023). Este recurso —desarrollado por KBLab, el laboratorio de datos e inteligencia artificial de la Biblioteca Nacional de Suecia— ha servido para entrenar y evaluar modelos de reconocimiento automático del habla y de identificación de oradores, permitiendo ajustar el audio con el texto y una búsqueda mucho más ajustada dentro de los contenidos parlamentarios. Combinado con el portal de datos abiertos del *Riksdag* (API y datasets), el ecosistema facilita transcripciones rápidas y búsqueda por palabra/frase en grandes volúmenes de intervenciones.

En Eslovenia, el ecosistema público de tecnologías del lenguaje ofrece servicios de reconocimiento del habla en esloveno (por ejemplo, *Razpoznavnik*), y la práctica institucional de la Asamblea Nacional distingue

entre un registro rápido y un registro verificado de las sesiones, lo que evidencia esfuerzos por mejorar la documentación accesible y su calidad; estas bases técnicas y metodológicas se están aprovechando para agilizar transcripciones y enriquecer los corpus parlamentarios.

Noruega, por su parte, ha desplegado el proyecto StorSak en el *Storting* para gestionar de principio a fin la producción documental y los procedimientos parlamentarios, explorando el uso de aprendizaje automático/IA —especialmente en el tratamiento de metadatos y la categorización temática de documentos y expedientes—(Wahl, T., 2024).

También fuera de Europa se ensayan soluciones con clara vocación de apertura. En Singapur, Pair Search —un buscador potenciado con IA— facilita rastrear décadas de diarios de sesiones con mayor pertinencia que los motores centrados en las palabras clave y ha sido presentado por el propio Parlamento como un salto en accesibilidad pública (The Straits Times, 6 de mayo de 2024; Parliament of Singapore, 13 de agosto de 2024). Más que una mejora incremental, esta herramienta utiliza técnicas avanzadas de búsqueda con inteligencia artificial que superan los sistemas basados únicamente en coincidencias de palabras clave tales como la recuperación semántica, que interpreta el significado de las consultas más allá de las palabras exactas, y un ranking contextual, que ordena los resultados según la relevancia del contenido en función del contexto del debate, acercando así registros complejos a audiencias no técnicas.

El acceso conversacional a fondos y expedientes parlamentarios es otra buena muestra de las posibilidades que se presentan a los Parlamentos. En el Parlamento Europeo, los Archivos Históricos han lanzado “Ask the EP Archives”, un servicio que permite “chatear” con documentos a través de modelos generativos y técnica RAG, abriendo a públicos no especializados un acervo que, sin mediación técnica, sería opaco o difícil de recorrer (European Parliament, s. f.). La herramienta, pensada para preguntas del tipo “¿quién fue Simone Veil?” o “¿qué fue el Tratado de Maastricht?”, no sustituye la lectura crítica, pero reduce barreras de acceso y mejora la accesibilidad de investigadores y ciudadanos. El Parlamento Europeo está integrando la IA tanto en funciones parlamentarias nucleares (analizar votos, procesar enmiendas) como en proyectos innovadores para explorar nuevas capacidades (modelos generativos).

Ese patrón —bajar barreras de entrada mediante procesamiento del lenguaje natural— se repite en cámaras nacionales. En 2025, la Cámara de Diputadas y Diputados de Chile presentó ArChileBot, un asistente conversacional que permite consultar, en lenguaje cotidiano, el acervo legislativo y documental

de la Corporación (Carmona Aguirre & Sánchez Rivera, 2025). La iniciativa se inspira en ArchiBot del Parlamento Europeo (Ask the EP Archives), que aplica enfoques de generación aumentada con recuperación (RAG) para responder con base en documentos oficiales y acompañar las respuestas de citas verificables. ArChileBot adopta esa lógica: traduce preguntas informales ("¿qué se debatió sobre X en los últimos cinco años?") a búsquedas estructuradas sobre fondos bajo control institucional, devuelve los documentos que fundamentan la respuesta y ofrece filtros avanzados por tipo de pieza, fechas o materias. Con ello, el sistema produce itinerarios de búsqueda reproducibles y verificables: reproducibles, porque los pasos (consulta en lenguaje natural → equivalentes de búsqueda y filtros aplicados → conjunto de documentos resultante) pueden repetirse y obtener el mismo recorrido; y verificables, porque cada afirmación está trazada a sus fuentes primarias mediante enlaces y referencias a los documentos oficiales. El efecto no es solo una mejora incremental: acerca archivos complejos a audiencias no técnicas, refuerza la transparencia y acelera la investigación aplicada sobre leyes, debates y otros materiales parlamentarios.

La IA no solo abre el archivo, también sirve para facilitar la participación y la colaboración en curso. La IPU documenta usos que traducen preguntas en lenguaje ordinario en consultas SPARQL sobre datos abiertos parlamentarios —por ejemplo, en el Senado italiano—, de modo que cualquier persona pueda consultar el grafo de conocimiento sin conocimientos técnicos (p. ej., "¿qué comisiones debatieron el proyecto X y cómo se votó en el pleno?"). Aquí "interrogar ontologías legislativas" significa realizar consultas sobre un modelo formal (ontología) que define entidades como leyes, sesiones, votos, diputadas y comisiones, y las relaciones entre ellas; al ejecutar la consulta en el sistema SPARQL del parlamento, el sistema devuelve resultados precisos y trazables a los documentos oficiales.

En paralelo, otros casos recogen la asistencia automática para transcribir y subtitular procedimientos (p. ej., Cámara de los Comunes de Canadá), con beneficios de accesibilidad y reducción del tiempo de publicación de las actas (IPU, 2024b). En todos estos casos, los modelos de lenguaje hacen de puente entre corpus parlamentarios y usuarios no expertos frente a las barreras que genera el uso de un vocabulario jurídico y técnico especializado que resulta en ocasiones difícil de comprender.

El balance común de estas experiencias es nítido. La aplicación de IA mejora las formas de acceso a la legislación y a los expedientes; facilita la creación de nuevos modelos de buscadores como asistentes de búsqueda contextuales y semánticos, que superan el modelo textual basado en

palabras clave; permite la transcripción automática de plenos y comisiones con posibilidad de análisis posterior; y ofrece capacidades de anotación semántica —esto es, añadir a cada intervención y documento metadatos normalizados que identifican de forma inequívoca quién interviene (persona y cargo), en qué órgano, sobre qué materia o norma (con su identificador persistente), en qué fase del procedimiento y con qué resultado (p. ej., votación), además de relaciones como propone, enmienda, debate o vota— junto con visualizaciones que, gracias a ese marcado, convierten el archivo legislativo en un bien público comprensible, navegable y reutilizable.

Con todo, siguen siendo prudentes dos advertencias: combinar la IA con revisión humana cuando la precisión es crítica (p. ej., transcripción taquigráfica) y acompañar la apertura de datos con mediación informativa (resúmenes y explicaciones en lenguaje claro), algo en lo que la IA también puede servir de ayuda, para que la transparencia sea efectiva y útil para la ciudadanía.

2.3 IA para la participación y colaboración ciudadana

La participación ciudadana en la función legislativa también se está reconfigurando por obra de la IA. Allí donde antes los parlamentos podrían verse desbordados por el volumen, la heterogeneidad y la repetición de aportaciones públicas (Gonzalo, M.A et al, 2021), hoy es posible agrupar, sintetizar y visualizar miles de contribuciones en tiempos compatibles con el calendario parlamentario y la capacidad de sus señorías. Las guías y casos de uso compilados por la Unión Interparlamentaria muestran precisamente este desplazamiento: de un modelo artesanal y reactivo a flujos de trabajo donde el análisis automatizado de grandes corpus de aportaciones ciudadanas, la consulta en lenguaje natural y la transcripción asistida por IA sirven de soporte a formas de participación más informadas y donde las instituciones pueden interactuar con la sociedad, más allá de interlocuciones meramente formales o protocolarias (Inter-Parliamentary Union [IPU], 2024b).

La estandarización técnica refuerza esta promesa y la enlaza con la participación y la colaboración. Cuando los expedientes se publican en Akoma Ntoso (AKN) —estándar XML de OASIS para documentos legislativos que define estructura, metadatos y identificadores persistentes a nivel de artículos, disposiciones y versiones— las capas de IA (consultas en lenguaje natural, resúmenes, detección de cambios) se integran con menos fricción y con mayor interoperabilidad futura. Al existir un formato común y estable:

- la participación mejora, porque la ciudadanía y la prensa pueden buscar, comparar y citar pasajes concretos (por ejemplo, seguir qué cambió entre dos versiones) de forma reproducible;
- la colaboración entre cámaras, bibliotecas y archivos se facilita, ya que todos comparten anclas y metadatos compatibles, lo que permite reutilizar flujos de trabajo, herramientas y conjuntos de datos;
- y los chatbots y asistentes de búsqueda funcionan mejor: el modelo puede recuperar el fragmento exacto (RAG), explicar de dónde sale la respuesta con citas verificables y detectar cambios para evitar alucinaciones sobre textos desactualizados. Así, prototipos como chatbots documentales, buscadores semánticos o anotación automática no quedan encapsulados, sino que se proyectan en un ecosistema compartido y auditable.

En Brasil, la Cámara de Diputados ha diseñado un caso de uso de IA para ampliar la participación pública mediante el análisis automatizado de opiniones ciudadanas sobre proyectos de ley (Cámara dos Deputados de Brazil, 2024). El sistema reúne las aportaciones recibidas por encuestas y otros canales, las divide en frases y las transforma en representaciones numéricas que permiten agrupar mensajes similares por significado. A partir de ahí, clasifica la posición de cada intervención (a favor o en contra) y analiza su tono (positivo, negativo o neutro). Las diputadas y los diputados, así como el personal de comunicación, pueden seleccionar un expediente concreto y explorar los principales grupos de argumentos en listados y vistas sencillas (nubes de palabras y mapas), ajustar cuántos grupos desean ver y corregir resultados; esas correcciones alimentan un ciclo de mejora continua del sistema. El flujo también contempla la integración con herramientas de moderación de comentarios y con módulos de analítica y elaboración de informes. Para hacerlo posible se necesita, por un lado, una base de datos que relacione cada comentario con su proyecto de ley y, por otro, flujos de procesamiento que indexen el contenido y generen vectores semánticos (las representaciones numéricas mencionadas), además de mecanismos de seguimiento del rendimiento y la calidad. Cuando estos sistemas funcionan bien, se reduce el tiempo de análisis y mejora tanto el volumen como la calidad de las aportaciones de quienes los usan. El objetivo declarado es pasar de una lectura manual costosa —a veces materialmente inviable por la cantidad de comentarios— a una visión estructurada y trazable de los argumentos ciudadanos, de modo que la “señal” deliberativa llegue oportunamente a comisiones y ponencias.

Este potencial conlleva condiciones para que la participación no derive en una “participación simulada”. Las directrices de la Westminster Foundation

for Democracy recomiendan, para proyectos de IA en parlamentos, salvaguardas de trazabilidad (qué datos alimentan al sistema y con qué sesgos), auditoría de modelos, supervisión humana significativa y, sobre todo, mecanismos de retorno que expliquen cómo se han incorporado las contribuciones ciudadanas a las decisiones (Fitsilis/WFD, 2024). Dicho de otro modo: sin gobernanza de datos y de modelos, la apertura se vuelve fachada; con ella, la IA puede ampliar de veras el perímetro deliberativo. Como recuerda una evaluación reciente, “un Congreso inclusivo, responsable, transparente, accesible y receptivo es clave en la construcción de una sociedad democrática madura” (Rubio Núñez, Marañón Martín, & Gonzalo Rozas, 2021, p. 269).

