Legislating in the Age of AI: Key Challenges in Implementing Large Language Models within Legislative Assemblies

Erik Longo

Abstract

This study explores the application of Large Language Models within legislative assemblies, assessing both its potential benefits and inherent risks. These AI systems are increasingly used to enhance legislative research, streamline administrative functions, and improve public engagement, marking a significant evolution in the digitalisation of representative institutions. However, adopting AI in legislative assemblies raises critical legal, ethical, and institutional challenges. The study examines risks related to data protection, cybersecurity vulnerabilities, and algorithmic bias, emphasising the need for transparency, accountability, and democratic oversight. It also highlights the regulatory gaps surrounding AI use in legislative settings, assessing current legal frameworks such as the EU AI Act and recent international policy developments. In response to these challenges, the study advocates developing comprehensive governance frameworks to ensure AI's responsible implementation in legislative assemblies. It underscores the necessity of clear guidelines, robust regulatory instruments, and cross-institutional cooperation to safeguard democratic principles. The research concludes that a balanced approach is essential to preserving the legitimacy and resilience of democratic institutions in the digital era.

Dieser Beitrag untersucht die Anwendung von Large Language Model in gesetzgebenden Versammlungen und bewertet sowohl die potenziellen Vorteile als auch die damit verbundenen Risiken. KI-gesteuerte Werkzeuge werden vermehrt dazu eingesetzt, die parlamentarische Recherchearbeit zu verbessern, Verwaltungsfunktionen zu rationalisieren und die öffentliche Teilnahme zu verbessern; sie stellen eine bedeutende Entwicklung hin zur Digitalisierung von repräsentativen Institutionen dar. Der Einsatz von KI in gesetzgebenden Versammlungen bringt jedoch kritische rechtliche, ethische und institutionelle Herausforderungen mit sich. Die Studie untersucht die Risiken in Bezug auf Datenschutz, Cybersicherheitsschwachstellen und algorithmische Verzerrung und unterstreicht die Notwendigkeit von Transparenz, Rechenschaftspflicht und demokratischer Aufsicht. Sie zeigt auch die Regulierungslücken im Zusammenhang mit der Nutzung von KI in rechtlichen Rahmenbedingungen auf und bewertet die aktuellen rechtlichen Rahmenbedingungen wie das KI-Gesetz der EU und die jüngsten internationalen politischen Entwicklungen. Als Antwort auf diese Herausforderungen befürwortet die Studie die Entwicklung eines umfassenden Governance-Rahmens, um eine KI im legislativen Umfeld verantwortungsvoll umzusetzen. Sie unterstreicht die Notwendigkeit klarer Richtlinien, robuster Regulierungsinstrumente und institutionenübergreifender Zusammenarbeit zur Wahrung demokratischer Grundsätze. Die Studie kommt zum Schluss, dass ein ausgewogener Ansatz unerlässlich ist, um die Legitimität und Widerstandsfähigkeit der demokratischen Institutionen im digitalen Zeitalter aufrechtzuerhalten.

I. Introduction

The integration of advanced software and computational techniques that can automate various aspects of the work done by members of elected assemblies and parliamentary bureaucracies – especially within the legislative process – has become an undeniable reality, drawing significant scholarly attention.[1]

As early as the late 1990s and the beginning of the twenty-first century, information and communication technologies (ICT) were already being utilised in elected assemblies to facilitate the flow of information within institutional structures,[2] strengthen representative-represented relations, and improve the formulation of public policies.[3]

---

1 See *Costa/Fitsilis*, Parliamentary Administration Facing the Digital Challenge, in: Christiansen/Griglio/Lupo (Hg), The Routledge Handbook of Parliamentary Administrations (2023), 105.

2 *Francesconi*, The Winter, the Summer and the Summer Dream of Artificial Intelligence in Law, Artificial Intelligence and law 30 (2022), 147.

3 On the use of ICT to achieve a better relationship between citizens and representatives, see *Leston-Bandeira*, The impact of the internet on parliaments: A legislative studies framework, Parliamentary Affairs 60 (2007), 655; *Williamson*, The effect of digital media on MPs' communication with constituents, Parliamentary Affairs 62 (2009), 514; *Griffith/Leston-Bandeira*, How Are Parliaments Using New Media to Engage with Citizens?, The Journal of Legislative Studies 18 (2012), 496; *Romanelli*, Designing e-Sustainable Parliaments, in: Torre/Braccini/Spinelli (Hg), Empowering organizations (2016), 29; *Wahl*, The Rise of Data and ai in Parliamentary Proceedings – The Norwegian Parliament, Stortinget, International Journal of Parliamentary Studies 4 (2024), 79; *Longo/Lorenzini*, Ict e parlamenti: oltre la mera diffusione dei contenuti, in: Conti/Milazzo (Hg), La crisi del Parlamento nelle regole della sua percezione (2017), 155. In general on the use of technology to make policies more transparent see *Harrison/Sayogo*, Transparency, participation, and accountability practices in open government: A comparative study, Government information quarterly 31 (2014), 513; *De Vries/Bekkers/Tummers*, Innovation in the public sector: A systematic review and future research agenda, Public Administration 94 (2016), 146; *Campos-Domínguez/Ramos-Vielba*, Parliaments and Key Transformations in Digital Communication, in: García-Orosa (Hg. Digital Political Communication Strategies Multidisciplinary Reflections (2022), 25. On the general transformation that parliaments are undergoing, in addition to the numerous bibliography that will be quoted from here on, see *Giddings*, The Future of Parliament: Issues for a New Century (2005); *Dai/Norton*, The Internet and Parliamentary Democracy in Europe, The Journal of Legislative Studies 13 (2007), 342; *Fallon/Allen/Williamson*, Parliament 2020: Visioning the Future Parliament: International Comparison: Australia, Canada, Chile and the United Kingdom, London (2010); *Fitsilis/Mikros*, Crowdsourcing the digital parliament, The Journal of Legislative Studies (2024), 1.

