Asamblea. Revista Parlamentaria de la Asamblea de Madrid
ISSN: 1575-5312. eISSN: 2951-665X
Núm. 48, primer semestre 2025, pp. 161-193
https://doi.org/10.59991/rvam/2025/n.48/1025

La inteligencia artificial en la transformación digital de los parlamentos: en busca de un modelo *ad hoc* de gobernanza

Artificial Intelligence in the digital transformation of parliaments: in search of an *ad hoc* Governance model

Esther de Alba Bastarrechea
Letrada de la Asamblea de Madrid
https://orcid.org/0000-0002-6149-5807

Fecha de recepción: 11/05/2025
Fecha de aceptación: 30/05/2025

RESUMEN

El presente artículo aborda el análisis jurídico de la digitalización de los parlamentos, la incorporación de la inteligencia artificial (IA) y el cumplimiento normativo en materia de protección de datos personales en el contexto del Reglamento General de Protección de Datos (RGPD) y del Reglamento de Inteligencia Artificial (RIA). Se examinan, en primer lugar, los principios fundamentales del RGPD en su aplicación a tratamientos automatizados; en segundo término, la estructura, principios y obligaciones del RIA; en tercer lugar, las dificultades prácticas de implementación normativa en los parlamentos, incluyendo la labor de los delegados de protección de datos y la evaluación de impacto; en cuarto lugar, el papel de los parlamentos como usuarios y reguladores de IA, destacando la necesidad de un modelo ético de gobernanza tecnológica; y, finalmente, se analizan las sinergias institucionales entre cuerpos técnicos (letrados, archiveros e informáticos) como elemento clave en la integración responsable de tecnologías. El estudio concluye con una propuesta de gobernanza normativa que armoniza innovación, protección de derechos fundamentales y seguridad jurídica en el uso de la IA en el ámbito parlamentario.

PALABRAS CLAVE: Inteligencia artificial, RGPD, RIA, protección de datos, parlamentos, gobernanza tecnológica, derechos fundamentales, evaluación de impacto, interoperabilidad institucional.

ABSTRACT

This article presents a legal analysis of the interaction between artificial intelligence (AI) and personal data protection under the General Data Protection Regulation (GDPR) and the Artificial Intelligence Act (AI Act), with a specific application to parliamentary contexts. The paper is structured into five sections. First, it explores the core GDPR principles as applied to automated data processing. Second, it analyzes the AI Act's structure, guiding principles, and obligations framework. Third, it addresses the practical challenges of regulatory implementation in parliaments, including the role of data protection officers and impact assessments. Fourth, it examines the dual function of parliaments as both users and regulators of AI, advocating for an ethical model of technological governance. Finally, it highlights the need for institutional synergy among legal advisors, archivists, and IT professionals to ensure the responsible adoption of disruptive technologies. The study concludes with a proposal for a normative governance framework that balances innovation with fundamental rights protection and legal certainty in the use of AI within parliamentary settings.

KEYWORDS: Artificial intelligence, GDPR, Artificial Intelligence Act, data protection, parliaments, technological governance, fundamental rights, impact assessment, institutional interoperability.

I. LA TRANSFORMACIÓN DIGITAL DE LOS PARLAMENTOS: FUNDAMENTOS JURÍDICOS Y RETOS INICIALES

1.1. Introducción

La digitalización de los parlamentos constituye una de las manifestaciones más relevantes de la transformación institucional impulsada por la revolución tecnológica contemporánea. Esta dinámica, que va a afectar tanto a los procedimientos legislativos como a los mecanismos de interacción con la ciudadanía y a los sistemas de gestión documental, plantea exigencias jurídicas inéditas en términos de transparencia, seguridad, protección de datos personales y garantía de los derechos fundamentales[1].

Este trabajo tiene por objeto examinar los fundamentos normativos que sustentan la digitalización parlamentaria, así como identificar los principales desafíos iniciales derivados de su implementación. Se subraya de manera particular la necesidad de una actuación coordinada entre cuerpos técnicos —letrados, archiveros y personal informático— para asegurar la eficacia, legitimidad y sostenibilidad de los procesos de transformación digital.

1.2. La transformación digital como fenómeno jurídico

La transformación digital no puede ser entendida únicamente como un fenómeno técnico o administrativo. Implica, en realidad, una reconfiguración estructural del funcionamiento institucional que afecta a principios básicos como la publicidad de los actos parlamentarios, el derecho de acceso a la información, el principio de legalidad en la tramitación de procedimientos legislativos y el respeto de los derechos fundamentales, en especial el derecho a la protección de datos personales[2].

El fenómeno de la digitalización, en el ámbito parlamentario, debe ser enmarcado dentro de la doctrina del gobierno abierto y de la administración electrónica, categorías que han recibido respaldo normativo tanto en el derecho internacional como en el derecho interno de los Estados. En este sentido, destacan instrumentos como la Declaración de Principios sobre la Libertad de Expresión y el Acceso a la Información Pública de la OEA[3] y las Directrices de la Unión Interparlamentaria sobre la Democracia Electrónica Parlamentaria[4].

---

[1] Cano Bazaga, E. (2021). *Gobierno abierto y transformación digital*. Aranzadi.

[2] De Miguel Asensio, P. (2020). *Protección de datos y derecho digital*. Thomson Reuters-Aranzadi.

[3] Organización de los Estados Americanos (OEA). (2000). *Declaración de Principios sobre la Libertad de Expresión*.

[4] Unión Interparlamentaria (UIP). (2018). *Directrices sobre la democracia electrónica parlamentaria*.

La legislación nacional también ha incorporado disposiciones que apuntalan la digitalización. En el caso español, por ejemplo, la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas, y la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público, establecen un marco jurídico robusto para la transformación digital, aplicable también, en lo pertinente, a las Cámaras legislativas.

Por tanto, la digitalización parlamentaria no es un proceso opcional ni carente de regulación: constituye una obligación jurídica derivada de principios de rango constitucional y legal, cuyo incumplimiento podría comprometer la validez de los procedimientos legislativos y la vigencia de los derechos de los ciudadanos.

1.3. Fundamentos constitucionales de la digitalización parlamentaria

La digitalización debe anclarse en los principios constitucionales que rigen la actividad parlamentaria. Entre ellos, destacan:

— El principio de publicidad de los actos parlamentarios: recogido en el artículo 80 de la Constitución Española (CE), que exige que las sesiones de las Cámaras sean públicas salvo en los casos en que se acuerde lo contrario por mayoría absoluta.
— El derecho de acceso a la información pública: consagrado en el artículo 105.b) CE y desarrollado por la Ley 19/2013, de 9 de diciembre, de transparencia, acceso a la información pública y buen gobierno.
— La protección de los datos personales: garantizada en el artículo 18.4 CE, que establece el derecho fundamental a la protección de los datos personales y la obligación de las administraciones públicas de utilizar los medios técnicos adecuados para preservar dicho derecho.

Estos principios imponen un deber de adaptación tecnológica que no puede ser eludido por los parlamentos. La omisión de medidas de digitalización que garanticen la publicidad, la transparencia o la protección de datos podría vulnerar derechos fundamentales y, en consecuencia, generar responsabilidad jurídica para las instituciones parlamentarias[5].

En este contexto, la actuación de los parlamentos no puede limitarse a la mera informatización de procedimientos existentes, sino que debe diseñar una estrategia digital integral, que abarque tanto los aspectos tecnológicos como los organizativos y normativos.

[5] Sáez Vacas, F. (2018). *Sociedad digital: el cambio histórico actual*. Editorial Complutense.