2.4 Rendición de cuentas y control con herramientas de IA

La rendición de cuentas parlamentaria exige que los representantes expliquen y asuman sus decisiones y el uso de recursos ante la ciudadanía, apoyados por controles internos y externos capaces de prevenir abusos (Villoria Mendieta, 2020). La IA puede reforzar este ecosistema de control al proporcionar una “lupa digital” tanto a las instancias institucionales (tribunales de cuentas, contralorías, comités de ética) como a la sociedad civil (periodistas, organizaciones anticorrupción y ciudadanía organizada). El caso brasileño de *Operação Serenata de Amor* es ilustrativo: su *bot* Rosie analizó automáticamente los reembolsos de gastos de los diputados, cruzándolos con otras fuentes (fechas, lugares, conceptos) para detectar anomalías y emitir alertas públicas que generaron presión social y provocaron la devolución de gastos no justificados. La evaluación académica del proyecto documenta 629 reembolsos sospechosos asociados a 216 parlamentarios por más de 370.000 reales (Coutinho, 2021, párrs. 114–118); el Banco Mundial lo ha señalado como un hito de social *accountability* potenciada por datos abiertos e IA (Cordova & Gonçalves, 2019a, 2019b). Colectivos cívicos están usando herramientas automatizadas que, con aprendizaje automático, detectan señales de alerta en contratos, subvenciones y declaraciones patrimoniales. El sistema agrupa indicios — importes atípicos, adjudicaciones repetidas, empresas sin trayectoria— y ordena los expedientes para que la revisión humana se centre donde más falta hace. (Open Contracting Partnership, 2024; De Michele, 2022; World Bank, 2021; Salazar et al., 2024; Decarolis et al., 2022).

Dentro de los propios parlamentos, la IA también puede ayudar a monitorear la integridad al relacionar información dispersa –por ejemplo, comparar pautas de voto con declaraciones de intereses o con donaciones registradas públicamente– y señalar posibles conflictos que un comité de ética deba

revisar. Varias organizaciones recomiendan mejorar la calidad y estandarización de esos registros (declarante, clientes, sectores, cuantías) para habilitar análisis automatizados y sanciones efectivas en caso de incumplimiento. En el ámbito europeo, los informes recientes de Transparencia Interancional reclaman formularios más estructurados y controles más exigentes sobre empleos y actividades secundarias de los eurodiputados, como condición para una supervisión analítica efectiva (Transparency International EU, 2024; 2024b). En la misma línea, el Parlamento Europeo y su servicio de estudios han compilado un conjunto de buenas prácticas en transparencia e integridad que refuerzan la trazabilidad de intereses y la *accountability* (Vidačak, 2023). Aun cuando el uso de IA para correlacionar votos e intereses está en fase incipiente, la normalización y apertura de datos es el prerequisite técnico para que estos análisis sean posibles a escala.

3. Desafíos éticos y jurídicos del uso de IA en el ámbito parlamentario

La incorporación de la inteligencia artificial en los procesos democráticos plantea una serie de desafíos éticos y jurídicos que, aunque afectan también al gobierno y a la Administración pública, requieren atención específica en el contexto concreto del Parlamento.

3.1 La opacidad algorítmica

La opacidad algorítmica alude a la dificultad de entender cómo un modelo de IA —especialmente los de aprendizaje automático— llega a sus resultados o recomendaciones; de ahí la exigencia de transparencia y explicabilidad, que supone “proporcionar información suficiente para que las partes afectadas puedan comprender cómo funcionan los sistemas de IA [...] y [...] cuestionar sus resultados” (Rubio Núñez, 2025, p. 85). Muchas de las tecnologías que utilizan IA son esencialmente cajas negras: incluso sus propios desarrolladores no pueden explicar fácilmente por qué una red neuronal clasificó un texto de cierta manera o por qué un sistema de recomendación priorizó un elemento sobre otro. Esta falta de explicabilidad choca frontalmente con la cultura de transparencia y publicidad que debe reinar en las instituciones democráticas. Si un parlamento empieza a usar algoritmos para, digamos, gestionar correspondencia ciudadana o priorizar enmiendas, pero no puede explicar el criterio cuando se le pregunte, estaría violando el principio de motivación de los actos públicos. En esta línea, Cotino subraya que «...los sistemas de aprendizaje no pueden incorporarse en el sector público si no se puede obtener una motivación comprensible en lenguaje natural» (Cotino Hueso, 2023, p. 49). En palabras de Rubio, “los

algoritmos se han convertido en el «aparato disciplinario de nuestro tiempo» y, como tal, es necesario reformar su comprensibilidad para que las partes interesadas puedan tener claridad y estar seguras de su funcionamiento ético, responsable y políticamente neutral" (Rubio et al., 2024, p. 312).

Por ello, cualquier aplicación de estas tecnologías debe venir acompañada de soluciones para la transparencia algorítmica, tanto de puertas hacia afuera (rendición de cuentas externa), como internamente, garantizando que parlamentarios y funcionarios puedan entender los sistemas que utilizan para evitar que sus usuarios lo apliquen sin conocer su fiabilidad o sesgos. Algunas opciones que se están aplicando ya pasan por utilizar modelos interpretables (preferir IA sencillas, como árboles de decisión, que permiten seguir la lógica, en lugar de *deep learning* opaco, al menos para decisiones sensibles); exigir a los proveedores de IA desgloses de sus algoritmos (acceso al código o al menos a descripciones técnicas); o implementar herramientas de *explainable*. Al que generen explicaciones aproximadas de las decisiones (por ejemplo, métodos *SHAP/LIME* que indican qué variables pesaron más en una predicción). Un punto clave, común a todas ellas, es documentar cómo funcionan las herramientas de IA usadas en parlamento, con información accesible no sólo a expertos sino a los órganos de supervisión e incluso al público cuando corresponda. En ese sentido IPU (2024c) sugiere que los parlamentos publiquen notas técnicas sobre cada solución de IA adoptada: qué hace, con qué datos, y qué métodos de control se aplican, mientras se aboga por programas de alfabetización algorítmica dentro de los parlamentos.

3.2 Sesgos y discriminación algorítmica: riesgos para la equidad democrática

Los sesgos en IA constituyen uno de los problemas éticos más documentados. Estos contribuyen a la consolidación de errores atávicos y suponen un obstáculo para que el Parlamento pueda adaptarse al cambio social y liderar su progreso. Como advierte Rubio, "otro aspecto preocupante del uso de la IA en la política es su capacidad para facilitar prácticas de acoso y discriminación. Las plataformas digitales pueden amplificar discursos de odio y violencia, creando entornos hostiles que disuaden la participación cívica y democrática. Este fenómeno no solo afecta a los individuos directamente atacados, sino que también deteriora la calidad del debate público y la cohesión social. Además, la manipulación algorítmica puede romper la neutralidad político-ideológica en la jerarquización de resultados de motores de búsqueda, feeds de usuarios y sugerencias de contenidos, perjudicando así a candidatos vinculados a grupos vulnerables o minoritarios

y favoreciendo la difusión de contenidos prejuiciosos o estereotipados" (Rubio et al., 2024, p. 20).

Los sistemas de IA aprenden de datos históricos; si esos datos arrastran prejuicios o desigualdades, la IA tenderá a reproducirlos o incluso amplificarlos. En un contexto parlamentario, esto podría traducirse en resultados discriminatorios al procesar información o interactuar con el público. Por poner un ejemplo, un asistente virtual ciudadano entrenado mayoritariamente con preguntas de residentes urbanos podría, sin querer, proveer respuestas menos completas o empáticas a consultas de residentes rurales o de grupos étnicos con menor presencia en el conjunto de entrenamiento. En el mismo sentido, un algoritmo que analice comentarios en consultas públicas podría ignorar sistemáticamente cierto vocabulario usado por minorías, concluyendo erróneamente que sus temas no son relevantes. Estos sesgos algorítmicos atentan contra el principio democrático de representatividad equitativa: todas las voces deben ser escuchadas con igual peso. Si la IA silencia algunas, es un fallo grave, y si lo hace sin que se pueda apreciar que lo ha hecho, resulta todavía más grave.

Por otro lado, existen sesgos ideológicos, que afectan a los criterios de selección de la información y la prioridad que se le da a la misma. Imaginemos una IA que clasifique automáticamente peticiones ciudadanas por tema y urgencia. Si fue entrenada con datos donde peticiones sobre cierto tema (ejemplo: cambio climático) recibían menos atención, podría darles menor prioridad futura, perpetuando la marginación de ese tema. De esta forma, la IA podría favorecer inadvertidamente ciertas ideologías o agendas simplemente reflejando el statu quo, en actos parlamentarios como comparecencias, discriminando opiniones minoritarias y privándolas de la visibilidad necesaria para participar en el debate público.

Un principio central es que la igualdad ante la ley debe trasladarse a igualdad ante el algoritmo. Es decir, la IA parlamentaria no debe introducir tratamientos diferenciados injustificados hacia personas, colectivos o ideas.

Para mitigar sesgos, se plantean varias estrategias:

Directrices éticas específicas. Desde el diseño es posible prevenir para que el algoritmo no use determinadas variables sensibles (género, raza) a menos que sea para corregir un sesgo.

Inclusión en los códigos éticos (ver apartado 4.5) del principio de no discriminación. Por ejemplo, si un parlamento lanza una plataforma de participación moderada por un sistema de IA, el código debería exigir

explícitamente que la IA trate todas las aportaciones con los mismos criterios, sin sesgar por origen, lenguaje o ideología de quien opina.

Detección y corrección activa. Cada sistema de IA debe testar sus sesgos antes de ser adoptado. Por ejemplo, darle inputs de distintos grupos (mujeres vs hombres, mayorías vs minorías) y verificar que los outputs no difieran injustificadamente. Y en caso de que se detecten sesgos, ajustar el algoritmo o los datos que lo alimentan.

Diversificar datos de entrenamiento. Estos deben incluir muestras representativas de todos los segmentos poblacionales relevantes (distintas regiones, lenguajes, grupos étnicos, etc.) con distintos criterios, no sólo el sociológico. Si se detecta subrepresentación, será necesario complementarla con datos sintéticos o *oversampling*.

Técnicas de *debiasing* algorítmico. Hoy existen métodos para re-entrenar modelos imponiendo equidad (por ejemplo, en un clasificador, agregar penalizaciones si la tasa de error difiere entre grupos).

Revisión humana plural. La evolución de estos instrumentos debe contar con expertos en derechos civiles o representantes de minorías, que puedan señalar sesgos que a un programador se le escapan.

En suma, los sesgos algorítmicos son combatibles pero requieren una atención proactiva. Dejarlo al azar sería irresponsable. Se requiere dotar a los parlamentos de capacidad técnica o alianzas con instituciones académicas para auditar sus IAs continuamente. También la legislación general está previendo que sistemas en sector público se consideren de alto riesgo, obligando a evaluaciones de impacto algorítmico antes de usarse. Esto encaja con la recomendación de hacer un análisis de impacto ético previo a cualquier despliegue de IA parlamentaria. En dicho análisis se identifican posibles sesgos discriminatorios y se establecen salvaguardas para evitar violar la igualdad y no discriminación.