In recent years, the rapid advancement of artificial intelligence (AI) – driven by the proliferation of a data-driven economy and an increasing reliance on evidence-based decision-making – has enabled the development of sophisticated *e-government* mechanisms.[4] These innovations now allow for the partial automation of public decision-making processes, including certain aspects of assemblies' decision-making.

The COVID-19 pandemic further accelerated the adoption of digital solutions in legislative institutions, primarily due to the necessity of ensuring the continuity of parliamentary functions during periods when in-person activities were not possible.[5]

Currently, AI serves as a pivotal driver of change within policy-making institutions.[6] Worldwide, the emergence of "GovTech" marks a significant shift in governance, placing technological innovations at the heart of legislative and administrative processes.[7] This transformation has also facilitated

4 On this topic, see *De Lungo*, Le prospettive dell'AI generativa nell'esercizio delle funzioni parlamentari di controllo e indirizzo. Un primo inquadramento costituzionale, fra asimmetria informativa e forma di governo, Federalismi.it (2024), 68; *Alexopoulos et alii*, How Machine Learning is Changing e-Government, Proceedings of the 12th International Conference on Theory and Practice of Electronic Governance (2019), https://dx.doi.org/10.1145/3326365.3326412; *Maragno et alii,* The spread of Artificial Intelligence in the public sector: a worldwide overview, 14th International Conference on Theory and Practice of Electronic Governance (2021), https://dx.doi.org/10.1145/3494193.3494194; *Fitsilis*, Artificial Intelligence (AI) in parliaments – preliminary analysis of the Eduskunta experiment, The Journal of Legislative Studies 27 (2021), 621.

5 *Verrigno*, Il Parlamento italiano nel tempo della tecnica: quale rapporto tra regolamenti parlamentari e nuove tecnologie digitali?, Osservatorio sulle fonti (2023), 365.

6 *Cardone*, "Decisione algoritmica" *vs* decisione politica? A.I. Legge Democrazia (2021); *Novelli et alii*, Artificial Intelligence for the Internal Democracy of Political Parties, Minds and Machines 34 (2024), 1.

7 *GovTech* refers to technologically sophisticated solutions resulting from the involvement of public sector organisations with start-ups and small companies. Different approaches related to government modernisation and efficiency have been mapped in the literature: solutions developed by start-ups to transform public services, government technology transformation processes and government strategy to incorporate technology tools. *de Magalhães Santos*, Dynamic Capabilities in the Public Sector to Deal with GovTech, in: Janssen et alii (Hg), Electronic Government: 23rd IFIP WG 8.5 International Conference, EGOV 2024, Ghent-Leuven, Belgium, September 3–5, 2024, Proceedings (2024), 470; *Eom/Lee,* Digital government transformation in turbulent times: Responses, challenges, and future direction, Government Information Quarterly 2 (2022) 101690; *Mergel et alii*, Scoping GovTech dynamics in the EU, Luxembourg (2022).

the establishment of standardised frameworks for the digital drafting of legal documents.[8]

The introduction of the Resource Description Framework (RDF) – a standard model for data exchange on the web, issued as a set of recommendations by the World Wide Web Consortium[9] (W3C) – was soon followed by the OASIS standard *Akoma Ntoso*[10] (AKN), specifically designed for use in parliamentary contexts.

Within the European Union, AKN has received significant institutional backing, particularly through its application to the markup of EU legislation.[11] Furthermore, the creation of the European Interoperability Framework (EIF) and its funding via the ISA (Interoperability Solutions for Public Administrations)[12] programme have further strengthened the adoption of legal document standardisation in legislative assemblies.

Implementing AI in these processes requires technical advancements and a reconfiguration of organisational structures and legal frameworks.[13] Legislative institutions must establish new rules, guidelines, and procedural mechanisms to leverage these technologies' transformative potential fully. Cutting-edge AI tools present a range of possibilities, including en-

8 *Sartor et alii*, Legislative XML for the semantic web: principles, models, standards for document management (2011).

9 See W3C "RDF", available at https://www.w3.org/RDF/ (25.02.2025).

10 The AKN is routinely used by the European Parliament, the Senate of Italy, the Senate of Brazil, the Parliament of Uruguay, the Chamber of Deputies of Argentina, the Chamber of Deputies of Chile, the institutions of the United Kingdom and the House of Representatives of the United States. *Palmirani/Vitali*, Akoma-Ntoso for legal documents, in: Sartor et alii (Hg), Legislative XML for the Semantic Web: Principles, Models, Standards for Document Management (2011), 75; *Palmirani*, Lexdatafication: Italian legal knowledge modelling in Akoma Ntoso, in: Rodríguez-Doncel et alii (Hg), AI Approaches to the Complexity of Legal Systems XI-XII: AICOL International Workshops 2018 and 2020: AICOL-XI@ JURIX 2018, AICOL-XII@ JURIX 2020, XAILA@ JURIX 2020, Revised Selected Papers XII (2021), 31. Il sito di Akoma Ntoso è al seguente URL: http://akomantoso.info/ (25.02.2025).

11 AKN4EU (Akoma Ntoso for European Union) AKN4EUA *Common Structured Format for EU Legislative Documents*, https://op.europa.eu/en/web/eu-vocabularies/akn4eu (25.02.2025).