1.4. Principales retos jurídicos de la digitalización parlamentaria

La implementación de tecnologías digitales en los parlamentos plantea retos jurídicos de gran envergadura, entre los cuales pueden destacarse:

a) Seguridad jurídica de los procedimientos digitales

La transición de procedimientos legislativos tradicionales a formatos digitales exige asegurar su plena validez jurídica. Ello implica establecer marcos normativos claros sobre la autenticidad de los documentos electrónicos, la integridad de los registros, la conservación de las evidencias digitales y la trazabilidad de las actuaciones parlamentarias.

b) Protección de datos personales y privacidad

El tratamiento de datos personales en entornos digitales parlamentarios requiere medidas específicas de cumplimiento del Reglamento General de Protección de Datos (RGPD) y de la normativa nacional en materia de protección de datos, como la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales. Esto incluye la implementación de políticas de privacidad, evaluaciones de impacto, medidas de seguridad técnicas y organizativas y designación de Delegados de Protección de Datos (DPD) y la dotación a estos de medios personales y materiales adecuados para el correcto ejercicio de su función.

c) Transparencia y acceso a la información en el entorno digital

La digitalización debe potenciar la transparencia parlamentaria, facilitando el acceso ciudadano a la información en formatos accesibles, reutilizables y comprensibles. La opacidad tecnológica —por ejemplo, el uso de algoritmos no explicables en la gestión documental— podría convertirse en una nueva forma de restricción ilegítima de la información pública[6].

d) Preservación digital y gestión documental

La conservación a largo plazo de los documentos electrónicos parlamentarios plantea problemas técnicos y jurídicos de gran complejidad, relacionados con la autenticidad, la integridad y la disponibilidad de la información. Se requiere el diseño de políticas de archivo electrónico basadas en estándares internacionales, como el modelo OAIS (Open Archival Information System) y la normativa ISO 14721.

---

[6] De la Quadra-Salcedo Janini, T. (2017). *La transparencia como valor constitucional*. Centro de Estudios Políticos y Constitucionales.

1.5. El papel de los cuerpos técnicos en la transformación digital

La transformación digital parlamentaria no puede ser encomendada exclusivamente a técnicos informáticos o a asesores externos. Requiere una cooperación estructurada entre distintos cuerpos profesionales:

— Letrados parlamentarios: encargados de asegurar la conformidad de los procedimientos digitales con los principios constitucionales, la legislación vigente y las reglas parlamentarias internas.
— Archiveros-documentalistas: responsables de diseñar e implementar políticas de gestión documental electrónica, garantizando la conservación, autenticidad e integridad de los registros parlamentarios.
— Informáticos parlamentarios: encargados del desarrollo, implantación y mantenimiento de las infraestructuras tecnológicas, así como de la implementación de medidas de seguridad de la información.

La colaboración interdisciplinaria es esencial para articular soluciones tecnológicas que respeten las exigencias jurídicas y archivísticas, evitando el riesgo de que la innovación tecnológica comprometa la seguridad jurídica o los derechos fundamentales.

Por tanto, la digitalización de los parlamentos, más que un desafío tecnológico, constituye un verdadero desafío jurídico y organizativo que interpela a los principios más esenciales del constitucionalismo democrático. Superar los retos que plantea exige una acción concertada basada en el respeto a los derechos fundamentales, la preservación de la seguridad jurídica, la transparencia y la colaboración interdisciplinaria de los cuerpos técnicos parlamentarios. Solo así será posible construir parlamentos digitales legítimos, accesibles y resilientes frente a las transformaciones tecnológicas futuras.

II. INTELIGENCIA ARTIFICIAL EN LOS PARLAMENTOS: OPORTUNIDADES, RIESGOS Y LÍMITES JURÍDICOS

La irrupción de la inteligencia artificial (IA) en el ámbito parlamentario representa un cambio de paradigma en la manera en que se procesan datos, se toman decisiones administrativas y se gestiona la información legislativa. Esta tecnología emergente ofrece enormes oportunidades para mejorar la eficiencia, la transparencia y la calidad de los servicios parlamentarios, pero también introduce riesgos relevantes que afectan a derechos fundamentales y principios democráticos esenciales[7].

[7] Floridi, L., Cowls, J., Beltrametti, M., Chatila, R., Chazerand, P., Dignum, V., … & Vayena, E. (2018). AI4People—An Ethical Framework for a Good AI Society. *Minds and Machines*, 28(4), 689–707.

2.1. La IA como herramienta de transformación en los parlamentos

Los parlamentos están comenzando a adoptar soluciones de inteligencia artificial en múltiples áreas de su actividad institucional. Estas aplicaciones incluyen, entre otras:

— Sistemas de gestión documental inteligente: utilización de algoritmos de *machine learning* para clasificar, indexar y recuperar documentos parlamentarios de manera eficiente.
— Análisis legislativo automatizado: empleo de IA para evaluar el impacto de propuestas legislativas, identificar inconsistencias normativas y ofrecer sugerencias de mejora en los proyectos de ley.
— Asistentes virtuales: implementación de *chatbots* y asistentes conversacionales para facilitar a los ciudadanos el acceso a información parlamentaria y normativa.
— Detección de desinformación: uso de algoritmos para identificar y contrarrestar campañas de desinformación que puedan afectar al debate público o al proceso legislativo.
— Optimización de procesos administrativos internos: automatización de tareas rutinarias mediante robots de software (RPA) para mejorar la eficiencia de la gestión parlamentaria.

Estas aplicaciones muestran el potencial transformador de la IA en el entorno parlamentario, permitiendo liberar recursos humanos para tareas de mayor valor añadido y mejorar el servicio ofrecido a la ciudadanía[8].

No obstante, su implementación sin el debido control jurídico puede derivar en riesgos graves para los derechos fundamentales y para la legitimidad de las instituciones democráticas.

2.2. Riesgos jurídicos derivados del uso de IA en el ámbito parlamentario

El despliegue de sistemas de inteligencia artificial en los parlamentos plantea riesgos de índole jurídica que deben ser cuidadosamente valorados:

a) Opacidad algorítmica y falta de transparencia

Uno de los principales problemas asociados al uso de IA es la dificultad para comprender el funcionamiento interno de los algoritmos, fenómeno conocido

[8] Calo, R. (2017). Artificial Intelligence Policy: A Roadmap. *University of California, Davis Law Review*, *51*(2).

como «caja negra algorítmica»[9]. Esta opacidad puede comprometer el principio de transparencia parlamentaria y dificultar la rendición de cuentas.

b) Discriminación algorítmica y sesgos

Los sistemas de IA pueden reproducir y amplificar sesgos existentes en los datos de entrenamiento, generando decisiones automatizadas discriminatorias que vulneren derechos fundamentales como la igualdad ante la ley[10].

c) Vulneración del derecho a la protección de datos personales

La recolección masiva de datos personales y su tratamiento mediante IA plantea riesgos elevados de injerencias ilegítimas en la privacidad, especialmente si se utilizan técnicas de elaboración de perfiles o decisiones automatizadas sin base jurídica suficiente[11].

d) Afectación al principio de legalidad

El uso de sistemas automatizados para tareas legislativas o administrativas debe respetar escrupulosamente el principio de legalidad. La adopción de decisiones basadas exclusivamente en algoritmos sin una intervención humana significativa podría ser incompatible con las garantías constitucionales del debido proceso.

e) Riesgos para la preservación de la memoria democrática

La utilización de IA en la gestión documental plantea interrogantes sobre la autenticidad, integridad y conservación a largo plazo de los registros parlamentarios, esenciales para la preservación de la memoria democrática.

2.3. Límites jurídicos aplicables al uso de IA en los parlamentos

Para garantizar que el uso de la inteligencia artificial en los parlamentos sea compatible con el Estado de Derecho y los derechos fundamentales, deben observarse estrictos límites jurídicos, derivados tanto del derecho interno como del derecho internacional:

---

[9] Burrell, J. (2016). How the machine 'thinks': Understanding opacity in machine learning algorithms. *Big Data & Society*, *3*(1).

[10] Eubanks, V. (2018). *Automating Inequality: How High-Tech Tools Profile, Police, and Punish the Poor.* St. Martin's Press.

[11] Rodotà, S. (2004). *La vida y las reglas: entre el derecho y lo no justo*. Trotta.

a) Cumplimiento del Reglamento General de Protección de Datos (RGPD)

El RGPD establece reglas estrictas sobre el tratamiento de datos personales mediante sistemas automatizados, incluyendo:

— Principio de transparencia (art. 5 RGPD): obligación de informar claramente sobre el funcionamiento de los algoritmos y su impacto en los interesados.
— Derecho a no ser objeto de decisiones automatizadas (art. 22 RGPD): los ciudadanos tienen derecho a no ser sometidos a decisiones basadas únicamente en tratamientos automatizados que produzcan efectos jurídicos o les afecten significativamente.
— Evaluaciones de impacto (art. 35 RGPD): obligación de realizar evaluaciones de impacto en protección de datos antes de implantar tecnologías que puedan suponer un alto riesgo.

b) Principio de explicación

Los sistemas de IA empleados en el entorno parlamentario deben ser explicables, es decir, deben permitir comprender, en términos razonables, la lógica de sus decisiones o recomendaciones[12].