3.3 Automatización de decisiones políticas: dilemas de legitimidad

La automatización de decisiones políticas provoca tensión entre los principios de eficiencia y legitimidad democrática. En palabras de Rubio, Franco Alvim y de Andrade Monteiro, la automatización "impulsada por IA, [está] aumentando el alcance y la eficiencia del proselitismo electoral", pero "el modelo emergente afecta a aspectos centrales de la legitimidad democrática" (Rubio et al., 2024, p.307). Si esto plantea problemas a la democracia en general supone un cuestionamiento directo a la lógica

parlamentaria, socavando los principios de representación y de deliberación que sustentan el modelo del parlamento.

La representación, a lo largo de la historia, ha buscado siempre garantizar la participación de la sociedad en la toma de las decisiones públicas y el control periódico del cumplimiento de esta función. A través de la misma, los representantes públicos tratan de reproducir las ideas e intereses de quienes los han elegido, en la confianza de que la contraposición de argumentos, bajo la premisa del pluralismo político, permitirá llegar a decisiones que, además de resultar beneficiosas para la sociedad, representen su posición política de manera equitativa. Como sintetiza Manin, desde su invención el gobierno representativo descansa en principios como la elección periódica, la libertad de opinión de los gobernados y el debate público; en su formulación: "quienes gobiernan son nombrados por elección con intervalos regulares" (Manin, 1998, p. 14). A través de esta los representantes públicos tratan de reproducir las ideas e intereses de aquellos que les han elegido en la confianza de que la contraposición de argumentos, bajo la premisa del pluralismo político, permitirá llegar a decisiones que además de resultar beneficiosas para la sociedad, representan su posición política de manera equitativa.

De esta manera, en el parlamento, la representación necesita de la deliberación que permite ponderar valores, representar intereses diversos y llegar a acuerdos. Son tareas cargadas de juicio subjetivo, de debate normativo, donde no existe una "respuesta correcta" calculable. Si se intenta delegarlas a una IA, se corre el riesgo de desnaturalizar el proceso. Por ejemplo, supongamos un algoritmo que priorice qué enmiendas a un proyecto de ley son más relevantes, basándose en similitud de texto o frecuencia de aparición de ciertos términos. Podría dejar fuera enmiendas que, aunque menos "populares" en texto, representan visiones minoritarias importantes. O priorizar enmiendas de manera que refleje un criterio tecnocrático (ej. descartando las muy ideológicas). En todo caso, estaría filtrando el debate según un patrón que dejaría al margen la representación y la deliberación, promoviendo una visión autoritaria, en el que la intermediación institucional sería sustituida por una intermediación algorítmica.

Estudios recientes, sobre la probabilidad de elegir libremente frente a las propuestas de la IA, ponen de manifiesto que el riesgo del "piloto automático" legislativo es real. Si los parlamentarios se vuelven meros validadores de lo que la IA sugiere, la política se deshumaniza. Se perderían matices, negociaciones creativas, compromisos emergentes de discusiones

cara a cara. Además, la responsabilidad política se diluye: ¿a quién culpar si una decisión polémica resultó básicamente de una recomendación algorítmica? Los representantes podrían alegar que confiaron en la herramienta, esquivando rendir cuentas. Eso sería inaceptable en democracia, donde los representantes son elegidos para asumir responsabilidad, no para transferirla a una máquina.

Para enfrentar estos dilemas, es necesario definir límites claros a la automatización y mantener siempre el componente humano en la toma de decisiones. Como advierten Rubio, Franco Alvim y de Andrade Monteiro, "el punto de partida radica en reconocer la centralidad del ser humano en el debate sobre la IA: la IA debe estar al servicio de la humanidad, y no al revés" (Rubio et al., 2024, p. 84). A partir de ese principio, las buenas prácticas recomiendan circunscribir la IA a funciones de soporte técnico o informativo, evitando delegar en sistemas automatizados decisiones que exigen juicios de valor o conciliación de intereses; además, "debe facilitarse información suficiente para que puedan explicarse los resultados de estos sistemas", favoreciendo la transparencia y la rendición de cuentas (Rubio et al., 2024, p. 84) Es decir, la IA como asistente, no como legislador. De esta manera es necesario delimitar qué tareas nunca pueden ser objeto de automatización. La Constitución implícita de la democracia reserva las decisiones sustantivas a órganos representativos; delegarlas a un ente no responsable ante el pueblo sería una alteración de las reglas del juego democrático, independientemente de su inteligencia.

Además, dada la influencia que las labores de soporte pueden tener en la decisión final, incluso a estas funciones que permitirían el uso de la IA debería aplicársele el principio de supervisión humana. Un funcionario o representante debe validar críticamente cualquier resultado de la IA antes de tomarlo como base de decisión. En un código de conducta interno se podría estipular que "ningún informe o propuesta generada por IA será presentada oficialmente sin revisión y aval de personal humano responsable". Este es el llamado principio de "humans in the loop" explicitado en la literatura (Jobin et al., 2019), que se refleja también en la legislación (el Reglamento 2024/1689 del Parlamento Europeo y del Consejo, de 13 de junio de 2024 exige supervisión humana especialmente en contextos de alto riesgo, Art. 14).

Otro punto es la capacitación en alfabetización en IA para los propios parlamentarios y su personal. Deben comprender las limitaciones y alcances de estas herramientas para no otorgarles confianza ciega. Si un diputado piensa equivocadamente que "la computadora es infalible" cometerá el error

de abdicar su criterio. Es vital inculcarles que los algoritmos pueden errar, alucinar datos o reflejar sesgos de sus programadores. Con esa conciencia, usarán la IA como ayuda, pero manteniendo criterio. Como se sugiere: "la última palabra ha de seguir siendo humana".

Finalmente, podríamos también reforzar el papel de órganos deliberativos y escrutadores, por ejemplo, comités de ética o comisiones especiales que evalúen el impacto democrático de cada nueva IA introducida.

No se trata de velar exclusivamente por los resultados, al cuestionar sus pilares está en juego la propia supervivencia de la democracia. Para preservar la legitimidad es crucial no caer en la comodidad del automatismo. La IA puede agilizar, pero nunca debe substituir la deliberación. Un parlamento que se limitase a decir "sí a todo lo que el modelo sugiere" perdería la confianza ciudadana y llevaría a la sociedad a cuestionar la propia lógica de la representación democrática, ¿para qué elegir representantes, si al final decide un algoritmo? El equilibrio es delicado pero alcanzable con reglas claras y cultura institucional.

3.4 Exceso de confianza y sesgo de automatización

El peligro señalado en el punto anterior se amplifica al conocer la tendencia psicológica al exceso de confianza en resultados automatizados generados por la IA, fenómeno conocido como sesgo de automatización (*automation bias*). Este sesgo describe la tendencia a sobreestimar la exactitud de un sistema automatizado y aceptar sus recomendaciones sin un escrutinio suficiente, lo que provoca errores por comisión (seguir un consejo erróneo) y por omisión (dejar de detectar un problema cuando la automatización falla) (Parasuraman y Manzey, 2010; Goddard, Roudsari y Wyatt, 2012).

En entornos clínicos, diversos estudios experimentales han mostrado que el consejo automatizado puede arrastrar decisiones correctas hacia decisiones erróneas. En un ensayo controlado sobre interpretación de electrocardiogramas (ECG), cuando se presentó un dictamen informático incorrecto, las personas participantes acordaron con ese dictamen en el 67,7% de las veces, lo que provocó una disminución de la exactitud global (Tsai, Fridsma y Gatti, 2003). En un estudio con más de nueve mil interpretaciones de electrocardiogramas, la presencia de diagnósticos automatizados erróneos redujo significativamente la exactitud de la interpretación humana (Bond et al., 2018). Fuera del ámbito médico, en la aviación, la investigación en factores humanos integra la complacencia con la automatización y el sesgo de automatización muestra que la interacción entre características personales, situacionales y de la automatización puede

mermar la vigilancia y favorecer la aceptación acrítica del consejo de sistemas automáticos (Parasuraman y Manzey, 2010).

En un contexto parlamentario, el sesgo de automatización podría manifestarse, por ejemplo, en los resúmenes de informes complejos, que tiende a asumirse como un resumen fiel y completo sin leer el original; o, si un modelo pronostica impacto económico positivo de un proyecto normativo, podría relajarse el debate técnico dando por válida la supuesta validación computacional. Esta relajación de la vigilancia crítica es problemática porque los sistemas de IA no son infalibles: pueden generar alucinaciones (información inventada), cometer errores sutiles o quedar desactualizados respecto de la realidad.

Algunos parlamentos ya han comenzado a detectar estos problemas. Por ejemplo, la Biblioteca del Congreso de Estados Unidos ha experimentado con IA para apoyar la descripción y la catalogación y concluye que, dado el nivel de calidad requerido, la salida generada por IA debe revisarse antes de publicarse; hoy no existen herramientas suficientemente fiables para operar sin supervisión, por lo que se prototipan procedimientos con persona en el bucle (Library of Congress Labs, 2024; Library of Congress, 2024).

Para reducir el riesgo de que en los parlamentos se confíe en exceso en los resultados que ofrecen los sistemas de inteligencia artificial, es necesario actuar en varios frentes que combinan la formación de las personas, la forma de trabajar y la propia cultura institucional.

La monitorización humana ha de ser activa: la IA es una herramienta que se equivoca y, por ello, debe someterse a verificación sistemática. Esto exige asignar tiempo, incentivos y recursos para la revisión y la resolución de discrepancias, así como responsabilidades claras sobre quién decide en última instancia.

En primer lugar, resulta clave invertir en formación y concienciación tanto de las y los diputados como de los equipos técnicos, mostrándoles ejemplos en los que la IA comete errores para que aprendan a mantener una actitud crítica y de vigilancia frente a sus resultados (Goddard et al., 2012). También es útil establecer procedimientos que obliguen a verificar de manera sistemática algunos de los resultados producidos por la IA, como puede ser el caso de la clasificación de peticiones ciudadanas, de modo que siempre pasen por la revisión de una persona distinta antes de que se adopte una decisión.

En el diseño de las herramientas conviene evitar que las interfaces transmitan una sensación de certeza absoluta, incorporando en cambio

indicadores de confianza o de incertidumbre que estén bien calibrados. Esto ayuda a que la dependencia respecto a la IA sea más equilibrada, aunque la utilidad de esos indicadores depende de la calidad de la calibración y del tipo de tarea en cuestión (Kunze, Gonzalez, Wiczorek y Bengler, 2019; Tejeda-Lemus, Kumar y Steyvers, 2023). Aunque es preciso advertir que, según estudios en otras áreas científicas, la transparencia, por sí sola, no garantiza la reducción del impacto del sesgo (Poursabzi Sangdeh, Goldstein, Hofman, Wortman Vaughan y Wallach, 2021).

Finalmente, es aconsejable fomentar una cultura del “doble chequeo” humano: si una persona asesora redacta un informe con apoyo de la IA, otra debería elaborar un resumen de manera independiente y luego comparar ambos resultados, asegurando así una mayor fiabilidad.

El sesgo de automatización es un riesgo silencioso que puede erosionar la calidad de las decisiones. Reconocerlo y contrarrestarlo es parte de una cultura institucional sana en la era de la IA. Los parlamentos deberían promover la máxima: “Confiar, pero verificar”. La IA puede resultar muy útil, pero no se debe confiar a ciegas en ella, del mismo modo que no se confía ciegamente en una única fuente de información sin corroborarla.