12 *Campmas/Iacob/Simonelli*, How can interoperability stimulate the use of digital public services? An analysis of national interoperability frameworks and e-Government in the European Union, Data & Policy 4 (2022), 1.

13 *Fitsilis et alii* (Hg), Guidelines for AI in Parliaments, Westminster Foundation for Democracy (2024).

hanced legislative research and analysis,[14] improved support for legislative functions, automation of administrative tasks, increased transparency, and greater public engagement.

The use of digital technologies in the activities of legislative assemblies falls within the emerging field of the *constitutional law of technology*.[15] This burgeoning area of legal scholarship highlights the growing importance of "calculability" within the law and indicates a potential paradigm shift in our understanding of constitutionalism.[16]

Against this background, the article will examine the critical issues of data protection and security concerning generative AI (GenAI) use in parliaments. We will analyse and comment on two key documents recently produced by expert organisations that have long studied the impact of technological advancements on parliamentary institutions.[17]

II. Leveraging Large Language Models in legislative assemblies: Key Considerations

Over the past decade, remarkable advancements in artificial intelligence (AI) techniques – particularly in machine learning, deep learning, and neural networks – have significantly improved our capacity to process vast volumes of data with unprecedented speed and efficiency. This technological revolution has enabled new private and public power forms, reshaping decision-making processes across various domains. The advent of genera-

14 Artificial intelligence systems can assist parliamentary staff in conducting comprehensive legislative research and analysis. Machine learning algorithms can analyse vast volumes of legislative documents, identifying patterns, trends and relevant ideas. Furthermore, AI-driven data analysis platforms can facilitate evidence-based policymaking, synthesising disparate sources of information and highlighting key findings for decision-makers. See *Inter-Parliamentary Union*, Guidelines for AI in parliaments, (2024).

15 *Simoncini*, Il linguaggio dell'Intelligenza Artificiale e la tutela costituzionale dei diritti, Rivista AIC 14 (2023), 1.

16 See *Simoncini/Longo*, Fundamental Rights and the Rule of Law in the Algorithmic Society, in: Micklitz et alii (Hg), Constitutional Challenges in the Algorithmic Society (2021), 27; *Longo/Pin*, Oltre il costituzionalismo? Nuovi principi e regole costituzionali per l'era digitale, DPCE (2023), 103; *Santosuosso/Sartor*, Decidere con l'IA. Intelligenze artificiali e naturali nel diritto (2024); *De Gregorio*, Digital Constitutionalism in Europe: Reframing Rights and Powers in the Algorithmic Society (2022).

17 See *Inter-Parliamentary Union,* Guidelines for AI in parliaments, and *Fitsilis et alii* (Hg), Guidelines for AI in Parliaments.

tive artificial intelligence (hereafter GenAI) marks a further extraordinary leap forward, fundamentally transforming how information is collected, managed, and utilised.[18]

The application of Large Language Models (LLMs), a subset of GenAI systems, to legislature procedures is one of the most compelling developments in the ongoing digital transformation of representative institutions. However, a comprehensive analysis of this shift – encompassing both procedural aspects, such as drafting legislative texts and behavioural dynamics within and beyond legislative assemblies – reveals that modernising representative institutions is not merely a technocratic exercise.[19] Instead, it involves complex socio-political variables that must be carefully considered. Enhancing institutional efficiency must not overshadow the fundamental democratic principle of ensuring the broadest possible engagement of citizens in the political process. The very nature of an assembly system demands that technological innovations uphold and reinforce, rather than undermine, the participatory foundations of democracy.

Moreover, the inherent limitations of machine-based decision-making must be acknowledged.[20] Just as computational sciences have yet to fully explain the reasoning processes of AI systems operating through deep neural networks, so do the natural sciences struggle to predict the behaviour of

18 The most important advances in this technology are usually reported in the proceedings of the annual conferences on 'Neural Information Processing Systems' (NIPS) and 'Machine Learning' (ICML). Some of these papers form the basis of the advances made by OpenAI, Google, Meta, AWS: *Vaswani et alii*, Attention Is All You Need (2017); *Brown et alii,* Language models are few-shot learners (2020); *Ramesh et alii*, Zero-shot text-to-image generation (2021); *Arjovsky/Chintala/Bottou*, Wasserstein generative adversarial networks (2017). Una spiegazione molto efficace della GenAI è effettuata da *Feuerriegel et alii,* Generative AI, Business & Information Systems Engineering 66 (2024), 111; *Narayanan/Kapoor*, AI Snake Oil: What Artificial Intelligence Can Do, What it Can't, and How to Tell the Difference (2024). For an interesting evaluation of the first releases of ChatGPT, see *Ray*, ChatGPT: A comprehensive review on background, applications, key challenges, bias, ethics, limitations and future scope, Internet of Things and Cyber-Physical Systems 3 (2023), 121.

19 If we are to benefit from the revolution underway, then rethinking the relationship between humans and machines becomes essential, without forgetting that in the context of parliamentary procedures, the use of AI cannot be confined to a mere "technical variable". The collection and processing of vast amounts of data provide a new value to parliamentary activities and enable political choices and decision-making processes to be backed up by the most accurate predictions possible.