Este principio se deriva de los requisitos de transparencia, rendición de cuentas y no discriminación que informan tanto el derecho constitucional como la legislación ordinaria aplicable a los parlamentos.

c) Principio de intervención humana significativa

El uso de IA no debe sustituir la responsabilidad humana en los procedimientos parlamentarios. En especial, las decisiones de relevancia política o jurídica deben ser adoptadas por personas físicas debidamente autorizadas, y no por sistemas automatizados, conforme al principio de intervención humana significativa[13].

d) Principio de finalidad y minimización de datos

Conforme al RGPD, los datos personales utilizados en sistemas de IA parlamentarios deben ser recogidos para fines específicos, explícitos y legítimos, y su tratamiento debe limitarse a lo estrictamente necesario para dichos fines (art. 5 RGPD).

---

[12] Goodman, B., & Flaxman, S. (2017). European Union regulations on algorithmic decision-making and a «right to explanation». *AI Magazine*, *38*(3).

[13] Comisión Europea (2021). *Proposal for a Regulation Laying Down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act)*.

e) Garantía de conservación de documentos públicos

La utilización de IA en la gestión documental debe asegurar la preservación de la autenticidad, integridad, disponibilidad y accesibilidad de los documentos públicos a largo plazo, conforme a los estándares archivísticos internacionales y a la legislación sobre patrimonio documental.

2.4. Principios éticos y guías internacionales sobre IA en parlamentos

Diversas organizaciones internacionales han emitido directrices y principios éticos aplicables al uso de IA en entornos públicos y parlamentarios. Entre ellos destacan:

— Principios de la OCDE sobre inteligencia artificial (2019): establecen que los sistemas de IA deben ser transparentes, explicables, robustos y sujetos a supervisión humana.
— Directrices de Ética de la Comisión Europea sobre IA confiable (2019): identifican requisitos esenciales como la agencia y supervisión humana, la transparencia, la diversidad y la equidad.
— Carta de Derechos Digitales de la Unión Europea: refuerza los derechos fundamentales en el entorno digital, incluyendo límites al uso de IA.

La adecuación de los parlamentos a estos principios es fundamental para preservar su legitimidad democrática en la era digital.

2.5. El papel de los cuerpos técnicos en la implantación responsable de IA

Como ha quedado expuesto más arriba, la implantación de IA en los parlamentos, al igual que en el resto de aspectos de su digitalización, exige una colaboración interdisciplinaria:

a) Letrados parlamentarios: garantes de la legalidad, los derechos fundamentales y la calidad normativa

Los letrados parlamentarios desempeñan un papel insustituible en la integración jurídica de los sistemas de inteligencia artificial en el entorno parlamentario. Como asesores jurídicos principales de las Cámaras legislativas, les corresponde verificar que cualquier tecnología implantada respete las normas constitucionales, estatutarias y reglamentarias que rigen la acti-

vidad parlamentaria. Esta tarea se vuelve especialmente delicada cuando se introducen herramientas de IA capaces de influir directa o indirectamente en procedimientos legislativos, mecanismos de control, o en el tratamiento de datos personales.

Uno de los cometidos fundamentales de los letrados es el control de legalidad. En el caso de la IA, esto supone analizar, desde una perspectiva jurídica, los algoritmos empleados, los datos tratados y los fines perseguidos, evaluando si el sistema cumple con las exigencias del principio de legalidad, el respeto al debido proceso y la garantía de los derechos fundamentales. Los letrados deben emitir informes jurídicos sobre la procedencia de los tratamientos automatizados, identificar posibles incompatibilidades normativas y recomendar, en su caso, modificaciones reglamentarias.

Además, los letrados deben vigilar el cumplimiento del Reglamento General de Protección de Datos (RGPD) y de la Ley Orgánica 3/2018, incluyendo la necesidad de realizar evaluaciones de impacto, delimitar las bases jurídicas del tratamiento y garantizar la intervención humana en decisiones con efectos jurídicos relevantes.

Otro ámbito clave es el de la calidad normativa, especialmente cuando se introducen sistemas de IA para analizar o redactar textos legislativos. En estos casos, los letrados deben asegurarse de que las propuestas generadas o evaluadas por algoritmos respeten los principios de jerarquía normativa, coherencia del ordenamiento y técnica legislativa, evitando que se erosionen las competencias exclusivas del legislador humano.

Por tanto, los letrados no solo son garantes de legalidad, sino actores estratégicos que deben liderar el diseño jurídico de una IA parlamentaria legítima, transparente y controlada, asegurando que la innovación tecnológica no contravenga los principios básicos del Estado de Derecho.

b) Archiveros-documentalistas: custodios de la memoria institucional y responsables de la gestión documental fiable

En el proceso de incorporación de inteligencia artificial a los parlamentos, los archiveros-documentalistas desempeñan un papel esencial en lo que respecta a la organización, conservación y autenticidad de la información parlamentaria. Su función es especialmente crítica cuando se utilizan algoritmos para gestionar grandes volúmenes de documentos legislativos, actas, intervenciones, informes y expedientes administrativos.

Uno de los desafíos más importantes es asegurar que los sistemas de IA respeten los principios archivísticos de autenticidad, integridad, fiabilidad y accesibilidad. Esto implica que los documentos procesados por inteligencia artificial mantengan sus características esenciales para ser considerados como prueba válida de los actos parlamentarios, tanto en el presente como en el futuro. La intervención de los archiveros es indispensable para definir metadatos estructurados, normas de descripción y taxonomías que per-

mitan una clasificación automatizada sin pérdida de contexto jurídico o institucional.

En la dimensión de la preservación digital a largo plazo, los archiveros deben evaluar si los sistemas de IA cumplen con estándares internacionales como el modelo OAIS (Open Archival Information System) y con las directrices de ISO 14721. Dado que los algoritmos pueden modificar o resumir contenidos, es fundamental que existan procedimientos que garanticen la conservación del documento original, y que cualquier proceso de procesamiento automatizado deje trazabilidad completa, con constancia de las acciones realizadas.

Los archiveros también son responsables de garantizar que la transparencia documental no se vea afectada por la opacidad algorítmica. En este sentido, deben colaborar en la documentación del funcionamiento de los algoritmos empleados para la recuperación o clasificación de información, asegurando que los ciudadanos y los investigadores puedan acceder a la información de manera comprensible y fiable.

Finalmente, deben colaborar con los letrados y los técnicos informáticos para que las herramientas de IA sean diseñadas teniendo en cuenta las necesidades archivísticas desde el inicio, evitando que los desarrollos tecnológicos comprometan la conservación de la memoria institucional o el cumplimiento de la normativa sobre patrimonio documental y acceso a la información pública.

c) Informáticos parlamentarios: diseñadores de sistemas seguros, explicables y alineados con los principios constitucionales

El personal informático de los parlamentos tiene la responsabilidad técnica de implementar y mantener los sistemas de inteligencia artificial, asegurando que estos funcionen de manera eficiente, segura y conforme a los principios legales y éticos definidos por el marco normativo. Su papel es estratégico en la fase de diseño, desarrollo, implantación y monitorización de soluciones tecnológicas que afectan al funcionamiento institucional y a los derechos de los ciudadanos.

Uno de los principales retos que enfrentan los informáticos parlamentarios es garantizar la seguridad de la información, evitando accesos no autorizados, fugas de datos o manipulaciones indebidas en los sistemas que manejan datos sensibles o registros oficiales. Esto implica la aplicación de políticas robustas de ciberseguridad, protocolos de autenticación, sistemas de cifrado y pruebas continuas de vulnerabilidades, todo ello conforme al Esquema Nacional de Seguridad (ENS) y a las mejores prácticas internacionales en materia de seguridad TIC.

En lo relativo a los sistemas de IA, los informáticos deben aplicar principios de explicación y trazabilidad algorítmica, diseñando soluciones que permitan comprender y auditar los criterios mediante los cuales los algoritmos

toman decisiones o procesan información. Esto es especialmente importante en entornos parlamentarios, donde la rendición de cuentas y la transparencia institucional son pilares del sistema democrático.

También les corresponde, en estrecha colaboración con el DPD, aplicar metodologías de desarrollo que incorporen desde el inicio el enfoque «protección de datos desde el diseño y por defectos» exigido por el RGPD, lo cual supone garantizar que la protección de datos esté integrada estructuralmente en cada fase del diseño del sistema.