3.5 Privacidad y protección de datos personales

En la labor parlamentaria se manejan con frecuencia datos personales de ciudadanos (p. ej., peticiones, comparecencias, visitas). La introducción de herramientas de IA para la gestión de esos datos refuerza la obligación de velar por la privacidad y cumplir las normas de protección de datos. Principios como la limitación de la finalidad, minimización de datos, limitación del plazo de conservación y la integridad/confidencialidad deben guiar todos los tratamientos (RGPD, art. 5.1 b–f; responsabilidad proactiva del art. 5.2). En el caso del parlamento algunos de estos datos pueden afectar a categorías especiales relacionadas con la ideología o la orientación política a las que habría que aplicar las restricciones al tratamiento establecidas por el art. 9 (RGPD, arts. 6 y 9).

El uso de la IA no exige de anonimizar los datos personales, cuando sea posible y proporcional al fin. En este sentido, conviene evaluar si el algoritmo puede operar con datos anonimizados o, al menos, pseudoanonimizados. La antigua WP29 (hoy EDPB) recuerda los límites y riesgos de reidentificación en técnicas de anonimización; no toda desidentificación equivale a anonimato real (WP29, 2014). Además, el EDPB ha precisado en 2025 criterios técnicos y jurídicos para la pseudoanonimización eficaz (p. ej., separación del “secreto” y controles de acceso). (WP29, 2014; EDPB, 2025).

Antes de desplegar instrumentos de IA que utilicen datos personales, los parlamentos deberían realizar una Evaluación de Impacto relativa a la Protección de Datos (EIPD) cuando el tratamiento entrañe alto riesgo (RGPD, art. 35). La AEPD ha publicado guías prácticas y listados orientativos (art. 35.4 y 35.5), aplicables —por ejemplo— a tratamientos con biometría o perfilado a gran escala (AEPD, 2021; 2023).

La arquitectura de estas soluciones de IA debe incorporar protección de datos desde el diseño y por defecto (RGPD, art. 25) limitarse a recolectar solo los datos necesarios, restringir accesos, acotar plazos de conservación y exponer indicadores de incertidumbre cuando proceda.

El lugar donde se alojan y procesan los datos parlamentarios también es crítico. Las transferencias a terceros países deben cumplir el Capítulo V del RGPD y la doctrina del TJUE en Schrems II, que invalidó el antiguo Privacy Shield y exige garantizar un nivel esencialmente equivalente de protección mediante cláusulas y medidas suplementarias (EDPB 01/2020). Este contexto aconseja, cuando sea viable, alojar y procesar datos en la UE y bajo jurisdicción local, o instrumentar salvaguardas contractuales y técnicas robustas con verificación continua. (C-311/18 TJUE; EDPB, 2021).

El derecho de supresión (art. 17 RGPD) plantea retos cuando los datos han influido en modelos entrenados. La literatura técnica explora lo que denomina el *machine unlearning* para permitir "olvidar" selectivamente sin reentrenar de cero (Bourtoule et al., 2021; Ginart et al., 2019). Hoy por hoy, estas técnicas son prometedoras pero todavía complejas; la mejor práctica sigue siendo minimizar retenciones, documentar conjuntos de entrenamiento y mantener la capacidad de depuración de los datos fuente. (RGPD, art. 17; Bourtoule et al., 2021; Ginart et al., 2019).

Por último, para sistemas de alto riesgo en el sector público, el AI Act de la UE introduce —entre otras obligaciones— la evaluación del impacto en derechos fundamentales (FRIA) para determinados supuestos de despliegue por administraciones públicas; su entrada en vigor y calendario de aplicación están escalonados (véase art. 27 y cronograma). Algo que complementa, pero no sustituye, a la EIPD del RGPD.

En resumen, la IA no debe introducirse a costa de sacrificar derechos. Debe cumplir estrictamente las normas de datos, aplicar minimización y seguridad reforzada, y operar bajo la supervisión del DPD y de los órganos de control, con trazabilidad de decisiones automatizadas y mecanismos eficaces de rectificación y supresión.

3.6 Seguridad informática y resiliencia frente a ataques

La adopción de IA en sistemas parlamentarios, abre nuevos retos de ciberseguridad, dado que "la 'superficie de ataque' de una sociedad digital altamente interconectada será demasiado amplia para que los operadores humanos puedan defenderla manualmente" (Kissinger, Schmidt y Huttenlocher, 2021), ello obliga a automatizar parte de las funciones defensivas y a reforzar los controles institucionales también en el ámbito parlamentario. Además de los riesgos clásicos (intrusiones, ransomware, fuga de correos), aparecen riesgos específicos asociados a la IA.

Por un lado, la posibilidad de insertar determinados datos fabricados dentro de los datos de entrenamiento del sistema para sesgar resultados o degradar rendimiento (Biggio, Nelson & Laskov, 2012). También las pequeñas perturbaciones en las entradas (imágenes o texto) que pueden inducir predicciones erróneas que, como hemos visto, suelen ser recibidas con altos niveles de confianza (Goodfellow, Shlens & Szegedy, 2015, pp. 2-4; Wallace et al., 2019, pp. 2153-2156). Por último, pueden producirse la manipulación del flujo de información. Es verosímil que se intente inundar canales de participación automatizados con entradas sintéticas para "fabricar" mayorías artificiales o adulterar documentos en la realización de síntesis y resúmenes.

Aunque el uso de IA parlamentaria es emergente, sí existen precedentes de ciberataques a instituciones parlamentarias como el Bundestag que sufrió en 2015 una intrusión que afectó a su red y correos. El Stortinget (Parlamento noruego) notificó en 2020 acceso no autorizado a cuentas de correo y el Parlamento de Nueva Zelanda sufrió un ataque en 2021 atribuido por sus autoridades a un actor extranjero. Estos casos ilustran el nivel de amenaza al que ya están expuestos los legislativos.

La IPU recoge estas preocupaciones en sus Directrices para IA en parlamentos y propone controles técnicos, organizativos y humanos para sus sistemas de IA que fortalezcan la seguridad, como controles de integridad de datos y gobernanza del ciclo de vida de los mismos que incluye la ingesta validada, registros de procedencia, auditoría, mecanismos de entrenamiento adversarial o la monitorización de desvíos. Complementariamente, la Comisión Europea ha impulsado programas públicos de "bug bounties" —es decir, recompensas económicas a personas expertas que detectan y notifican vulnerabilidades de seguridad antes de que puedan ser explotadas— aplicados al software abierto utilizado por las instituciones europeas (programas EU-FOSSA y OSPO). Esta práctica, que combina transparencia tecnológica y colaboración ciudadana, resulta extrapolable a las plataformas cívicas y a los entornos digitales de los parlamentos, donde

podría contribuir a reforzar la seguridad y la confianza pública en sus infraestructuras digitales. En España, el Esquema Nacional de Seguridad (ENS) (RD 311/2022) fija principios, requisitos mínimos y auditoría de seguridad para sistemas del sector público y sus proveedores, aplicable también cuando se externalizan servicios de IA, que resulta de aplicación a la institución parlamentaria.

Para reforzar la seguridad digital en los parlamentos resulta recomendable adoptar una estrategia basada en varias capas de protección. Esto implica, por un lado, garantizar que la información esté siempre protegida mediante cifrado, tanto cuando se transmite como cuando se almacena, y acompañarlo de controles de acceso seguros, como el uso de contraseñas reforzadas y la verificación en dos pasos. También es importante llevar un registro de las actividades y repartir las responsabilidades para evitar fallos o abusos. A ello se suma la necesidad de revisar periódicamente los sistemas con auditorías y pruebas que permitan detectar posibles puntos débiles, así como mantener actualizados los programas y componentes de inteligencia artificial para corregir vulnerabilidades.

Otra medida esencial es optar por soluciones que puedan ser revisadas externamente y establecer procedimientos claros para informar y corregir fallos de seguridad, siguiendo las recomendaciones europeas. En algunos casos puede ser útil recurrir a programas de recompensas que animen a especialistas externos a identificar fallos, como ya han hecho algunos gobiernos. Junto a ello, conviene contar con planes de emergencia que incluyan copias de seguridad desconectadas y la capacidad de seguir trabajando manualmente si algún sistema de IA deja de funcionar. Finalmente, no hay que olvidar la formación del personal en buenas prácticas digitales, especialmente en la prevención del phishing, pues la experiencia demuestra que el factor humano suele ser el punto más vulnerable de la seguridad.

Junto a estos avances, conviene fijar límites y garantías. Las *Guidelines for AI in Parliaments* recomiendan auditorías periódicas de datos y modelos, informes de transparencia sobre sesgos y controles de calidad, y, cuando sea viable, preferencia por soluciones abiertas o auditables para permitir la verificación externa (Westminster Foundation for Democracy [WFD], 2025). En este sentido, abrir código o publicar información sobre los algoritmos empleados por los parlamentos –o, como mínimo, garantizar su auditabilidad independiente– es una buena práctica que reduce el riesgo de comportamientos anómalos no detectados.

Estos cambios obligan también a prestar atención a la seguridad de la información parlamentaria. Aunque no sea "transparencia" en sentido estricto, preservar la integridad de redes, documentos y comunicaciones es una condición de posibilidad de la accountability: si el expediente o el correo de un diputado se altera o se exfiltra, la cadena de custodia se rompe. Tras el ciberataque al Bundestag de 2015, la UE impuso sanciones a los responsables, subrayando la necesidad de capacidades de detección temprana (incluida la analítica basada en IA) para identificar phishing, intrusiones y movimientos laterales en redes legislativas (Council of the EU, 2020). Este tipo de defensa algorítmica es hoy práctica estándar en muchas administraciones y debe consolidarse en los parlamentos si se quiere proteger la trazabilidad de decisiones y la confianza pública.

La resiliencia parlamentaria exige integrar la IA en la estrategia global de ciberseguridad institucional, desarrollada habitualmente de manera integral por los Estados y que incluye inventario de activos, análisis de riesgos, controles proporcionales, pruebas periódicas y gobernanza clara. Con ello, se reduce la superficie de ataque y se protege la confianza ciudadana en la era digital.

4. Principios y Directrices para una IA Parlamentaria Responsable.

Ante los riesgos descritos, distintas instituciones nacionales e internacionales han formulado principios éticos y directrices sobre el uso de la inteligencia artificial en el sector público y, específicamente, en los parlamentos. Estas guías buscan asegurar que la adopción de IA se alinee con los valores democráticos y los derechos fundamentales, minimizando los impactos negativos.

4.1. Principios rectores: no discriminación, privacidad y derechos humanos

Diversos marcos éticos convergen en ciertos principios generales que deben regir cualquier uso de IA en la esfera pública. Tres de los más relevantes para el contexto parlamentario son: no discriminación, privacidad y respeto a los derechos humanos.

a) No discriminación.

Como ya se explicó, es indispensable evitar sesgos injustos. Este principio exige que los sistemas de IA no introduzcan tratos diferenciados injustificados hacia personas o grupos. En un parlamento, significa, por ejemplo, que una plataforma de participación ciudadana que utiliza la IA valore todas las aportaciones con los mismos criterios, sin favorecer u omitir sistemáticamente

ciertas procedencias o ideologías. Salvaguardar la no discriminación es esencial para respetar la igualdad ante la ley y los derechos civiles. En coherencia con el encuadre de los derechos digitales propuesto por Tamara Álvarez Robles —que reclama que estos “conviertan al Estado en el obligado y custodio, a las compañías en las responsables y a los ciudadanos en sus titulares” (Álvarez Robles, 2022, p. 5)—, la adopción de IA parlamentaria debe plasmar esa triple asignación de deberes y garantías, de modo que la igualdad de trato sea medible, auditada y exigible.