20 *Diurni/Riccio*, ChatGPT: Challenges and Legal Issues in Advanced Conversational AI, Italian LJ 9 (2023), 473.

complex physical systems.[21] This epistemic constraint renders it impossible to entrust such AI-driven models by formulating unequivocal legal choices. Furthermore, human societies are characterised by continuous evolution, unpredictability, and resilience – qualities that artificial systems, however sophisticated, cannot replicate independently. While AI can algorithmically analyse the correlations between the syntactic, semantic, and pragmatic dimensions of natural language,[22] it cannot supplant human agency without presupposing the outright elimination of humankind itself – a dystopian prospect.[23]

The use of digital technologies by legislatures must, therefore, be understood not merely as an instrument for enhancing procedural efficiency but as a catalyst for broader transformations in the fundamental elements that shape the production of law: time, space, and action.

However, AI-driven innovations do not simply accelerate legislative processes; they have the potential to redefine the temporal, spatial, and procedural dimensions of law-making, thereby altering long-standing institutional practices and rituals.[24] This process of technological disruption does not eliminate law *per se* but reshapes the social interactions that constitute legal systems. In particular, it reconfigures the internal dynamics of institutions such as parliaments and courts, redefining their symbolic and procedural structures. As scholars have recently observed, these changes entail a "profound transformation in the constitution of legal meaning, its symbolic redefinition, and its implications for the very formation of legal professionals." [25]

The next phase of digital evolution – encompassed by the anticipated transition to Web 4.0 – promises an even greater integration of autonomous AI systems within human decision-making processes.[26] This technological paradigm, often described as symbiotic, pragmatic, and ubiquitous, envisions software agents that not only communicate with one another au-

21 *Santosuosso/Sartor*, Decidere con l'IA. Intelligenze artificiali e naturali nel diritto.
22 *Cicconi*, Linguaggio giuridico e Intelligenza Artificiale, in: Alpa (Hg), Diritto e intelligenza artificiale (2020), 59.
23 *Revelli*, Umano Inumano Postumano. Le sfide del presente (2020).
24 *Garapon*, La despazializzazione della giustizia (2021), con riguardo alla giustizia.
25 *Garapon/Lassègue*, La giustizia digitale. Determinismo tecnologico e libertà (2021). Our translation.
26 *Casanovas/de Koker/Hashmi*, Law, Socio-Legal Governance, the Internet of Things, and Industry 4.0: A Middle-Out/Inside-Out Approach, J 5 (2022), 64.

tonomously (*machine-to-machine*) but also collaborate with human actors in increasingly sophisticated ways (*human-to-machine*).[27]

While LLMs are poised to facilitate progress along these lines, critical questions remain: What are the potential costs of such integration? What risks does it entail for democratic governance, legal interpretation, and the rule of law? These pressing concerns demand rigorous reflection as parliaments and legal scholars navigate the challenges and opportunities of the accelerating AI revolution.

III. LLMs in Parliaments: Implications and Challenges

It is essential to examine the broader implications of employing LLMs within representative institutions before addressing the risks associated with integrating these tools into parliamentary activities.

AI is not a singular technology but an expansive domain encompassing a range of systems, methods, models, and approaches aimed at replicating and approximating human cognitive processes to solve complex problems.[28]

AI has rapidly developed and transformed in recent years, with profound implications for both the private and public sectors.[29] However, among the various domains impacted by this technological revolution, representative institutions have been among the slowest to embrace AI-driven transformations despite their central role in governance.[30]

Although parliaments are increasingly positioned within the broader digital evolution that has fostered integrated ecosystems of applications and

27 *Francesconi*, Artificial Intelligence and law 30 (2022), 156.

28 Today, a very clear definition can be found both in OECD documents and in Article 3 of Regulation (EU) No 2024/1689, known as the AI Act.

29 *Wirtz/Weyerer/Geyer*, Artificial Intelligence and the Public Sector—Applications and Challenges, International Journal of Public Administration 42 (2019), 596; *Madan/Ashok*, AI adoption and diffusion in public administration: A systematic literature review and future research agenda, Government Information Quarterly 40 (2023), 101774.

30 *Fitsilis/de Almeida*, Artificial intelligence and its regulation in representative institutions, in: Charalabidis/Medaglia/Van Noordt (Hg), Research Handbook on Public Management and Artificial Intelligence (2024), 151.

services based on open and interconnected legal information,[31] the awareness of AI's transformative potential within this domain remains relatively underdeveloped.[32]

Several factors contribute to this lag. On the one hand, there appears to be limited interest from technology companies in investing in AI-driven parliamentary technology — a sub-sector of *ParlTech* —[33] due to the relatively small number of potential clients worldwide, which results in an insufficiently attractive return on investment (ROI) for major firms.[34] On the other hand, the application of AI in legislature settings presents a unique set of challenges. Unlike other public and private sector domains, parliamentary institutions operate within a particular and tradition-bound environment, requiring significant adaptations in strategy, leadership, workforce skills, digital culture, and user engagement.

A key difficulty arises from the inherent complexity of these activities, which cannot be fully reduced to mere statistical or digital data points. AI applications often attempt to homogenise disparate phenomena, particularly the intricate relationship between legal texts and their extra-legal context.

However, given the multifaceted and evolving nature of lawmaking and deliberation, the capacity to mathematically or statistically capture the full complexity of legislative processes remains limited. Furthermore, as public institutions steeped in historical and procedural traditions, parliaments inherently resist rapid technological overhauls.[35] The erroneous or inappro-

---

31 Innovation Tracker of the Inter-Parliamentary Union: https://www.ipu.org/knowledge/ipu-innovation-tracker (25.02.2025). IPU, World e-Parliament Report 2020, Paris (2021).

32 *Fitsilis*, The Journal of Legislative Studies 27 (2021); *Fitsilis/Koryzis/Schefbeck, Legal Informatics Tools for Evidence-Based Policy Creation in Parliaments*, cit, 8 ff.