Por último, deben asegurar la interoperabilidad entre sistemas parlamentarios y otras plataformas públicas, garantizar el cumplimiento de estándares abiertos y contribuir al desarrollo de soluciones tecnológicas accesibles, inclusivas y alineadas con los objetivos institucionales. La colaboración continua con los letrados y archiveros resulta imprescindible para que las soluciones tecnológicas respondan no solo a criterios de funcionalidad, sino también de legalidad y sostenibilidad.

III. PROTECCIÓN DE DATOS PERSONALES EN EL ENTORNO PARLAMENTARIO DIGITAL: OBLIGACIONES NORMATIVAS Y DESAFÍOS OPERATIVOS

La progresiva digitalización de los parlamentos y la incorporación de tecnologías emergentes, como la inteligencia artificial, han multiplicado exponencialmente el volumen, la variedad y la velocidad de los datos tratados por estas instituciones. En este contexto, el tratamiento de datos personales se ha convertido en un eje central de la acción parlamentaria, no solo desde una perspectiva administrativa, sino también como garante de los derechos fundamentales de los ciudadanos y de los propios parlamentarios. La protección de datos se erige, así, en un requisito estructural del funcionamiento parlamentario en la era digital[14].

En este trabajo examinaremos las obligaciones derivadas del Reglamento General de Protección de Datos (RGPD) y de la Ley Orgánica 3/2018 en el contexto parlamentario, con especial atención a las singularidades institucionales de las Cámaras legislativas y en relación con los desafíos técnicos y organizativos que conlleva el cumplimiento efectivo de estas normas. Asimismo, propondremos criterios de actuación adaptados a la realidad institucional parlamentaria.

[14] Bygrave, L. A. (2014). *Data Protection Law: Approaching Its Rationale, Logic and Limits* (2nd ed.). Oxford University Press.

3.1. El Parlamento como responsable del tratamiento de datos

Los parlamentos, en tanto órganos constitucionales dotados de autonomía organizativa, son considerados responsables del tratamiento de datos personales en los términos del artículo 4.7 del RGPD. Esta responsabilidad implica que deben determinar los fines y medios del tratamiento, asumiendo directamente las obligaciones legales derivadas del marco normativo de protección de datos.

La actividad parlamentaria implica múltiples tratamientos de datos personales, entre los cuales pueden destacarse:

— Registro y publicación de iniciativas parlamentarias, preguntas, intervenciones y votos nominativos.
— Gestión administrativa del personal, tanto parlamentario como de apoyo técnico.
— Tramitación de solicitudes de información ciudadana.
— Gestión de archivos audiovisuales de sesiones parlamentarias.
— Aplicación de herramientas de inteligencia artificial y análisis de datos.

Dada la naturaleza pública y constitucional de los parlamentos, la legitimidad de estos tratamientos suele estar amparada en misiones de interés público o en el ejercicio de poderes públicos, conforme al artículo 6.1.e) del RGPD. No obstante, esta base jurídica no exime del cumplimiento de los principios rectores de la normativa de protección de datos.

3.2. Principios aplicables al tratamiento parlamentario de datos personales

El RGPD establece una serie de principios fundamentales que deben observarse en todo tratamiento de datos personales, también en el contexto parlamentario. Estos principios son:

a) Licitud, lealtad y transparencia (art. 5.1.a RGPD)

El tratamiento debe ser legítimo, leal y transparente con respecto a los interesados. En el caso parlamentario, esto implica garantizar que los ciudadanos, parlamentarios y trabajadores conozcan claramente qué datos se recogen, con qué fines, durante cuánto tiempo se conservan y con qué medidas de seguridad se protegen (arts. 13 y 14 RGPD). Las políticas de privacidad institucionales deben ser accesibles, comprensibles y actualizadas.

b) Limitación de la finalidad (art. 5.1.b RGPD)

Los datos solo pueden tratarse para fines determinados, explícitos y legítimos. En los parlamentos, esto exige delimitar con precisión los objetivos de cada tratamiento, evitando usos secundarios incompatibles, como la reutilización de grabaciones parlamentarias para fines comerciales o partidistas.

c) Minimización de datos (art. 5.1.c RGPD)

Deben tratarse únicamente los datos estrictamente necesarios para los fines perseguidos. La incorporación de sistemas de IA puede inducir a una sobre-recolección de datos («data creep»), por lo que resulta esencial diseñar sistemas con enfoque de minimización por defecto.

d) Exactitud (art. 5.1.d RGPD)

Los datos deben ser exactos y estar actualizados. Esto es relevante en registros públicos parlamentarios, ya que la publicación de información inexacta sobre votaciones o iniciativas puede tener consecuencias reputacionales y jurídicas.

e) Limitación del plazo de conservación (art. 5.1.e RGPD)

Los datos no deben conservarse más tiempo del necesario. En el ámbito parlamentario, esta obligación debe compatibilizarse con las exigencias archivísticas de conservación permanente de ciertos documentos como patrimonio documental público.

f) Integridad y confidencialidad (art. 5.1.f RGPD)

Deben adoptarse medidas técnicas y organizativas adecuadas para proteger los datos frente a accesos no autorizados, pérdida o destrucción. La seguridad de los sistemas digitales parlamentarios debe ser máxima, habida cuenta de la sensibilidad institucional de muchos de sus datos.

g) Responsabilidad proactiva *(accountability)* (art. 5.2 RGPD)

El responsable debe ser capaz de demostrar el cumplimiento de todos estos principios. Esto implica una gestión activa de cumplimiento, incluyendo documentación, auditorías internas, y formación continua del personal parlamentario.

3.3. Singularidades del tratamiento parlamentario de datos

El cumplimiento del RGPD en el contexto parlamentario presenta peculiaridades relevantes, derivadas de la especial posición constitucional de las Cámaras legislativas y de su autonomía institucional.

a) Autonomía normativa, pero plena sujeción al control externo pleno

A diferencia de las Administraciones públicas ordinarias, los parlamentos gozan de autonomía para regular sus propios procedimientos internos, no obstante, ello no plantea interrogantes sobre la aplicación directa de determinadas obligaciones del RGPD, como la supervisión por parte de las autoridad de control (AEPD y autoridades autonómicas de protección de datos).

b) Tratamientos derivados del ejercicio de la función parlamentaria

Cuando el tratamiento de datos personales se produce directamente en el ejercicio de funciones legislativas o de control político (por ejemplo, publicación de intervenciones o registro de votos), existe un interés constitucional superior que puede modular la aplicación de ciertos derechos individuales, como el derecho de supresión o rectificación.

c) Difusión de datos a través de canales institucionales

La obligación de publicidad parlamentaria puede entrar en tensión con los principios de minimización y confidencialidad. Es fundamental que los canales institucionales (webs, archivos audiovisuales, redes sociales) se gestionen conforme a directrices claras sobre qué información puede y debe ser difundida y durante cuánto tiempo, procurando, al mismo tiempo, que la base legitimadora del tratamiento sea clara, transparente y pública.

d) Tratamiento de datos de menores, colectivos vulnerables o personas en situaciones sensibles

Las comparecencias parlamentarias o la actividad institucional pueden implicar la mención de datos sensibles o la participación de personas en situación de especial protección. En estos casos, se requiere una protección reforzada conforme al artículo 9 del RGPD y a los principios de ética institucional. Ello no obstante, la libertad de expresión inherente al debate parlamentario y la utilización de vídeos y presentaciones que sustituyen, en ocasiones, a las intervenciones de viva voz, hacen que las medidas técnicas y organizativas adoptadas por los parlamentos puedan llegar a ser insuficientes para la salvaguarda de los datos personales, siendo necesario responsabilizar también al compareciente del necesario respeto a la protección de datos de terceros.

3.4. Evaluaciones de impacto y medidas de seguridad

Uno de los instrumentos clave para garantizar el cumplimiento normativo en el ámbito parlamentario es la realización de Evaluaciones de Impacto en Protección de Datos (EIPD). El artículo 35 del RGPD exige llevarlas a cabo cuando el tratamiento pueda entrañar un alto riesgo para los derechos y libertades de las personas físicas, especialmente cuando se utilicen nuevas tecnologías.

En el entorno parlamentario, deben considerarse de alto riesgo, entre otros:

— El uso de algoritmos para analizar la actividad legislativa.
— La publicación en línea de grandes volúmenes de datos personales no anonimizados.

Las EIPD deben ser elaboradas por un equipo interdisciplinar que incluya al DPD, a responsables jurídicos (letrados) y a expertos técnicos (informáticos), así como a los archiveros-documentalistas cuando el tratamiento afecte a fondos documentales. Esta colaboración garantiza una visión holística del riesgo y permite diseñar medidas de mitigación eficaces.