Las directrices de la Unión Europea sobre inteligencia artificial incorporan este principio; por ejemplo, las Directrices Éticas para una IA Fiable elaboradas por el Grupo de Expertos de Alto Nivel en Inteligencia Artificial de la Comisión Europea destacan la equidad y la no discriminación como uno de los siete requisitos esenciales de una IA confiable, junto con la transparencia, la responsabilidad y la supervisión humana (High-Level Expert Group on Artificial Intelligence, 2019, pp. 11-13). Asimismo, la Declaración de la UIP de 2024 sobre IA y democracia (149ª Asamblea) recalca la inclusión y la equidad en el desarrollo y uso de estas tecnologías, reconociendo que la IA mal diseñada puede perpetuar prejuicios, discriminación y desigualdades. En otras palabras, tanto Europa como la comunidad interparlamentaria global coinciden en que la justicia algorítmica (*fairness*) es pilar esencial de la IA responsable (Inter-Parliamentary Union, 2024c).

b) Privacidad.

Como también hemos visto, los sistemas de IA manejan habitualmente datos personales (a veces altamente sensibles), por lo que es crucial proteger la privacidad individual. Cualquier uso de IA en un parlamento debe cumplir escrupulosamente las normas de protección de datos vigentes (por ejemplo, el RGPD en la Unión Europea). Esto implica utilizar solo los datos estrictamente necesarios para la tarea, recabar el consentimiento cuando proceda o basarse en habilitaciones legales claras, permitir a las personas ejercer sus derechos (acceso, rectificación, supresión de sus datos, oposición, etc.), y establecer medidas de seguridad robustas para prevenir filtraciones o accesos no autorizados. Además, se deben programar borrados regulares de datos personales una vez cumplida su finalidad. Para garantizar su cumplimiento algunos parlamentos cuentan con Delegados de Protección de Datos (como exige el

RGPD) que supervisan estos aspectos; su rol se extiende a la vigilancia de proyectos de IA internos. Por ejemplo, el Congreso de los Diputados en España cuenta con una Delegada de Protección de Datos encargada de velar por el cumplimiento de estas normas. En suma, la privacidad debe considerarse un requisito legal ineludible en cualquier iniciativa de IA: sin respeto a la protección de datos, no solo se vulnerarían derechos fundamentales, sino que también se minaría la confianza ciudadana en las instituciones.

c) Respeto a los derechos humanos y valores democráticos.

En última instancia, ningún despliegue de IA debería vulnerar libertades básicas (expresión, participación política, privacidad, debido proceso, etc.) ni ir en contra de los valores democráticos fundamentales. Más bien, la IA debe servir para promover los derechos: por ejemplo, facilitando el acceso a la información (derecho a saber) y la inclusión en la vida pública. Este principio, enmarcado en la noción de IA confiable (*trustworthy AI*), supone que la tecnología esté al servicio de las personas y del Estado de Derecho, nunca al revés. De ahí que documentos internacionales como la Recomendación de la UNESCO sobre la Ética de la IA (2021) o la Recomendación del Consejo de Europa sobre IA y derechos humanos (2020) enfatizan la centralidad del ser humano, la dignidad inherente de cada persona y la necesidad de control democrático sobre estas herramientas. En particular, la UNESCO subraya que “ningún ser humano ni comunidad humana debería sufrir daños o sometimiento [...] durante ninguna etapa del ciclo de vida de los sistemas de IA” y que “a lo largo de su ciclo de vida, los sistemas de IA deberían mejorar la calidad de vida de los seres humanos” (UNESCO, 2021, párr. 14).

Estos tres principios actuando en conjunto crean un marco claro: la IA parlamentaria debe ser justa (no discriminatoria), legal (respetuosa de la privacidad y las leyes) y centrada en el ser humano (respetando los derechos humanos y beneficiando a la sociedad). Por supuesto, no son los únicos principios relevantes (también están la transparencia, la seguridad, la rendición de cuentas, etc., que veremos enseguida), pero sí están entre los más vinculados a obligaciones jurídicas firmes.

4.2. Transparencia y explicabilidad de los algoritmos

Para garantizar los principios anteriores, resulta crucial el principio de transparencia algorítmica. Este se refiere a que los algoritmos y modelos de

IA usados en procesos parlamentarios sean lo más transparentes posible. En la práctica, esto implica documentar detalladamente cómo funcionan esas herramientas, qué datos usan para tomar decisiones, y compartir esa información con los órganos de supervisión internos e incluso con el público cuando corresponda.

La transparencia algorítmica facilita la auditoría independiente de las herramientas, permitiendo detectar sesgos o errores a tiempo. Por ejemplo, si un parlamento lanza un *chatbot* legislativo, podría acompañar su lanzamiento con la documentación técnica correspondiente, o incluso publicar parte del código describiendo el flujo de decisión y las fuentes de datos utilizadas (por ej., «entrenado con todas las leyes publicadas hasta 2024; actualizable mensualmente con nuevas leyes»), así como sus limitaciones conocidas. También se sugiere que los parlamentos mantengan un registro público de los sistemas de IA que utilizan, indicando su finalidad y características, a modo de “algoritmoteca”. Algo que en otros entornos como las ciudades (como Ámsterdam) han hecho al publicar un catálogo abierto de algoritmos municipales usados en la gestión pública.

Con transparencia, los ciudadanos y expertos pueden entender y confiar más en el uso IA en las instituciones públicas. Ahora bien, este principio debe balancearse con consideraciones de seguridad (no exponer detalles que faciliten usos maliciosos) y de propiedad intelectual en caso de software licenciado (lo que puede generar ciertos conflictos). Pero la tendencia actual es clara: más transparencia equivale a más confianza y menos posibilidades de abuso. España, a través de la Agencia de Protección de Datos, ha impulsado la idea de promover algoritmos explicables, y algunos instrumentos recientes (como la Carta de Derechos Digitales, 2021) recogen el derecho a obtener explicaciones de las decisiones automatizadas públicas, algo que ha sido confirmado por el Tribunal Supremo en el caso Bosco ¹ y por el TJUE en aplicación del artículo 15, apartado 1, letra h del RGPD, en los asuntos C-634/21 (SHUFA) de 7.12.2023 ² y C-203/22 de 27.2.2025

¹ Tribunal Supremo (Sala de lo Contencioso-Administrativo, Sección 3.ª), STS 119/2025, 11-IX-2025, ECLI:ES:TS:2025:3826, rec. 7878/2024

² TJUE, Sala Primera, sentencia de 7-XII-2023, OQ v. Land Hessen, C-634/21, ECLI:EU:C:2023:957 (SCHUFA Holding – Scoring)

(Dun & Bradstreet Austria)³. Este derecho se refuerza ahora más con el artículo 13.1 del Reglamento de Inteligencia Artificial⁴.

Junto a la transparencia se plantea la obligación de señalar el uso de IA cuando se produce este. Esto supone informar explícitamente cuando una tarea parlamentaria es realizada con ayuda de IA. Por ejemplo, si se emplea un sistema para clasificar correos ciudadanos o para generar borradores de informes, debe hacerse pública la utilización de este tipo de herramientas de IA mediante notas en el documento, comunicados de prensa o avisos en la web. Esta divulgación fortalece la confianza, pues evita la sensación de que la tecnología se usa de forma encubierta o sin control público. En definitiva, el parlamento no debe actuar con IA de modo oculto, sino de manera abierta y proactivamente informativa. Esto no quita legitimidad al proceso; al contrario, es reflejo de la honestidad que debe presidir la relación de confianza entre el Parlamento y la sociedad.

Además, la transparencia interna permite a los propios parlamentarios contar con insumos para la toma de decisiones informadas sobre la IA: sabrán qué riesgos corre su institución y cómo mitigarlos. Por tanto, entre los principios base de un eventual código ético del Parlamento debería figurar algo como: "El Parlamento publicará información sobre los algoritmos que use, su propósito, alcance y controles implementados, salvo que razones de seguridad nacional u otras excepcionales lo impidan. En estos casos se informará al menos a los órganos internos competentes, bajo deber de confidencialidad".

4.3. Supervisión humana permanente ("*human-in-the-loop*")

Ligado a lo anterior, un principio esencial es la supervisión humana permanente de los sistemas de IA. Como ya se argumentó, ningún sistema automático debería operar sin una instancia humana de control y validación en su ciclo de uso. Este principio consagra que el juicio humano prevalezca, evitando que un sistema actúe por su cuenta sin control humano. En la práctica parlamentaria, la supervisión humana se traduce en la intervención de una persona en la supervisión de cualquier proceso parlamentario, en el que se haya utilizado la IA para realizar ciertas tareas, antes de la adopción de decisiones políticas o administrativas basadas en ellos. Por ejemplo, si una IA genera un resumen de las enmiendas a un proyecto de ley, personal

³ TJUE, Sala Primera, sentencia de 27-II-2025, CK v. Magistrat der Stadt Wien, C-203/22 (Dun & Bradstreet Austria GmbH), ECLI:EU:C:2025:117

⁴ Reglamento (UE) 2024/1689 del Parlamento Europeo y del Consejo, de 13-VI-2024, por el que se establecen normas armonizadas en materia de inteligencia artificial (AI Act), art. 13(1) "Transparencia y suministro de información a los usuarios"; DOUE L (12-VII-2024)

parlamentario debería revisarlo antes de entregarlo a la comisión correspondiente, para asegurarse de que refleja fielmente su contenido. O si un algoritmo sugiere un orden del día "óptimo" para el pleno, la Mesa del Parlamento (o quien corresponda) debe evaluar esa sugerencia críticamente antes de adoptarla.

Este principio se conoce en la jerga como mantener a los "humanos en el bucle" (human-in-the-loop), y forma parte de casi todos los marcos éticos recientes (OCDE, UE, UNESCO, etc.). En la resolución de la UIP de 2024 ya mencionada, se hace énfasis en mantener la primacía del control humano en la deliberación y las decisiones parlamentarias (Inter-Parliamentary Union, 2024c). Para implementarlo, un código interno podría establecer roles claros: por ejemplo, designar responsables humanos de cada sistema de IA, que aseguren de la supervisión humana. También mecanismos de override que permita a estos responsables anular o modificar las propuestas de la IA si las consideran inadecuadas. De hecho, Reglamento Europeo de IA (RIA) prevé que los sistemas de alto riesgo tengan siempre la posibilidad de intervención humana hasta llegar a desconectar la automatización (Art. 14).

¿Por qué es vital esta supervisión? Ya se vio: por legitimidad democrática, por prevención de errores y sesgos, por adaptabilidad a casos particulares. Y, desde una perspectiva filosófica, porque reafirma la agencia humana en las instituciones democráticas. No queremos parlamentos pilotados en automático, sino asistidos por IA, pero donde las personas que desempeñan la representación legítima de la sociedad tengan la última palabra.