33 *Malaschini/Pandolfelli*, PARLTECH. Intelligenza Artificiale e Parlamenti: Una prima riflessione (2022).

34 *Williamson/Fallon*, Transforming the Future Parliament Through the Effective Use of Digital Media, Parliamentary Affairs 64 (2011), 781.

35 As recalled by *Fitsilis et alii*, Implementing Digital Parliament Innovative Concepts for Citizens and Policy Makers, in: Nah/Tan (Hg), HCI in Business, Government and Organizations. Interacting with Information Systems: 4th International Conference, HCIBGO 2017, Held as Part of HCI International 2017, Vancouver, BC, Canada, July 9-14, 2017, Proceedings, Part I (2017), 154, parliaments, as institutional structures of democracy, are traditional organisations in the sense that they rely heavily on tradition. As a direct consequence, parliaments have considerable "friction" to change. Their institutional identity, organisational structure and rules of procedure often remain stable for long periods of time. The recognition that new means of bottom-up

priate implementation of AI-based solutions in legislative processes could hinder their effectiveness, resulting in democratic deficits, reputational harm, and a loss of public trust.

For instance, if a legislative assembly were to mismanage AI-driven tools for citizen engagement, it could inadvertently generate misleading communications or create avenues for misinformation, thereby undermining public confidence in democratic processes. Consequently, before fully embracing AI, assemblies' administrations must ensure that certain foundational prerequisites are met. A transition from a predominantly paper-based institution to an AI-supported working environment cannot be achieved through mere technological implementation; rather, it necessitates a broader commitment to organisational and procedural innovation, coupled with the political will to drive these changes.[36]

Despite the abovementioned challenges, AI has already been deployed in various parliamentary functions.[37] Documented use cases range from AI-driven tools designed to assist legislators in research and representative duties to sophisticated platforms to facilitate citizen engagement in political debates and legislative processes.

In recent years, we have witnessed a proliferation of digital solutions designed to enhance transparency, accountability, and citizen interaction with parliaments. AI-driven services have also improved public access to legis-

---

or top-down political communication are crucial for parliamentary life and that political parties can no longer be the most effective channels for this communication has convinced political leaders, parliamentarians and parliamentary administrations of the need to find alternative means of interaction through digital technologies.

36 Interesting in this respect is the case of the initiative launched by the Chamber of Deputies between 2023 and 2024. See the Rapporto del Comitato di vigilanza sull'attività di documentazione della Camera dei deputati, Utilizzare l'intelligenza artificiale a supporto del lavoro parlamentare, Roma (2024).

37 A survey conducted in late 2022 - before the introduction of free basic services via OpenAI's ChatGPT - revealed the existence of 39 active Al solutions in 10 parliamentary chambers. The arrival of ChatGPT triggered a wave of interest in generative Al solutions with direct or indirect implications for legislation. Notably, in 2023, the US Congress purchased 40 ChatGPT Plus licences to explore generative Al within its ranks. These licences were distributed among Congressional offices, allowing legislators and staff to experiment with this transformative technology internally. In April 2024, the Committee on House Administration (CHA) of the US House of Representatives issued a set of general guidelines to be used for any Al tool or technology in use within the House. See *Fitsilis et alii*, Guidelines for AI in Parliaments; *Ziouvelou/Giannakopoulos/Giannakopoulos*, Artificial Intelligence in the Parliamentary Context, in: Mikros/Fitsilis (Hg), Smart Parliaments (2022), 43.

lative information, enabling more refined citizen feedback and preferences analysis.[38] Notably, however, among the cases examined in academic literature, there appear to be no AI systems explicitly dedicated to monitoring or directing governmental action – a gap that warrants further exploration.[39]

According to the *2018 World E-Parliament Report*, two of the most anticipated improvements in parliamentary technology are expanding open data publication capabilities and enhancing mechanisms for disseminating legislative information to the public.[40] These advancements are closely linked to the broader trend of *open-linked parliamentary data*, which enables seamless access to legislative documents and proceedings. In this context, adopting open standards—such as XML—has become a mature technological solution for parliaments. However, the practical design and implementation of parliamentary ICT systems based on open standards must also adhere to well-established criteria, including usability, adaptability, and certified software development.[41]

Integrating AI in parliamentary settings thus presents unprecedented opportunities and significant challenges. A key issue concerns the regulatory vacuum surrounding the phenomenon. There are no specific legal frameworks governing the use of AI in parliaments, creating uncertainties regarding oversight, accountability, and compliance. More critically, deploying AI in legislatures raises pressing concerns about data protection, system security, and institutional integrity. The potential exposure of parliamentary

38 The processes and tasks associated with legislative procedures were prioritised, especially with regard to the drafting and deliberation of laws, plenary sessions and committee meetings. Particular emphasis was placed on the digital transformation of the legislative process, which has become increasingly complex over the years. Many of these include the development of digital platforms that have similar design features and have in common that they are powered by AI. Due to the increase in digital inclusion and the strengthening of public sector accountability mechanisms, the general level of access to information has increased significantly. As a result, the mission of representing citizens has become more complex. Among other things, analyses of large data sets in shorter timeframes are necessary to keep up with society. AI-related tools and services have the potential to provide satisfactory answers to these challenges. *Wahl*, International Journal of Parliamentary Studies 4 (2024); *Fitsilis*, The Journal of Legislative Studies 27 (2021).

39 *Fitsilis/de Almeida*, Artificial 123; *De Lungo*, Federalismi.it (2024).

40 *Inter-Parliamentary Union,* World e-Parliament Report (2018).