Entre las medidas técnicas y organizativas que deben implementarse en entornos parlamentarios destacan:

— Segmentación de accesos y control de privilegios.
— Registro de actividades de tratamiento.
— Cifrado de bases de datos sensibles.
— Trazabilidad y auditoría de las operaciones algorítmicas.
— Protocolos de anonimización o seudonimización de datos en registros públicos.

3.5. Derechos de los interesados y su garantía en el ámbito parlamentario

El RGPD reconoce a los ciudadanos una serie de derechos en relación con sus datos personales, entre los que se incluyen el derecho de acceso, rectificación, supresión (derecho al olvido), limitación del tratamiento, portabilidad y oposición (arts. 15 a 21 RGPD). La efectividad de estos derechos en el entorno parlamentario presenta particularidades derivadas de la tensión entre el principio de transparencia institucional y la protección individual.

a) Derecho de acceso

Todo interesado puede solicitar información sobre si sus datos están siendo tratados por el parlamento, los fines de dicho tratamiento, su origen y

los destinatarios. Para garantizar su ejercicio, las instituciones parlamentarias deben disponer de procedimientos ágiles y accesibles, lo que incluye la habilitación de canales electrónicos seguros para la presentación de solicitudes y la verificación de identidad.

b) Derecho de rectificación y supresión

Si bien estos derechos son plenamente exigibles en el ámbito administrativo parlamentario (por ejemplo, en la gestión de recursos humanos), su aplicación a contenidos derivados de la función parlamentaria (intervenciones, votaciones, publicaciones en diarios de sesiones) debe valorarse con cautela. En algunos casos, como se ha señalado, puede prevalecer el interés público en la preservación del contenido original, por lo que la supresión podría no proceder.

c) Derecho de oposición y tratamiento automatizado

El artículo 22 del RGPD prevé que los interesados puedan oponerse a decisiones basadas únicamente en tratamientos automatizados, incluida la elaboración de perfiles. Si se emplean sistemas de IA en la tramitación de información ciudadana o en procesos internos, el parlamento debe garantizar que no se adopten decisiones con efectos jurídicos sin intervención humana significativa y que se respeten los derechos de impugnación y revisión.

d) Derecho a la información

Uno de los aspectos clave en el cumplimiento del RGPD es proporcionar información clara, completa y actualizada sobre los tratamientos realizados. Para ello, los parlamentos deben desarrollar registros públicos de actividades de tratamiento, avisos de privacidad específicos por área, y materiales divulgativos adaptados a distintos perfiles de usuarios (ciudadanos, trabajadores, parlamentarios, proveedores).

3.6. El Delegado de Protección de Datos (DPD) en los parlamentos

El DPD es una figura clave en la gobernanza de la privacidad y la protección de datos. Su designación es obligatoria en el sector público conforme al artículo 37.1.a) del RGPD, y su perfil debe reunir independencia funcional, conocimientos especializados y capacidad operativa. En los parlamentos, el DPD debe actuar como un puente entre los distintos cuerpos técnicos, asegurando el cumplimiento normativo de forma transversal.

Las funciones del DPD incluyen:

— Asesorar a los responsables y encargados del tratamiento.
— Supervisar el cumplimiento del RGPD y de las políticas internas.
— Coordinar evaluaciones de impacto.
— Actuar como punto de contacto con la autoridad de control.
— Promover la cultura de protección de datos a través de formación y sensibilización.

En los parlamentos, su independencia debe ser garantizada también frente a los órganos políticos, lo que refuerza su papel institucional como garante del derecho fundamental a la protección de datos. En algunos casos, como en el Parlamento Europeo o en el Bundestag alemán, se han consolidado estructuras de gobernanza robustas con unidades internas de protección de datos dotadas de autonomía y recursos, situación muy alejada de la existente en los parlamentos españoles, donde los DPD, además de sus funciones propias, realizan otras funciones adicionales, con merma de su tiempo para la supervisión y el asesoramiento en protección de datos y carecen de recursos adecuados para el correcto desempeño de esta actividad que, a menudo, se considera accesoria y ni principal. Sin embargo, el tratamiento de datos personales en el contexto de la actividad parlamentaria digital representa uno de los desafíos jurídicos más complejos de nuestro tiempo. La aplicación del RGPD y de la legislación nacional exige adaptar los principios generales de protección de datos a la singular naturaleza institucional de los parlamentos, conjugando la transparencia y publicidad propias de la función parlamentaria con la protección de la intimidad, la seguridad de la información y la dignidad de las personas.

Este equilibrio requiere no solo un marco normativo claro, sino también una gestión organizativa eficaz, basada en la colaboración entre cuerpos técnicos (letrados, archiveros, informáticos) y en el liderazgo del DPD. A medida que se incorporen tecnologías cada vez más sofisticadas —como la inteligencia artificial o el análisis predictivo—, la necesidad de un enfoque proactivo, ético y jurídicamente robusto se vuelve aún más acuciante.

En definitiva, proteger los datos personales en el entorno parlamentario no es solo una obligación legal: es una condición de posibilidad para la legitimidad democrática en la era digital.

IV. EL REGLAMENTO EUROPEO DE INTELIGENCIA ARTIFICIAL (RIA) Y SU IMPACTO EN LOS PARLAMENTOS: IMPLICACIONES JURÍDICAS, ORGANIZATIVAS Y TÉCNICAS

La reciente aprobación del Reglamento Europeo de Inteligencia Artificial (RIA) por parte de la Unión Europea marca un hito normativo de primer orden. Se trata del primer marco legal integral a nivel mundial que regula el desarrollo, comercialización y uso de sistemas de inteligencia artificial, adoptando un enfoque basado en el riesgo para garantizar que estos sistemas respeten los derechos fundamentales, la seguridad y los valores democráticos[15].

Aunque el RIA se ha concebido principalmente para operadores económicos, sus disposiciones resultan plenamente aplicables también a entidades del sector público, incluidos los parlamentos nacionales y regionales, en la medida en que desarrollen, adquieran o utilicen sistemas de IA en el ejercicio de sus funciones administrativas o de apoyo institucional.

Esta sección analiza las implicaciones del RIA para los parlamentos, desde una triple perspectiva: jurídica, en cuanto a las obligaciones normativas que impone; organizativa, respecto a los cambios que exige en las estructuras y procesos internos; y técnica, en relación con los criterios de diseño, auditoría y supervisión de los sistemas de inteligencia artificial utilizados en el entorno parlamentario.

La relativamente reciente aprobación del RIA ha determinado la ausencia de abundante bibliografía acerca de su implantación en el entorno parlamentario, por lo que en el desarrollo sucesivo del presente trabajo nos ceñiremos a las referencias oportunas al propio RIA y al desarrollo de sugerencias propias basadas en la normativa que consideramos de aplicación.

4.1. Naturaleza y objetivos del RIA

El RIA establece un marco armonizado para el desarrollo y utilización de sistemas de IA en la Unión Europea. Su objetivo es doble: por un lado, fomentar la innovación responsable y el liderazgo tecnológico europeo en el campo de la IA y por otro, prevenir los riesgos que los sistemas de IA pueden suponer para los derechos fundamentales, la seguridad, la democracia y el Estado de Derecho.

Para ello, el Reglamento introduce un sistema de clasificación por niveles de riesgo, aplicando exigencias más estrictas a los sistemas de alto riesgo,

[15] Comisión Europea. (2021). *Proposal for a Regulation laying down harmonised rules on Artificial Intelligence (Artificial Intelligence Act)*, COM(2021) 206 final.

prohibiendo determinadas aplicaciones nocivas y estableciendo obligaciones horizontales de transparencia y supervisión.

Entre los principios que guían el Reglamento IA destacan:

— Respeto a los derechos fundamentales reconocidos en la Carta de Derechos Fundamentales de la UE.
— Transparencia, trazabilidad y explicación de los sistemas de IA.
— Supervisión humana significativa.
— Proporcionalidad y minimización de riesgos.
— Seguridad y solidez técnica.

4.2. Aplicabilidad del RIA a los parlamentos

Aunque los parlamentos disfrutan de un estatuto institucional autónomo, el RIA les resulta aplicable cuando actúan como usuarios o desarrolladores de sistemas de IA en el ejercicio de funciones administrativas, especialmente en las áreas de:

— Gestión documental y archivística.
— Tramitación automatizada de solicitudes ciudadanas.
— Análisis predictivo de textos legislativos.
— Asistentes virtuales para consulta normativa.
— Sistemas de vigilancia física (por ejemplo, control de accesos mediante IA).