4.4 Mitigación de sesgos y evaluación de impacto algorítmico

Otra directriz fundamental es que cualquier código ético o protocolo debe contener procedimientos explícitos para detectar y mitigar sesgos en las soluciones de IA. Esto complementa el principio de no discriminación, llevándolo al terreno práctico. En concreto, se recomienda la realización de evaluaciones de impacto algorítmico antes de desplegar una nueva herramienta. Estas evaluaciones, semejantes a un "informe de impacto ambiental" pero aplicado a algoritmos, buscan identificar posibles efectos discriminatorios o riesgos para derechos fundamentales antes de que se produzcan. Pueden incluir pruebas con diferentes subgrupos, consultas a partes interesadas (por ejemplo, ONGs de derechos digitales) y análisis de escenarios negativos hipotéticos. Algunos países (Francia, Canadá) ya exigen algo similar para sistemas de IA en el sector público.

Asimismo, se sugieren auditorías periódicas de los sistemas para verificar que su propio funcionamiento no ha generado o amplificado sesgos que

originalmente habían pasado desapercibidos por su escaso impacto. Si se hallan sesgos –por ejemplo, que un algoritmo de análisis de texto ignore sistemáticamente ciertos dialectos, o que un modelo de resumen omita perspectivas minoritarias– se deben ajustar los modelos o los datos de entrenamiento para corregirlo. Adicionalmente, fomentar la diversidad en los equipos técnicos que desarrollan o supervisan estas IA ayuda a captar sesgos inadvertidos. Así, si el parlamento contrata personal o asesores en IA, debería procurar incluir diversidad de género, origen, disciplinas, etc., alineado con el principio general de inclusión. Los sesgos muchas veces pasan desapercibidos cuando todos los diseñadores comparten un mismo sesgo de base.

En resumen, es necesario examinar con lupa el algoritmo, antes, durante y después de su uso, y corregirlo si hace falta. Esto puede llevarse a cabo dentro del parlamento a través de un comité de ética digital que supervise estos aspectos, emitiendo recomendaciones y asegurando su cumplimiento.

Diversos parlamentos han institucionalizado órganos específicos para examinar el impacto de la inteligencia artificial y otras tecnologías emergentes, producir recomendaciones y alimentar con evidencia la toma de decisiones. En el ámbito europeo, el Parlamento Europeo constituyó el Comité Especial sobre Inteligencia Artificial en la Era Digital (AIDA), con mandato temporal para evaluar impactos sociales, económicos y éticos de la IA y proponer una hoja de ruta institucional (informe final con recomendaciones a la Cámara)⁵. En Finlandia, el Committee for the Future del Eduskunta funciona de manera permanente como think tank parlamentario: prospectiva científica-tecnológica, audiencias, dictámenes a otras comisiones y análisis de largo plazo para anticipar efectos de la innovación y orientar la agenda legislativa. En Francia, la Oficina Parlamentaria para la Evaluación de Opciones Científicas y Tecnológicas (OPECST) —órgano conjunto de la Asamblea Nacional y el Senado— está encargada de informar al Parlamento sobre las consecuencias de las opciones científico-técnicas; ha emitido informes monográficos sobre IA (por ejemplo, *Pour une intelligence artificielle maîtrisée, utile et démystifiée*) que combinan audiencias públicas, trabajo pericial y propuestas operativas. En el Reino Unido, la House of Lords creó una Select Committee on Artificial Intelligence (2017–2018) para examinar implicaciones económicas, éticas y sociales de la IA y formular recomendaciones; sus conclusiones —difusión

⁵ Parlamento Europeo — Special Committee on Artificial Intelligence in a Digital Age (AIDA), informe final (Ag-0088/2022): https://www.europarl.europa.eu/doceo/document/A-g-2022-0088_EN.html

de buenas prácticas, gobernanza y estándares— se convirtieron en referencia para el seguimiento parlamentario posterior.

Por su parte, en América, el Senado de Chile mantiene una Comisión de Desafíos del Futuro, Ciencia, Tecnología e Innovación, de carácter permanente, cuyo mandato es incorporar desafíos científico-tecnológicos al trabajo legislativo, promover debates e informes y transformar hallazgos en iniciativas; la IA figura entre sus líneas de estudio. La Cámara de Diputados de Brasil ha creado una Comisión Especial sobre Inteligencia Artificial para analizar el PL 2338/2023, celebrar audiencias públicas y presentar un parecer técnico-político sobre la futura ley de IA. Por su parte, la Cámara de Representantes de Estados Unidos estableció en 2024 una Bipartisan Task Force on Artificial Intelligence, con composición intercomités y el encargo de producir un informe integral con principios, hallazgos y recomendaciones para guiar la acción legislativa en múltiples sectores. Estos precedentes ofrecen modelos replicables para comités de ética digital u órganos análogos orientados a supervisar, evaluar y rendir cuentas sobre el uso de algoritmos en sede parlamentaria.

4.5 Marcos de autorregulación: códigos éticos y de conducta

Más allá de los principios generales, los parlamentos pueden adoptar códigos de conducta o directrices internas específicas para el uso de la inteligencia artificial, formalizando compromisos y normas propias. Se trata de un ejercicio de autorregulación institucional que traduce la legislación nacional y los estándares internacionales en reglas concretas para la cámara legislativa. Recientemente algunos han dado pasos importantes en este sentido. Por ejemplo, el Parlamento del Reino Unido publicó en septiembre de 2025 una guía oficial para miembros de ambas cámaras sobre el uso seguro y responsable de la IA, la cual fue revisada y respaldada por comités internos antes de su adopción.

Estos códigos deberían incluir los principios ya mencionados de transparencia algorítmica (4.2), divulgación del uso de IA (4.2), supervisión humana permanente (4.3), mitigación de sesgos y revisiones (4.4), evaluaciones de impacto (4.4), a los que añadiríamos la capacitación continua, facilitando la formación a parlamentarios y personal sobre el funcionamiento y límites de la IA y fomentando la alfabetización digital y en datos; el establecimiento de mecanismos de denuncia, a través de canales que permitan que si algún funcionario detecta un funcionamiento problemático del sistema (p. ej., sospecha de sesgo o errores recurrentes), pueda reportarlo sin temor a represalias (similar al *whistleblowing*); y la

revisión y actualización del código que permita a los parlamentos seguir el ritmo de la tecnología (p. ej., cada uno o dos años) a la luz de nuevas experiencias y conocimientos.

La Unión Interparlamentaria (UIP) ha llamado a los parlamentos a compartir sus mejores prácticas en esta materia y, posiblemente en el futuro, se configure un modelo de "código de conducta global" para la IA parlamentaria. En octubre de 2024, la Unión Interparlamentaria adoptó una resolución que insta a los parlamentos a dotarse de marcos legales sólidos para una IA compatible con la democracia, los derechos humanos y el Estado de derecho. En su tenor literal: "Calls upon parliaments to effectively and transparently adopt or maintain strong legal frameworks and policies for the responsible creation, deployment and use of AI technology." (Inter-Parliamentary Union, 2024c, p. 2). España, en su Estrategia Nacional de IA (ENIA, 2020), ya apunta a fomentar la adopción de principios éticos en el sector público (Gobierno de España, 2020). Un eventual "Código Ético de las Cortes Generales para la IA" sería pionero en el mundo hispanohablante, y posiblemente la Revista Española de Transparencia –a la que se destina este artículo– podría servir de foro para discutir su contenido.

En conclusión, los códigos de conducta internos son la forma de cristalizar todos los principios y directrices mencionados, adaptándolos a la realidad particular de cada parlamento. Son herramientas flexibles, que no requieren pasar por un largo proceso legislativo, y muestran un compromiso institucional voluntario con un uso responsable de la IA. Por supuesto, estos códigos deben ir más allá de las palabras. Su eficacia radica en su implementación rigurosa y en que logren crear cultura organizativa. Pero su mera existencia ya fija un estándar y sirve de referencia para exigir *accountability*: la ciudadanía podrá reclamar "ustedes mismos en su código prometieron X, ¿lo están cumpliendo?".

4.6 Iniciativas internacionales y recomendaciones

Conviene, finalmente, situar estas directrices en el contexto de las iniciativas internacionales más recientes. Los parlamentos no operan aislados y pueden aprovechar marcos globales ya consensuados para orientar sus estrategias.

Las referencias más destacadas serían:

a) Unión Interparlamentaria (UIP)

En 2024, además del documento de "Use Cases for AI in Parliaments" (Inter-Parliamentary Union, 2024a), la UIP publicó las "Guidelines for AI in Parliaments" (Inter-Parliamentary Union, 2024b), que ofrecen un

marco comprensivo para que los parlamentos entiendan e implementen la IA de forma responsable y efectiva. Sus recomendaciones clave incluyen: comenzar con proyectos piloto acotados; asegurar una robusta supervisión humana; priorizar la transparencia y la rendición de cuentas; e invertir en alfabetización en datos/IA dentro de la organización. Asimismo, la UIP apremia a involucrar a diversos actores en el proceso de adopción (diputados de distintas tendencias, técnicos, academia, sociedad civil). Esencialmente, la UIP promueve todo lo que hemos expuesto: un enfoque incremental y ético, donde la IA se use para potenciar (no sustituir) la labor humana en la deliberación democrática.

Por otra parte, la resolución de la UIP sobre IA y democracia aprobada en su 149ª Asamblea, celebrada en Ginebra en 2024, por una amplia mayoría insta a los parlamentos a legislar pronto sobre IA a nivel nacional (equilibrando innovación y derechos) y apunta a la cooperación internacional para desarrollar normas éticas globales, por ejemplo en el uso de IA en procesos electorales. (IPU, 2024a).

b) Unión Europea.

El Reglamento (UE) 2024/1689, conocido como Reglamento de Inteligencia Artificial o AI Act, establece un marco jurídico armonizado para el desarrollo y uso de sistemas de IA en la Unión Europea (Unión Europea, 2024). Si bien su Reglamento de Inteligencia Artificial (RIA) se dirige principalmente a proveedores y usos de IA en general, genera obligaciones también para el sector público. El Reglamento clasifica ciertos usos (como los de fuerzas de seguridad, evaluación de personas, etc.) como alto riesgo, sujetándolos a requisitos estrictos de transparencia, gestión de datos, supervisión humana, etc. Un parlamento difícilmente caería en escenarios de “alto riesgo” (salvo que usara sistemas de biometría, reconocimiento facial en sede, etc.), pero seguramente deberá adoptar estándares similares en sus sistemas que como hemos visto están afectados por otros principios establecidos en el mismo como la transparencia (art. 13.1), en sus distintas vertientes, o la supervisión humana (art. 14). Aparte de la regulación, ya en vigor, la Comisión Europea ya había emitido en 2019 las Orientaciones Éticas para una IA de confianza, con 7 requisitos clave: intervención humana, robustez técnica, privacidad, transparencia, diversidad/no discriminación, bienestar social y rendición de cuentas. Todos esos temas resuenan con lo tratado aquí, y de hecho fueron incorporados por España en su Plan Nacional de

IA (ENIA).

c) Consejo de Europa.