41 To achieve legal and systemic interoperability when writing or editing bills, technical standards and open systems architectures must be used. *Koryzis et alii*, ParlTech: Transformation Framework for the Digital Parliament, Big Data and Cognitive Computing 5 (2021), 1.

AI systems to cybersecurity threats and data vulnerabilities necessitates the development of robust protective measures to safeguard parliamentary processes and sensitive information.

Given the novelty and complexity of AI integration, significant attention must be devoted to the training and capacity-building of parliamentary actors at the political level. A lack of adequate knowledge and preparedness could hinder the effective implementation of AI-driven procedures and expose parliamentary institutions to external manipulations or security threats.[42] Consequently, AI adoption within parliaments must be accompanied by the introduction of procedural safeguards, organisational frameworks, and regulatory standards designed to address concerns related to data privacy, IT security, and information access and ownership.

Several key considerations emerge in this regard. First, parliaments must carefully evaluate AI system hosting options, weighing the trade-offs between on-premises installations and cloud-based services, each presenting distinct risks and benefits. Additionally, the portability of AI-driven services and data must be ensured, while procurement policies should prioritise AI solutions from trusted suppliers with transparent ownership structures.

Furthermore, the non-partisanship and quality of AI training data must be safeguarded. AI algorithms used in parliamentary contexts must adhere to fundamental principles of transparency, explainability, and accountability, as these elements are essential for fostering public trust in AI-driven legislative tools. Moreover, AI systems should be designed to operate in multiple languages to accommodate the diverse linguistic needs of parliamentary institutions and their constituents. These principles should not only inform the technical development of AI algorithms and applications. Still, they must also be incorporated into the training of developers to ensure ethical and responsible AI deployment in legislative environments.

Concerning AI users – particularly legal professionals and parliamentary staff – upholding their autonomy in utilising AI tools is crucial. AI should serve as an assistive mechanism rather than a substitute for human expertise. Likewise, mechanisms for public participation must be preserved and strengthened to ensure that democratic values remain integral to parliamentary AI applications. Integrating AI into parliamentary workflows

42 Developing new skills and professionalism, as well as the ability to manage change, is a major challenge. Developing AI and data literacy among parliamentarians and staff is crucial for the effective use and supervision of these systems.

thus requires establishing standardised procedures and evaluative metrics to ensure the responsible and effective use of these technologies.[43]

These considerations also underscore the need for inter-institutional and inter-parliamentary cooperation in developing AI governance frameworks. Few parliamentary institutions possess the technical expertise or resources to address the multifaceted challenges posed by AI independently, so collaborative efforts at both national and international levels are essential. A balanced approach is required to maximise AI's transformative potential while safeguarding the institutional integrity, security, and democratic foundations of parliamentary systems.[44]

Implementing AI should be underpinned by broad-based, cross-party consensus to ensure continuity and legitimacy. Moreover, while AI offers significant efficiency gains in parliamentary processes, these technologies must not supplant the essential human elements of decision-making and democratic representation.[45] Human oversight remains crucial to maintaining institutional accountability, even for routine administrative tasks.[46]

A particularly salient area of AI's potential impact is citizen engagement.[47] AI-powered tools can facilitate more sophisticated analyses of public sentiment regarding legislative proposals, enabling real-time feedback mechanisms.[48] However, such advancements must complement – not replace – direct interactions between legislators and constituents. Preserving

43 For instance, rules and standards on data archiving and deletion, ethical supervision and continuous monitoring are needed to ensure that the Al systems in parliaments meet the highest standards.

44 To this end, a specific AI strategy should be developed for each individual representative institution - based on the national AI strategy - and accompanied by a set of operational rules that serve the purpose of ensuring that the adoption of AI does not interrupt the essential human elements of political discourse and decision-making. See *Inter-Parliamentary Union,* Guidelines for AI in parliaments and *Fitsilis et alii,* Guidelines for AI in Parliaments.

45 This is due not only to technical limitations but also to the fact that the subtle and often politically sensitive work of parliaments and parliamentary bureaucracies requires a level of judgement and ethical consideration that current AI systems cannot (yet) replicate.

46 *Inter-Parliamentary Union*, Guidelines for AI in parliaments, 18.

47 *De Lungo*, Federalismi.it (2024), 82 ff.

48 With the evolution of 'Natural Language Processing' (NLP) systems through Large Language Models (LLM), the most widely used functionalities are speech-to-text transformation, text classification and pattern recognition, which in turn includes voice, images, objects and facial recognition. *Surden*, ChatGPT, Artificial Intelligence (AI) Large Language Models, and Law, Fordham Law Review 92 (2024), 1942.

the human element of democratic representation remains paramount in an era of increasing automation.

The large-scale commercial deployment of LLMs has transformed AI applications in both the private and public sectors. These technologies provide significant capabilities in generating and analysing legislative texts, fact-checking, and enhancing public engagement.[49] Additionally, AI has been utilised in parliamentary administration for process automation, intelligent document retrieval, and policy research. However, AI systems – especially LLMs – must be trained on high-quality datasets to minimise the risk of bias or inaccuracy and operate effectively. Furthermore, given their management of sensitive legislative information, these systems must be reinforced against cybersecurity threats and vulnerabilities.

The following discussion will examine GenAI's general risks and drawbacks. It will then follow with an in-depth analysis of the specific data protection and cybersecurity risks linked to its implementation in parliamentary contexts.