Es importante subrayar que las funciones estrictamente legislativas (como el debate, la votación o la iniciativa legislativa) no están directamente sujetas al Reglamento, conforme al principio de separación de poderes. No obstante, el uso de sistemas de IA en tareas de apoyo técnico o administrativo a esas funciones sí puede estarlo, lo que obliga a delimitar claramente los ámbitos de aplicación interna.

En consecuencia, las Mesas de las Cámaras y las unidades de innovación tecnológica deben adoptar medidas para asegurar el cumplimiento del RIA en los procesos institucionales que involucren inteligencia artificial, garantizando una separación funcional y normativa entre las tareas parlamentarias puras y las funciones administrativas sujetas a regulación.

4.3. Clasificación de sistemas de IA en función del riesgo

El elemento central del RIA es su clasificación de los sistemas de IA según el nivel de riesgo que presentan para los derechos y la seguridad. Esta categorización condiciona el régimen jurídico aplicable y tiene repercusiones directas en los entornos parlamentarios:

a) Sistemas prohibidos (art. 5 RIA)

Se prohíben determinados sistemas de IA por considerarse incompatibles con los valores europeos, como:

— Sistemas de puntuación social masiva.
— Manipulación cognitiva subliminal.
— Identificación biométrica remota en tiempo real en espacios públicos (con excepciones).

Los parlamentos deben garantizar que no adquieren ni integran indirectamente este tipo de sistemas, incluso cuando provengan de proveedores externos.

b) Sistemas de alto riesgo (arts. 6 a 29 RIA)

Incluyen los sistemas utilizados en infraestructuras críticas, educación, empleo, servicios públicos y administración pública. En el caso parlamentario, podrían ser considerados de alto riesgo:

— Sistemas de IA que analicen o clasifiquen intervenciones parlamentarias.
— Plataformas que gestionen datos personales sensibles o votaciones internas.
— Aplicaciones de análisis predictivo legislativo con incidencia directa en decisiones administrativas.

Estos sistemas están sujetos a exigencias estrictas: registro obligatorio, gestión del ciclo de vida del sistema, gobernanza de datos, documentación técnica, supervisión humana y evaluación ex ante del impacto.

c) Sistemas de riesgo limitado o mínimo

Para herramientas como *chatbots* institucionales o sistemas de clasificación documental sin efectos jurídicos, el Reglamento establece obligaciones atenuadas: principalmente información clara al usuario y medidas de transparencia algorítmica.

Los parlamentos deben realizar un mapeo interno de los sistemas de IA empleados, clasificándolos conforme a estas categorías y aplicando los requisitos correspondientes, bajo la supervisión del órgano competente de cumplimiento normativo.

4.4. Obligaciones jurídicas para los parlamentos en el uso de IA

Cuando los parlamentos utilicen o desarrollen sistemas de inteligencia artificial que encajen en las categorías reguladas por el Reglamento IA, adquieren una serie de obligaciones jurídicas específicas, que requieren un rediseño profundo de los procedimientos técnicos, jurídicos y organizativos.

a) Evaluación de conformidad y documentación técnica

Los parlamentos deben realizar una evaluación de conformidad previa al uso de sistemas de IA de alto riesgo, lo que implica:

— Verificar que el sistema cumple con los requisitos esenciales del RIA (calidad de los datos, trazabilidad, seguridad, supervisión humana, etc.).
— Elaborar una documentación técnica detallada, incluyendo su arquitectura, fuentes de datos, lógica algorítmica, mecanismos de corrección y medidas de mitigación de riesgos.
— Mantener registros de uso, con trazabilidad completa de cada fase de desarrollo, implementación y operación.

b) Gestión de riesgos y gobernanza de datos

El Reglamento obliga a establecer sistemas internos de gestión de riesgos, que identifiquen, evalúen y mitiguen los posibles efectos adversos de la IA en los derechos fundamentales y en la seguridad institucional.

Esto implica adoptar políticas de:

— Calidad y representatividad de los datos utilizados.
— Detección y corrección de sesgos algorítmicos.
— Pruebas periódicas de robustez, resiliencia y precisión del sistema.
— Auditorías internas o externas independientes sobre el funcionamiento del sistema.

c) Supervisión humana significativa

Todo sistema de IA debe estar sometido a una supervisión humana efectiva, que permita intervenir o revertir decisiones automatizadas. En el contexto parlamentario, esto requiere:

— Formación específica del personal responsable de los sistemas de IA.
— Procedimientos claros de revisión humana ante decisiones críticas.
— Limitaciones al uso de IA sin intervención previa en procedimientos sensibles (como licitaciones, nombramientos, gestión de personal o análisis de propuestas legislativas).

d) Transparencia y deber de información

El RIA impone el deber de garantizar que los usuarios —internos o externos— sean conscientes de que están interactuando con un sistema de inteligencia artificial.

Esto incluye:

— Etiquetado claro de los sistemas automatizados.
— Políticas de transparencia algorítmica accesibles y comprensibles.
— Explicación del funcionamiento básico del sistema y de sus impactos previsibles.

e) Designación de personas o unidades de cumplimiento

Las entidades sujetas al Reglamento deben designar oficiales o unidades responsables del cumplimiento normativo en materia de IA. En el ámbito parlamentario, esta función puede recaer en una unidad conjunta entre servicios jurídicos, informáticos y el Delegado de Protección de Datos, o bien en una Oficina Técnica de Supervisión Algorítmica, similar a la prevista en algunas administraciones públicas europeas.

4.5. Impacto organizativo del RIA en los parlamentos

La aplicación del Reglamento IA exige a los parlamentos reformular su estructura organizativa interna, de forma que puedan asumir de manera eficaz las nuevas obligaciones. Esto supone:

a) Creación de protocolos internos

Los parlamentos deben adoptar protocolos institucionales para el uso de IA, que regulen:

— La adquisición de soluciones externas.
— Los procedimientos de evaluación de conformidad.
— La gestión de incidencias o brechas de funcionamiento.
— Las relaciones con los proveedores y la supervisión de contratos tecnológicos.

b) Capacitación del personal jurídico y técnico

La implementación responsable de IA requiere una formación transversal:

— Los letrados parlamentarios deben adquirir competencias en gobernanza algorítmica y supervisión jurídica de sistemas inteligentes.
— Los informáticos parlamentarios deben especializarse en cumplimiento normativo, seguridad funcional y documentación algorítmica.

— Los archiveros-documentalistas deben garantizar la conservación y trazabilidad de los *outputs* generados por IA, asegurando que los documentos producidos son auténticos, íntegros y susceptibles de ser archivados conforme a los estándares legales.

c) Gobernanza ética de la IA

Más allá del cumplimiento normativo, los parlamentos, dada su función representativa de la ciudadanía, están llamados a convertirse en referentes éticos en el uso de tecnología, lo cual implica:

— Adoptar cartas o códigos éticos sobre el uso de IA.
— Establecer comités internos de evaluación ética.
— Promover el uso de IA como instrumento de fortalecimiento democrático y no como mera herramienta de eficiencia técnica.

La entrada en vigor del RIA inaugura una nueva etapa en la gobernanza jurídica de las tecnologías emergentes, que afecta de manera directa a las instituciones parlamentarias. A partir de ahora, los parlamentos no solo deberán ser espacios de debate legislativo sobre los desafíos éticos y sociales de la IA, sino también sujetos activos de cumplimiento normativo cuando utilicen estas tecnologías en sus procesos administrativos o de apoyo institucional.

El Reglamento impone un conjunto de obligaciones complejas —evaluaciones de riesgo, supervisión humana, transparencia, documentación técnica, gobernanza de datos— que obligan a los parlamentos a desarrollar capacidades organizativas y técnicas especializadas. Esta exigencia se articula con el principio de responsabilidad proactiva, de modo que no basta con reaccionar ante fallos o incidentes, sino que debe anticiparse el riesgo desde el diseño mismo de las soluciones tecnológicas *(AI by design)*.

La correcta implementación del RIA exige, en consecuencia, una actuación coordinada e interdisciplinaria entre los cuerpos técnicos parlamentarios: los letrados deben interpretar y aplicar el marco normativo europeo e interno, estableciendo límites funcionales a los usos institucionales de la IA; los informáticos parlamentarios deben garantizar la seguridad, trazabilidad y explicación de los sistemas, alineándolos con los principios constitucionales y los archiveros-documentalistas deben asegurar la preservación, clasificación y accesibilidad de los resultados generados por la IA, evitando su opacidad.