El Convenio sobre Inteligencia Artificial, Derechos Humanos, Democracia y Estado de Derecho del Consejo de Europa (2024), conocido como Convention on Artificial Intelligence (CAI), constituye el primer tratado internacional vinculante que regula el desarrollo y uso de la IA desde una perspectiva basada en los derechos humanos, la democracia y el Estado de derecho (Consejo de Europa, 2024). Se trata de un tratado vinculante para los miembros del Consejo de Europa pero abierto a la ratificación de terceros países adopta un prisma centrado en los derechos humanos, la democracia y Estado de derecho, y, por su carácter abierto, aspira a ser el primer instrumento jurídico global en la materia. Mientras tanto, su Comité de Ministros ya emitió una Recomendación sobre los impactos en derechos humanos de los sistemas algorítmicos (CM/Rec(2020)1), que brinda orientaciones a los Estados para asegurar que el uso de algoritmos sea compatible con el Convenio Europeo de DD.HH. (Council of Europe, 2020). Además, distintos órganos del Consejo de Europa han producido guías sectoriales. Un ejemplo es la Carta Ética Europea sobre el uso de la IA en la Justicia (CEPEJ, 2018), que establece cinco principios para el uso de la IA en los tribunales: respeto de derechos fundamentales, no discriminación, calidad y seguridad, transparencia/imparcialidad, y "bajo control del usuario". Se trata de adaptar los valores generales a un contexto específico (el judicial en ese caso). Un ejercicio similar se podría hacer para los parlamentos, lo cual refuerza la idea de desarrollar códigos de conducta a medida (como vimos en 4.5).

d) Redes de parlamento abierto.

Organismos como ParlAmericas o la iniciativa OPSI de la OCDE también han abordado la IA legislativa. Por ejemplo, en junio de 2023 ParlAmericas lanzó una "Bancada Digital", un grupo de trabajo interparlamentario dedicado a la gobernanza digital e inteligencia artificial. En su evento de lanzamiento se subrayó "la necesidad de que América Latina y el Caribe participen de manera sustantiva en los diálogos internacionales sobre inteligencia artificial, para que los marcos normativos se desarrollen con principios democráticos e inclusivos". Iniciativas así fomentan el intercambio regional de buenas prácticas y la construcción de una visión compartida sobre la IA en la esfera pública.

Vale la pena destacar, por último, que los Principios de la OCDE sobre IA (2019) –adoptados por 50 países, incluida España– también recogen, de manera pionera, ideas muy similares: promover un crecimiento inclusivo mediante IA, respetar los derechos humanos y valores democráticos, garantizar transparencia, seguridad, y responsabilizar a quienes diseñan y operan los sistemas. Todas estas fuentes reafirman un punto: existe un consenso internacional emergente en torno a que la IA debe implementarse de forma responsable, humana y ética, especialmente en contextos democráticos. Lo que ahora importa es la ejecución concreta en cada institución. Los parlamentos tienen, por tanto, una hoja de ruta relativamente clara apoyada en este acervo compartido: se trata de poner en práctica esos lineamientos, medir resultados y compartir las lecciones aprendidas.

5. Conclusiones

La revolución digital basada en inteligencia artificial está reconfigurando aceleradamente los fundamentos de nuestras democracias y el modo en que se produce, accede y aplica el Derecho. A lo largo de este análisis hemos constatado, desde la perspectiva parlamentaria, que la IA constituye, a un tiempo, una oportunidad transformadora para fortalecer los valores democráticos y un desafío multidimensional que puede socavar estos si no se encauza correctamente.

Las promesas de la IA son notables. En las instituciones representativas, hemos visto cómo puede aumentar la transparencia parlamentaria, facilitando que los ciudadanos accedan ágilmente a la ingente producción legislativa y deliberativa y democratizando el acceso a las fuentes del Derecho de origen parlamentario. La IA también puede ayudar a ampliar las posibilidades de participación ciudadana, mejorando la información necesaria disponible sobre estos procesos, procesando masivamente aportaciones y permitiendo nuevas formas de deliberación colectiva. Fortalece además la rendición de cuentas, al potenciar, con su capacidad de procesamiento masivo de información, las posibilidades para auditar el uso de recursos públicos y detectar irregularidades.

En el ámbito de la producción normativa, la IA acelera la investigación legal, asiste en la redacción técnica de leyes, detectando, por ejemplo, ambigüedades, reiteraciones e incluso contradicciones y velando por la coherencia del sistema normativo ayudando a consolidar los cambios normativos de forma inmediata y sin errores. Todo ello redundará en normas de mayor calidad, mejor armonizadas con el ordenamiento existente y más comprensibles para todos.

Sin embargo, junto a estas luces se proyectan también sombras preocupantes. El "sesgo de automatización" nos enseña que los usuarios tendemos a confiar ciegamente en las recomendaciones de sistemas inteligentes, lo cual en contextos democráticos podría traducirse en representantes que deleguen acríticamente decisiones o ciudadanos que acepten sin filtro la información "curada" por algoritmos, perdiendo la deliberación indispensable para no perder el carácter democrático de nuestra institución parlamentaria.

Ante este panorama ambivalente, resulta imperativo adoptar marcos ético-jurídicos y políticas públicas que maximicen los beneficios de la IA a la vez que previenen o mitigan sus daños. Nuestro recorrido por las directrices ha subrayado algunos ejes de consenso, que coinciden con las habituales en el uso de la IA en otras instituciones democráticas: la exigencia de transparencia algorítmica, para que la actuación de las IA en la esfera pública sea auditable y comprensible; la necesidad de supervisión humana permanente, preservando siempre el control y la responsabilidad última de las decisiones en manos de personas; la no discriminación y la privacidad como líneas rojas que las aplicaciones de IA no deben cruzar; y la importancia de introducir controles contra sesgos, evaluaciones de impacto y capacitación interna para un uso consciente de estas herramientas. Estos principios deben traducirse en códigos de conducta y regulación, tanto interna (por ejemplo, en los parlamentos) como a nivel estatal e internacional.

Afortunadamente, en el ámbito parlamentario no partimos de cero. Iniciativas internacionales como la Resolución de la IPU de 2024 sobre IA y democracia, los Principios de la OCDE (2019), el Reglamento europeo de IA (2024), y el Convenio del Consejo de Europa (2024) nos brindan un acervo valioso de recomendaciones. Queda en manos de legisladores y autoridades implementarlas con determinación.

En síntesis, la IA es ya inseparable de la vida parlamentaria y del sistema democrático: las permea y las transforma. De ahí la necesidad de orientar su utilización para que sea un factor de fortalecimiento del Estado de Derecho, ampliando la transparencia, eficiencia y participación; y no un factor de erosión, que concentre poder en opacidades algorítmicas o degrade la confianza en las instituciones.

Lograr este equilibrio requerirá un enfoque multidisciplinar y colaborativo: juristas, tecnólogos, politólogos, sociólogos, legisladores y la ciudadanía en general deben participar en el diálogo sobre qué IA queremos. También demandará una actitud proactiva de los poderes públicos: autorregularse (como los parlamentos que adoptan códigos éticos para IA), regular al sector

privado cuando corresponda (por ejemplo, imponiendo obligaciones de transparencia a las plataformas online respecto a sus algoritmos de recomendación, como hace la Ley de Servicios Digitales de la UE) y educar a la población para este nuevo entorno.

Como ocurre en otros sectores, y haciendo propia una afirmación que aspira a convertirse en tópico, estamos convencidos de que la IA no reemplazará a los actores democráticos humanos, pero aquellos actores que sepan usarla reemplazarán posiblemente a los que no. Esta sentencia, adaptada al contexto parlamentario, nos recuerda que abrazar la IA con sentido crítico es indispensable para no quedar rezagados. Los parlamentarios y juristas que integren inteligentemente estas herramientas servirán mejor a sus representados; quienes las ignoren, arriesgan quedarse obsoletos en un mundo cada vez más modelado por algoritmos.

Bibliografía

- Agencia Española de Protección de Datos. (2021). Gestión del riesgo y evaluación de impacto en tratamientos de datos personales (guía). Disponible en: AEPD (Agencia Española de Protección de Datos).
- Agencia Española de Protección de Datos. (2023). Orientaciones para la realización de una EIPD en el desarrollo normativo. Disponible en: AEPD.
- Álvarez Robles, T. (2022). Las garantías de los derechos fundamentales en y desde la red: El contexto español. *Revista Chilena de Derecho y Tecnología*, 11(1), 5–40. <https://doi.org/10.5354/0719-2584.2022.60197>
- Alvesalo-Kuusi, A., Alitalo, O., Peltoniemi, N., Rytönen, I., Sjölund, M., Laine, O., & Tuovinen, T. (2022). Lawradar: A research platform for Finnish law drafting and legislation (versión 1.0.0). Zenodo. <https://doi.org/10.5281/zenodo.6504432>
- Biggio, B., Nelson, B., & Laskov, P. (2012). Poisoning attacks against support vector machines. En *Proceedings of the 29th International Conference on Machine Learning (ICML 2012)*. Disponible en arXiv: <https://arxiv.org/abs/1206.6389>
- Bond, R. R., Novotny, T., Andrsava, I., Koc, L., Sisakova, M., Finlay, D., Guldenring, D., McLaughlin, J., Peace, A., McGilligan, V., Leslie, S. J., Wang, H., & Malik, M. (2018). Automation bias in medicine: The influence of automated diagnoses on interpreter accuracy and uncertainty when reading electrocardiograms. *Journal of Electrocardiology*, 51(6S), S6–S11. <https://doi.org/10.1016/j.jelectrocard.2018.08.007>

- Bourtole, L., Chandrasekaran, V., Choquette-Choo, C. A., et al. (2021). Machine unlearning. En Proceedings of the USENIX Security Symposium 2021. (SISA training). Disponible en Illinois Experts: <https://experts.illinois.edu/en/publications/machine-unlearning>
- Camera dos Deputados de Brasil. (2024, June 24). Analysis of citizens' opinions on bills [Use case 023]. In Inter-Parliamentary Union (IPU), Use cases for AI in parliaments. <https://www.ipu.org/ai-use-cases/analysis-citizens-opinions-bills>
- Carmona Aguirre, V., & Sánchez Rivera, E. (2025, 26 septiembre). From Valparaíso to Latin America: How the AI-driven archives revolution in Chile is transforming parliaments in the region. Inter-Parliamentary Union (IPU). <https://www.ipu.org/innovation-tracker/story/valparaiso-latin-america-how-ai-driven-archives-revolution-in-chile-transforming-parliaments-in-region>
- Congreso de los Diputados. (2025). I Plan de Parlamento Abierto del Congreso de los Diputados (2025–2027). BOCG, Congreso de los Diputados, Serie D, núm. 310, de marzo de 2025, p. 4.
- Consejo de Europa. (2024). Convention on Artificial Intelligence, Human Rights, Democracy and the Rule of Law (CETS No. 208). Estrasburgo: Council of Europe. Texto disponible en: <https://rm.coe.int/convention-on-artificial-intelligence-human-rights-democracy-and-the-/1680afae3c>
- Cotino Hueso, L. (2023). Qué concreta transparencia e información de algoritmos e inteligencia artificial es la debida. Revista Española de la Transparencia, 16, 17–63.
- EDPB (European Data Protection Board). (2021). Recommendations 01/2020 on measures that supplement transfer tools... Disponible en: https://www.edpb.europa.eu/system/files/2021-06/edpb_recommendations_202001vo.2.0_supplementarymeasurestransferstools_en.pdf
- EDPB (European Data Protection Board). (2025). Guidelines 01/2025 on Pseudonymisation. Disponible en: https://www.edpb.europa.eu/news/news/2025/edpb-adopts-pseudonymisation-guidelines-and-paves-way-improve-cooperation_en
- European Parliament. (s. f.). Ask the Archives: The EP Archives Unit launches its first generative AI tool. Historical Archives of the European Parliament. Recuperado el 1 de noviembre de 2025, de

<https://historicalarchives.europarl.europa.eu/en/sites/historicalarchive/home/cultural-heritage-collections/news/ai-dashboard.html>

Gobierno de España. (2020). Estrategia Nacional de Inteligencia Artificial (ENIA). Madrid: Secretaría de Estado de Digitalización e IA (Ministerio de Asuntos Económicos y Transformación Digital). Disponible en: <https://www.lamoncloa.gob.es/tecnologicas/estrategia-ia>

Gobierno de España. (2021). Carta de Derechos Digitales. Madrid: Secretaría de Estado de Digitalización e IA. Publicada el 14 de julio de 2021, disponible en: <https://derechosdigitales.gob.es>

Goddard, K., Roudsari, A., & Wyatt, J. C. (2012). Automation bias: A systematic review of frequency, effect mediators, and mitigators. *Journal of the American Medical Informatics Association*, 19(1), 121-127. <https://doi.org/10.1136/amiajnl-2011-000089>

Gonzalo Rozas, M. Ángel. (2018). Parlamento y participación ciudadana. *Revista de las Cortes Generales*, (105), 219-246.