A. General Risks of LLMs Use in Parliaments

The extensive capabilities of LLMs introduce a complex array of risks, many of which compound existing challenges associated with digital governance. In response to these concerns, certain institutions have already instituted regulatory frameworks—most notably, the EU AI Act.[50] At the same time, academic researchers have proposed a variety of security metrics and comprehensive taxonomies to classify AI-related risks.

49 These systems have two major objectives. First, parliaments seem to prioritise AI systems to streamline processes associated with legislative procedures, including deliberations, plenary sessions and committee meetings. Second, the emphasis is on digital services for citizens, including access to information by citizens and analysis of feedback received from citizens through public consultation tools. The emerging trend is to use a multiplicity of techniques to mitigate the risks posed by a single method and to use symbolic, sub-symbolic and neuro-symbolic AI in a hybrid approach. See *Fitsilis/de Almeida*, Artificial intelligence and its regulation in representative institutions.

50 The first comprehensive piece of legislation that considers AI risks as a main element for AI regulation is the EU Regulation 'laying down harmonised rules on artificial intelligence', the so-called AI Act (Regulation (EU) No 2024/1689). See also the Executive Order issued by the President of the United States of America: *Biden*, Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence (2023) repealed by President Trump in 2025.

Scholarly literature has identified a vast range of risks associated in general with LLMs, including "unethical use," "discrimination," "infringement of intellectual property rights," "information leakage," "malicious use," "security threats," "model illusion and pretence (the 'hallucination'[51])," "environmental, social, and regulatory risks," and "non-controllability of legal decisions".[52]

One of LLMs' most significant limitations is its tendency to generate fabricated or misleading outputs, commonly called *hallucinations*.[53] These inaccuracies arise from the model's inherent probabilistic nature and the potential for incorrect correlations between data points. Furthermore, the opacity of AI model architectures often exacerbates these risks, making it difficult to validate the accuracy and reliability of AI-generated legal content. The lack of clear transparency mechanisms in AI programming further complicates accountability, particularly when AI-generated recommendations influence legislative processes.

Intellectual property infringement remains another unresolved issue in the deployment of LLMs. Given the complex legal landscape governing copyright, it is currently impossible to determine with certainty whether AI-generated outputs violate existing intellectual property laws. Jurisdictional variations in copyright regulation exacerbate this ambiguity. However, parliamentary institutions must remain particularly vigilant in ensuring that AI-generated content does not inadvertently constitute plagiarism or unauthorized reproduction of protected works.

---

51 Hallucinations are a particular error whereby the generated output (eg a text) appears coherent on the surface but may be incorrect or completely made up. The term 'hallucination' refers to the generation of false, nonsensical or inaccurate information by large language models (LLM) or other generative artificial intelligence systems. For more information, see *Maleki/Padmanabhan/Dutta*, AI Hallucinations: A Misnomer Worth Clarifying, arXiv preprint arXiv:2401.06796 (2024).

52 Despite ongoing efforts, no unified categorisation of AI risks comprehensively covers all possible risks, taking into account the industry and government perspective. *Zeng et alii*, AI Risk Categorization Decoded (AIR 2024): From Government Regulations to Corporate Policies, arXiv preprint arXiv:2406.17864 (2024).

53 A typical example of ChatGPT's 'illusions and fictions' occurring in the legal profession occurred in *Mata v Avianca* in 2023 before a New York court. A lawyer submitted a pleading containing excerpts and quotes from fake cases. It turned out that the pleading had been created using ChatGPT. Unaware that ChatGPT can hallucinate, or perhaps trusting an inexperienced colleague, the lawyers did not check that the cited cases really existed. The consequences were disastrous. Once the error was discovered, the court dismissed their client's case and sanctioned the lawyers for acting in bad faith.

Like all machine learning-based technologies, LLMs inherit and may perpetuate existing biases embedded within their training data. If the datasets used to train AI systems contain structural biases – whether cultural, political, or demographic – these biases can become deeply entrenched within the AI's decision-making processes. This phenomenon can result in discriminatory or skewed legislative recommendations, undermining the principles of fairness, equality, and non-discrimination in parliamentary governance.[54]

Moreover, AI developers inevitably introduce subjective decisions into the training process by including or excluding specific data points or prioritising certain linguistic, legal, or cultural frameworks.[55] Such biases are particularly concerning in parliamentary settings, where algorithmic decision-making could inadvertently influence legislative deliberations in ways that are neither transparent nor subject to legal recourse.

To mitigate these risks, algorithmic systems used in parliaments should adhere to *ex-ante transparency* (ensuring openness at the time of implementation) and *ex-post* verifiability (allowing for auditing and oversight after results have been produced). However, achieving these objectives remains a significant challenge, as evidenced by the ongoing debate regarding *explainability* in AI ethics and legal interpretation.[56]

For this reason, algorithm-based systems should ensure transparency, *ex-ante*, at the time of their implementation. They should always be verifiable *ex-post*, when the result emerges. However, this is not always the case, as the 'explainability' debate applied to legal problems shows.

54 As was the case years ago with the COMPAS algorithm developed by Northpointe and used to assess the risk of recidivism, which came to light thanks to the Loomis case decided by the Wisconsin Supreme Court in 2016, which produced strong discrimination against certain sections of the American population. For a summary of the case see *Larson et alii*, How we analyzed the COMPAS recidivism algorithm (2016); *Kehl/Kessler*, Algorithms in the criminal justice system: Assessing the use of risk assessments in sentencing (2017); *Huq*, Racial equity in algorithmic criminal justice, Duke LJ 68 (2018), 1043; *Brennan/Dieterich*, Correctional offender management profiles for alternative sanctions (COMPAS), in: Singh et alii (Hg), Handbook of recidivism risk/needs assessment tools (2018), 49; *Sartor/Lagioia*, Il sistema COMPAS: algoritmi, previsioni, iniquità, in: Ruffolo (Hg), XXVI Lezioni di Diritto dell'Intelligenza Artificiale (2021), 226.