Además, los parlamentos deben asumir un rol ejemplar en el uso democrático de la inteligencia artificial, tanto por su función representativa como por su dimensión simbólica como garantes del Estado de Derecho. El RIA ofrece una oportunidad para avanzar hacia una institucionalidad tecnológica más ética, transparente y jurídicamente robusta. Aprovechar esta oportunidad exige voluntad política, pericia técnica y liderazgo normativo.

V. HACIA UNA GOBERNANZA PARLAMENTARIA DE LA INTELIGENCIA ARTIFICIAL: MODELO INSTITUCIONAL, GARANTÍAS JURÍDICAS Y COOPERACIÓN PROFESIONAL

La consolidación de tecnologías avanzadas como la inteligencia artificial en los entornos parlamentarios ha generado no solo una transformación funcional de las instituciones, sino también una creciente necesidad de establecer marcos de gobernanza interna que aseguren el cumplimiento normativo, la protección de los derechos fundamentales y la sostenibilidad institucional de los procesos digitales.

En este contexto, el simple cumplimiento formal del RGPD o del RIA no resulta suficiente: se requiere el diseño e implantación de un modelo institucional propio, específico para los parlamentos, que combine principios jurídicos, estructuras organizativas y competencias técnicas, orientado a garantizar una gobernanza ética, transparente y legítima de la IA en el ejercicio de la función pública parlamentaria.

Esta sección propone una arquitectura de gobernanza para los parlamentos que integre criterios legales, buenas prácticas institucionales, mecanismos de control y colaboración interdisciplinaria, tomando como referencia las mejores experiencias comparadas y las exigencias del constitucionalismo digital.

5.1. Fundamentos constitucionales de la gobernanza parlamentaria en la era digital

La construcción de un modelo institucional de gobernanza de la IA en los parlamentos debe basarse en los principios constitucionales que estructuran el poder legislativo y su función de representación democrática. Entre ellos destacan:

— Soberanía popular y representación política (art. 1.2. 23.1 y 66 CE): la inteligencia artificial no puede sustituir la deliberación humana ni la función representativa de los parlamentarios.
— Legalidad, publicidad y transparencia (arts. 9.3 y 80 CE): las decisiones adoptadas mediante sistemas de IA deben cumplir con los principios de publicidad y trazabilidad.
— Derechos constitucionales (arts. 18.4 y 105 CE): toda solución tecnológica debe respetar la privacidad, el derecho a la protección de datos y el derecho de acceso a la información pública.
— Autonomía parlamentaria: garantía institucional que permite a las Cámaras dotarse de su propia organización y normas internas, lo cual les habilita a establecer estructuras específicas de gobernanza digital.

Sobre estos principios se articula la necesidad de institucionalizar mecanismos internos que no solo gestionen los aspectos tecnológicos, sino que actúen como garantes del modelo constitucional en el entorno digital parlamentario.

5.2. Arquitectura institucional propuesta para la gobernanza de la IA parlamentaria

Se propone un modelo estructurado en torno a cinco ejes institucionales interconectados, cuya función conjunta garantice la aplicación ética, jurídica y técnicamente robusta de la IA en los parlamentos:

a) Oficina de Tecnología y Ética Parlamentaria

Sería un órgano de nueva creación, de carácter técnico y autónomo, cuya misión sería:

— Evaluar los riesgos éticos, jurídicos y sociales de los sistemas de IA utilizados en el parlamento.
— Emitir dictámenes preceptivos sobre proyectos tecnológicos.
— Establecer criterios éticos vinculantes para el diseño y uso de IA.
— Actuar como canal institucional de transparencia algorítmica.

Este órgano podría integrarse dentro de la Secretaría General o funcionar como unidad transversal al servicio de todas las dependencias parlamentarias. Su composición debería ser interdisciplinar, incluyendo juristas, expertos en ética digital, archiveros, informáticos y, eventualmente, miembros de la Mesa de la Cámara.

b) Comité de Supervisión Algorítmica

Inspirado en modelos como el *Algorithmic Accountability Committee* del Reino Unido, este comité se encargaría de:

— Aprobar los planes de uso de IA en entornos parlamentarios.
— Supervisar su implementación conforme a principios constitucionales.
— Garantizar la trazabilidad, reversibilidad y explicación de los sistemas.

Podría estar adscrito a la Mesa del Parlamento o a la Secretaría General y contar con participación plural: DPD, letrados y técnicos informáticos.

c) Delegación de Protección de Datos y Transparencia Tecnológica

La figura del DPD como órgano unipersonal resulta insuficiente en el entorno de la digitalización parlamentaria con la incorporación de herramientas de IA, por ello, debe reforzarse como una unidad administrativa

colegiada, con funciones específicas en el entorno de la IA, adscribiéndole funciones como:

— Supervisar los tratamientos automatizados y realizar evaluaciones de impacto.
— Velar por el respeto al principio de intervención humana significativa.
— Informar sobre incidentes o brechas de seguridad en sistemas de IA.
— Coordinar con autoridades de control como la AEPD o las autoridades autonómicas de protección de datos.

Esta delegación debería disponer de medios personales y materiales suficientes y autonomía operativa, con acceso a toda la información relativa a proyectos de IA institucionales.

d) Colaboración de los servicios técnicos

Los cuerpos de letrados, archiveros documentalistas y técnicos informáticos deberían constituir un núcleo funcional de implementación responsable de los proyectos de IA, garantizando desde sus respectivos ámbitos:

— Conformidad normativa y coherencia jurídica (letrados).
— Seguridad técnica y trazabilidad (informáticos).
— Preservación documental y accesibilidad (archiveros).

Su coordinación efectiva exige espacios formales de trabajo conjunto, protocolos interdepartamentales y formación cruzada.

e) Red parlamentaria de cooperación tecnológica

En la Conferencia de Presidentes de Parlamentos Autonómicos (COPREPA) se ha acordado la creación de una plataforma común para poder subir y compartir herramientas tecnológicas. A ello se podría añadir la creación de una red interparlamentaria de intercambio de buenas prácticas en gobernanza de IA, integrada por Cámaras legislativas nacionales y regionales, con participación en foros como la UIP, la OCDE o la Comisión de Venecia.

Esta red permitiría generar sinergias, evaluar modelos regulatorios compartidos y promover estándares comunes de gobernanza digital parlamentaria.

5.3. Garantías jurídicas de un modelo parlamentario de IA

Todo modelo institucional de gobernanza tecnológica debe estar sustentado por un conjunto de garantías jurídicas, que aseguren su legitimidad y su conformidad con los principios constitucionales y europeos. Estas garantías pueden articularse en distintos niveles:

a) Garantías normativas

Los parlamentos deben dotarse de normas internas específicas sobre el uso de inteligencia artificial, integradas en su Reglamento parlamentario o como normativa sectorial. Estas normas deberían:

— Definir con claridad los usos permitidos y prohibidos de IA.
— Regular los procedimientos de evaluación previa y seguimiento.
— Establecer derechos de información, revisión y oposición para los afectados.
— Establecer sanciones internas o medidas correctoras por uso indebido.

Asimismo, los contratos públicos de adquisición de soluciones tecnológicas deben incluir cláusulas de compatibilidad con el RIA, el RGPD y los principios de supervisión ética, así como auditorías *ex post* del comportamiento del sistema.

b) Garantías institucionales

La independencia funcional de los órganos supervisores (como la Oficina de Tecnología o la Delegación de Protección de Datos) debe estar garantizada reglamentariamente, así como su acceso irrestricto a los sistemas, datos y documentación técnica. Esta independencia ha de incluir protección frente a injerencias políticas, autonomía presupuestaria y organizativa y capacidad para emitir informes vinculantes.

c) Garantías procedimentales

Como reiteradamente venimos exponiendo en este trabajo, todo sistema de IA utilizado en los parlamentos debe ofrecer mecanismos de explicación de decisiones automatizadas a los usuarios; revisión por parte de humanos cualificados en caso de decisiones con efectos jurídicos; acceso a los registros de decisiones algorítmicas, con trazabilidad completa y evaluación de impacto jurídica y social previa a su implementación, especialmente en contextos sensibles (por ejemplo, uso de IA para analizar discurso parlamentario o gestionar recursos humanos).