Gonzalo Rozas, M. A., Marañón Martín, L., Rubio Núñez, R. (2021) ¿Existe el lobby ciudadano? Una experiencia de participación en el Congreso de los Diputados. *Revista De Las Cortes Generales*, (110), 235-271. <https://doi.org/10.33426/rcg/2021/110/1573>

Goodfellow, I. J., Shlens, J., & Szegedy, C. (2015). Explaining and harnessing adversarial examples. En *Proceedings of the ICLR 2015*. (FGSM descrito en pp. 2-4 del PDF). Disponible en arXiv: <https://arxiv.org/pdf/1412.6572>

High-Level Expert Group on Artificial Intelligence. (2019). Ethics Guidelines for Trustworthy AI. Brussels: European Commission. <https://digital-strategy.ec.europa.eu/en/library/ethics-guidelines-trustworthy-ai>

Hyvönen, E., Sinikallio, L., Leskinen, P., Drobac, S., Leal, R., La Mela, M., Tuominen, J., & Poikkimäki, H. (2024). Publishing and Using Parliamentary Linked Data on the Semantic Web: ParliamentSampo System for Parliament of Finland. *Semantic Web Journal*. Disponible en: <https://www.semantic-web-journal.net/content/publishing-and-using-parliamentary-linked-data-semantic-web-parliamentsampo-system-0>

Inter-Parliamentary Union (IPU). (2024a). Guidelines for AI in Parliaments. Ginebra: IPU Centre for Innovation in Parliament.

Inter-Parliamentary Union (IPU). (2024b). Use Cases for AI in Parliaments. Ginebra: IPU. Disponible en: <https://www.ipu.org/file/20635/download>

- Inter-Parliamentary Union (IPU). (2024c). The impact of artificial intelligence (AI) on democracy, human rights and the rule of law. Resolución adoptada por la 149ª Asamblea de la UIP (Ginebra, 17 de octubre de 2024). Disponible en: <https://www.ipu.org/es/resources/resoluciones-y-declaraciones> (texto en inglés)
- International Panel on the Information Environment (IPIE). (2025). The Role of Generative AI Use in 2024 Elections Worldwide: Searching for Solutions. Technical Paper, Panel "AI & Elections". Disponible en: <https://www.ipie.info/research/tp2025-2>
- Jobin, A., Ienca, M., & Vayena, E. (2019). The global landscape of AI ethics guidelines. *Nature Machine Intelligence*, 1(9), 389–399.
- Kissinger, H. A., Schmidt, E., & Huttenlocher, D. (2021, 20 de noviembre). Las máquinas de guerra no parpadean ni tienen sentimientos. *Newsweek en Español*. <https://newsweekespanol.com/2021/11/20/maquinas-guerra-ia-no-parpadean>
- Kunze, A., Gonzalez, C., Wiczorek, R., & Bengler, K. (2019). Automation transparency: Implications of uncertainty communication for human-automation interaction and interfaces. *Ergonomics*, 62(3), 345–360. <https://doi.org/10.1080/00140139.2018.1547842>
- Lessig, L. (1999). *Code and other laws of cyberspace*. New York: Basic Books. Disponible en: <https://lessig.org/images/resources/1999-Code.pdf>
- Lessig, L. (2006). *Code: Version 2.0*. New York: Basic Books.
- Library of Congress. (2024, 19 de noviembre). Could Artificial Intelligence Help Catalog Thousands of Digital Library Books? En *The Signal* (blog oficial de la Biblioteca del Congreso de EE.UU.). Disponible en: <https://blogs.loc.gov/thesignal/2024/11/could-artificial-intelligence-help-catalog-thousands-of-digital-library-books-an-interview-with-abigail-potter-and-caroline-saccucci/>
- Library of Congress Labs. (2024). Exploring Computational Description (ECD). Disponible en: <https://labs.loc.gov/work/experiments/ecd/>
- Manin, B. (1998). *Los principios del gobierno representativo* (F. Vallespín, trad.). Madrid: Alianza Editorial.
- Ministerio de Asuntos Económicos y Transformación Digital (España). (2022). Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad (ENS). Publicado en BOE-A-2022-7191. Disponible en BOE: <https://www.boe.es/buscar/act.php?id=BOE-A-2022-7191>

Nelson, T. (1974). *Computer Lib / Dream Machines*. Self-published.

OCDE. (2019). *Principios de la OCDE sobre Inteligencia Artificial*. París: OECD Legal Instrument 0449. (Conjunto de principios adoptados por 50 países, incluyendo dirección humana de los sistemas de IA, robustez y seguridad, transparencia, diversidad y no discriminación, y rendición de cuentas).

OASIS. (2018). *Akoma Ntoso Version 1.0 (Part 1: XML vocabulary)*. OASIS LegalDocML TC, 29 de agosto de 2018. Disponible en: <http://docs.oasis-open.org/legaldocml/akn-core/v1.0/os/part1-vocabulary/akn-core-v1.0-os-part1-vocabulary.html>

Parasuraman, R., & Manzey, D. H. (2010). Complacency and bias in human use of automation: An attentional integration. *Human Factors*, 52(3), 381–410. <https://doi.org/10.1177/0018720810376055>

ParlAmericas (Red de Parlamento Abierto). (2023). La RPA de ParlAmericas presenta un nuevo grupo de trabajo interparlamentario enfocado en IA y derechos digitales (Comunicado oficial, 22 de junio de 2023). Disponible en: <https://parlAmericas.org/news/> (consultado el 10/09/2025).

Parliament of Singapore. (2024, 13 de agosto). AI-powered search engine for Singapore's Hansard Reports (Nota de prensa oficial). Disponible en: <https://www.parliament.gov.sg/newsroom/events/Details/ai-powered-search-engine-for-singapore%27s-hansard-reports>

Poursabzi-Sangdeh, F., Goldstein, D. G., Hofman, J., Wortman Vaughan, J., & Wallach, H. (2021). Manipulating and measuring model interpretability. En *Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems*. New York: ACM. <https://doi.org/10.1145/3411764.3445315>

Rekathati, F. / KBLab. (2023). RixVox: A Swedish Speech Corpus with 5,500 Hours of Speech from Parliamentary Debates. KBLab Blog (9 de marzo de 2023). Disponible en: <https://kb-labb.github.io/posts/2023-03-09-rixvox-a-swedish-speech-corpus/>

Rubio Núñez, R. (2025). El uso de la inteligencia artificial en las campañas electorales y sus efectos democráticos. *Revista de Derecho Político*, (122), 65–102. doi:10.5944/rdp.122.2025.44742.

Rubio Núñez, R., et al. (2014). *Parlamentos abiertos: Tecnología y redes para la democracia*. Madrid: Congreso de los Diputados.

Rubio Núñez, R. (2022). El Parlamento en busca de la centralidad perdida. Entre el test de stress y la aceleración de procesos. *Asuntos Constitucionales*, 2, 5–22.

- Rubio Núñez, R., Marañón Martín, L., & Gonzalo Rozas, M. Á. (2021). ¿Existe el lobby ciudadano? Una experiencia de participación en el Congreso de los Diputados. *Revista de las Cortes Generales*, 110, 235–271.
- Rubio Núñez, R., Franco Alvim, F., & de Andrade Monteiro, V. (2024). *Inteligencia artificial y campañas electorales algorítmicas. Disfunciones informativas y amenazas sistémicas de la nueva comunicación política*. Madrid: Centro de Estudios Políticos y Constitucionales.
- Tejeda-Lemus, H., Kumar, A., & Steyvers, M. (2023). How displaying AI confidence affects reliance and hybrid human–AI performance. En P. Lukowicz et al. (Eds.), *HHAI 2023: Augmenting Human Intellect* (pp. 234–241). IOS Press. <https://doi.org/10.3233/FAIA230087>
- Tsai, T. L., Fridsma, D. B., & Gatti, G. (2003). Computer decision support as a source of interpretation error: The case of electrocardiograms. *Journal of the American Medical Informatics Association*, 10(5), 478–483. <https://doi.org/10.1197/jamia.M1279>
- UNESCO. (2021). *Recomendación sobre la Ética de la Inteligencia Artificial*. París: UNESCO (aprobada por la 41ª Conferencia General de la UNESCO el 24 de noviembre de 2021). Disponible en: https://unesdoc.unesco.org/ark:/48223/pf0000380455_spa
- Unión Europea. (2024). Reglamento (UE) 2024/1689 del Parlamento Europeo y del Consejo, de 13 de junio de 2024, por el que se establecen normas armonizadas en materia de inteligencia artificial (AI Act). *Diario Oficial de la Unión Europea*, L 2024/1689, 12 de julio de 2024.
- Vela Navarro-Rubio, R., Rubio Núñez, R. (2017a) *Parlamento Abierto: El Parlamento en el Siglo XXI*, Uoc, 2017. Págs. 216.
- Vela Navarro-Rubio, R., Rubio Núñez, R. (2017b) *El Parlamento Abierto en el mundo: Evolución y buenas prácticas*, Fundación Gimenez Abad, Colección Monografías, 2017. Págs. 236.
- Vela Navarro-Rubio, R., Rubio Núñez, R. (2018) "El Parlamento Abierto en España", en *Revista General de Derecho Constitucional*, número 17, Abril 2018.
- Villoria Mendieta, M. (2020). Rendición de cuentas. En B. Pendás García (Ed.), *Enciclopedia de las Ciencias Morales y Políticas para el siglo XXI: Ciencias Políticas y Jurídicas* (pp. 426–429). Real Academia de Ciencias Morales y Políticas; Boletín Oficial del Estado.

- Wahl, T. (2024). The rise of data and AI in parliamentary proceedings – The Norwegian Parliament (Stortinget). *International Journal of Parliamentary Studies*, 4(1), 1–9.
- Wallace, E., Feng, S., Kandpal, N., Gardner, M., & Singh, S. (2019). Universal adversarial triggers for attacking and analyzing NLP. En *Proceedings of EMNLP-IJCNLP 2019* (pp. 2153–2162). Disponible en ACL Anthology: <https://aclanthology.org/D19-1221.pdf>
- Westminster Foundation for Democracy (Fitsilis, A.). (2024). Guidelines for AI in Parliaments: A practical baseline. Londres: WFD. Disponible en: <https://www.wfd.org/sites/default/files/2024-07/wfd-ai-guidelines-for-parliaments-2024-english.pdf>
- WP29 (Grupo de Trabajo del Art. 29). (2014). Opinion 05/2014 on Anonymisation Techniques. Disponible en: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp216_en.pdf