5.4. Cooperación profesional y cultura organizativa

La construcción de una gobernanza eficaz de la inteligencia artificial en los parlamentos no depende únicamente de normas o estructuras, sino de una cultura organizativa basada en la cooperación entre cuerpos técnicos y en la responsabilidad institucional compartida.

Esta cultura organizativa cooperativa requiere una formación interdisciplinar, con la promoción y realización de una formación cruzada entre los distintos profesionales implicados: letrados que comprendan principios técnicos de arquitectura algorítmica, archiveros que dominen conceptos como metadatos generados por IA, logs de aprendizaje automático o preservación de salidas dinámicas e informáticos que interioricen principios constitucionales, protección de datos y rendición de cuentas institucional.

Esta formación debe ser continua y adaptada a los retos emergentes del ecosistema digital parlamentario.

También sería recomendable la formalización de protocolos interprofesionales que regulen: evaluaciones conjuntas de proyectos de IA, diseño conjunto de políticas de privacidad, archivo y seguridad y mecanismos de revisión ética de nuevas tecnologías.

Además, los órganos de gobierno parlamentario deben fomentar espacios de deliberación y planificación conjunta entre estos cuerpos, evitando la fragmentación funcional y potenciando una visión institucional integrada.

La gobernanza parlamentaria de la IA no puede ser una responsabilidad meramente técnica. Las Presidencias y las Mesas de las Cámaras deben involucrarse activamente en aprobar marcos normativos claros, dotar de recursos a los órganos de supervisión y promover un debate democrático sobre los límites y oportunidades de la IA en el que participen expertos, ciudadanía organizada y sociedad civil.

El Parlamento, como órgano representativo por excelencia, debe convertirse en un referente ético y jurídico en el uso institucional de la inteligencia artificial.

El despliegue de la inteligencia artificial en los parlamentos plantea desafíos sin precedentes para las estructuras, los procedimientos y los valores que han guiado tradicionalmente la función legislativa. Frente a estos retos, la respuesta no puede ser improvisada ni meramente técnica, por el contrario, debe ser institucional, normativa y organizativa, y estar orientada a preservar y actualizar los principios del constitucionalismo democrático en la era digital.

La construcción de un modelo institucional de gobernanza parlamentaria de la IA, con órganos especializados, procedimientos garantistas y colaboración profesional efectiva, constituye una condición necesaria para evitar los riesgos de automatización opaca, discriminación algorítmica o erosión de los derechos fundamentales.

Por todo ello, es preciso contar con un modelo que ha de ser jurídicamente robusto con cumplimiento normativo del RGPD, el RIA y la normativa

parlamentaria interna; ética y políticamente comprometido, con la participación de todos los actores institucionales; técnicamente viable y sostenible, adaptado a las capacidades y recursos de cada parlamento y transparente y participativo, abierto al control ciudadano y al escrutinio público.

En última instancia, se trata de asumir que el Parlamento no solo debe legislar sobre inteligencia artificial, sino también dar ejemplo en su aplicación responsable, en coherencia con su función de garante de la democracia y de los derechos fundamentales.

En definitiva, la transformación digital de los parlamentos, impulsada por la incorporación de tecnologías avanzadas como la inteligencia artificial, marca un punto de inflexión en la configuración institucional de las democracias contemporáneas. Este proceso, lejos de ser meramente técnico o administrativo, plantea profundos retos jurídicos, éticos y organizativos que afectan a la esencia misma de la función representativa y a los derechos fundamentales de la ciudadanía.

A lo largo de este trabajo se ha tratado de poner de manifiesto que la digitalización parlamentaria, la gestión documental electrónica, el uso institucional de sistemas de inteligencia artificial y la aplicación del RGPD y del RIA exigen una reconfiguración del modelo de gobernanza interna de los parlamentos. No basta con adoptar las tecnologías, es necesario rediseñar procedimientos, estructuras, garantías y relaciones interprofesionales.

En este escenario, se hace evidente que la colaboración entre los tres cuerpos técnicos clave de las cámaras legislativas —letrados, archiveros-documentalistas e informáticos— no es solo conveniente, sino imprescindible. Cada uno aporta un conjunto de competencias y responsabilidades insustituibles, y solo su cooperación efectiva puede asegurar que la innovación tecnológica no socave la legalidad, la memoria institucional ni los derechos de las personas.

Los letrados parlamentarios tienen la misión de garantizar la legalidad del proceso de transformación digital, asegurar la conformidad con el ordenamiento jurídico interno y europeo, y preservar los principios constitucionales en el diseño y uso de tecnologías disruptivas. Es una función de la máxima relevancia por cuanto les corresponde velar por el sistema constitucional mismo.

Los archiveros-documentalistas constituyen los garantes de la autenticidad, integridad, accesibilidad y conservación de la documentación parlamentaria, asegurando que la memoria institucional se preserve frente a la volatilidad tecnológica y que los registros electrónicos sigan siendo válidos jurídicamente en el tiempo.

Los informáticos parlamentarios son responsables de la arquitectura técnica que soporta la digitalización, incluyendo la seguridad de la información, la transparencia de los algoritmos, la trazabilidad de los sistemas de IA y el cumplimiento técnico de las exigencias normativas de protección de datos y supervisión algorítmica.

Sin un espacio estable de coordinación y colaboración entre estos tres cuerpos técnicos, los riesgos de fragmentación institucional, incumplimiento normativo, pérdida de control sobre las herramientas tecnológicas o vulneración de derechos fundamentales se multiplican. Por el contrario, una colaboración sostenida, basada en el respeto mutuo de funciones, en la formación cruzada y en el establecimiento de protocolos conjuntos, permite construir un ecosistema parlamentario digital jurídicamente robusto, éticamente responsable y tecnológicamente eficiente.

Este trabajo concluye, por tanto, subrayando que el futuro de los parlamentos digitales no dependerá exclusivamente de la tecnología que adopten, sino de la calidad institucional de la gobernanza que desarrollen. Y en el centro de esa gobernanza deben situarse los profesionales que, desde el derecho, la archivística y la ingeniería, sostienen día a día la legitimidad y el buen funcionamiento del poder legislativo.

VI. BIBLIOGRAFÍA

Burrell, J. (2016). How the machine 'thinks': Understanding opacity in machine learning algorithms. *Big Data & Society, 3*(1), 1–12. https://doi.org/10.1177/2053951715622512

Bygrave, L. A. (2014). *Data Protection Law: Approaching Its Rationale, Logic and Limits* (2nd ed.). Oxford University Press.

Calo, R. (2017). Artificial Intelligence Policy: A Roadmap. *University of California, Davis Law Review, 51*(2), 399–418.

Cano Bazaga, E. (2021). *Gobierno abierto y transformación digital*. Aranzadi.

Comisión Europea. (2021). *Proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on Artificial Intelligence (Artificial Intelligence Act)*. COM(2021) 206 final. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52021PC0206

De la Quadra-Salcedo Janini, T. (2017). *La transparencia como valor constitucional*. Centro de Estudios Políticos y Constitucionales.

De Miguel Asensio, P. (2020). *Protección de datos y derecho digital*. Thomson Reuters-Aranzadi.

Eubanks, V. (2018). *Automating Inequality: How High-Tech Tools Profile, Police, and Punish the Poor*. St. Martin's Press.

Floridi, L., Cowls, J., Beltrametti, M., Chatila, R., Chazerand, P., Dignum, V., … & Vayena, E. (2018). AI4People—An Ethical Framework for a Good AI Society. *Minds and Machines, 28*(4), 689–707. https://doi.org/10.1007/s11023-018-9482-5

Goodman, B., & Flaxman, S. (2017). European Union regulations on algorithmic decision-making and a «right to explanation». *AI Magazine, 38*(3), 50–57. https://doi.org/10.1609/aimag.v38i3.2741

Organización de los Estados Americanos (OEA). (2000). *Declaración de Principios sobre la Libertad de Expresión*. https://www.oas.org

Rodotà, S. (2004). *La vida y las reglas: entre el derecho y lo no justo*. Trotta.

Sáez Vacas, F. (2018). *Sociedad digital: el cambio histórico actual*. Editorial Complutense.

Unión Interparlamentaria (UIP). (2018). *Directrices sobre la democracia electrónica parlamentaria*. https://www.ipu.org/es/documentos/publicaciones/manual/2018-10/directrices-sobre-democracia-electronica-parlamentaria.