55 *Wachter/Mittelstadt/Russell*, Do large language models have a legal duty to tell the truth?, Royal Society Open Science 11 (2024), 1.

56 *Ződi*, Algorithmic explainability and legal reasoning, The Theory and Practice of Legislation 10 (2022), 67.

A fundamental issue of using LLMs in legal and parliamentary contexts concerns the legitimacy and authority of AI-generated legal reasoning. Legal scholars have long recognised that the complexity of law cannot be computationally reduced to mere statistical patterns.[57] Unlike mathematical models, legal norms are inherently interpretative, context-dependent, and often subject to ambiguity.

In contrast, AI models operate on inferential rather than causative reasoning. They lack empathy, normative judgment, and contextual awareness, rendering them ill-equipped to engage in deliberative reasoning that underpins democratic decision-making. While legal reasoning may share superficial similarities with algorithmic logic – both relying on structured sequences of rules – law is ultimately shaped by human values, ethical considerations, and social realities that cannot be quantified with absolute precision.

This distinction is crucial when considering the role of AI in legislative decision-making. Whereas algorithms rely on rigid, pre-defined logic, legal reasoning must remain adaptable and responsive to evolving social and political contexts. Therefore, applying AI to lawmaking risks imposing a false sense of determinism on inherently interpretative and dynamic processes.

Integrating AI in parliamentary settings necessitates balancing technological innovation and protecting fundamental rights.[58] While AI presents transformative opportunities to enhance efficiency and accessibility in legislative processes, its deployment must not compromise democratic accountability, human oversight, and individual freedoms.

Ensuring this balance requires a) transparency and accountability, b) independent oversight, c) non-discrimination and equality safeguards, and d) data protection and privacy compliance.

Subsequent sections will explore these considerations further. They underscore the urgent need for comprehensive legal and ethical frameworks to regulate the deployment of AI within legislative institutions. AI-driven governance must be designed to enhance procedural efficiency and uphold the core democratic principles of freedom, equality, and the rule of law.

The following section will explore the specific challenges associated with data protection and cybersecurity in implementing LLMs in parliaments.

---

57 *Garapon/Lassègue*, Justice digitale: Révolution Graphique et Rupture Anthropologique (2018).

58 *Bresciani/Palmirani*, Constitutional Opportunities and Risks of AI in the law-making process, Federalismi.it 2 (2024), 1.

B. Risks and Mitigation Strategies for Data Protection and Cybersecurity

As highlighted in various expert analyses,[59] data protection and cybersecurity are fundamental concerns in the regulation of AI within parliamentary institutions. Given the nature of their functions, parliaments routinely process vast amounts of personal data, including information categorised under special protections – historically referred to as *sensitive data*. The failure to implement adequate safeguards when using AI for data analysis, policy research, or decision-making could lead to privacy breaches, unauthorised data access, or misuse, thereby compromising the confidentiality of citizens, parliamentarians, and other stakeholders. Such breaches not only pose individual privacy risks but also threaten public trust in parliamentary processes, potentially undermining the legitimacy of democratic institutions.

Moreover, parliamentary data often includes information of strategic relevance to national security, necessitating heightened vigilance in mitigating risks such as data breaches, identity theft, cyber espionage, and digital misinformation campaigns. The consequences of such threats extend beyond institutional damage to the broader democratic framework, as compromised parliamentary systems could serve as entry points for external interference in legislative processes and public discourse.

Several critical considerations must be addressed during LLMs implementation to ensure robust data protection and cybersecurity.

The first is data localisation. Training and implementing AI systems require substantial computing and storage resources, often necessitating the use of public *cloud* systems. Therefore, it is essential to focus on localising such IT equipment within the EU and ensure that certain types of data remain on their own servers (*on-premises*). The risk of losing effective control over the data used to train these AI systems highlights the need for appropriate risk mitigation strategies, such as encryption or data minimisation.

The second major aspect of interest concerns the quality and accuracy of the data. We have already addressed the issue of training data. Artificial intelligence systems learn from the data provided to them and subsequently apply models to aid in making decisions, generating new content, or performing other tasks.

59 See *Inter-Parliamentary Union,* Guidelines for AI in parliaments; *Fitsilis et alii*, Guidelines for AI in Parliaments.

In the context of legislative and other activities, incorrect data can easily be encountered, whether it has been entered incorrectly, is outdated and thus too old to reflect current events, or has been processed improperly.[60] A system not trained to identify such issues will likely yield inaccurate forecasts. When erroneous data are employed for testing, research, or policy analysis, this can result in ineffective legislation or unintended negative consequences.[61]

Data quality is closely linked to data security. Ensuring data security essentially refers to applying the three parameters of the CIA paradigm (or triad): *confidentiality*, *integrity*, and *availability*. These parameters are the basis for the security of information systems, ie, a proper approach to information security is planned and executed.

Given the increasing interconnectivity of parliamentary IT systems, AI-driven legislative tools are particularly vulnerable to cyber intrusions, digital espionage, and AI model poisoning – where malicious actors introduce corrupt data into AI training models to manipulate outputs. Such attacks could compromise parliamentary deliberations, alter legislative drafting processes, or distort public participation mechanisms.

Furthermore, parliaments implementing AI to handle large-scale public participation may attract groups intent on manipulating democratic processes. Therefore, effective cybersecurity management strategies are crucial for maintaining a secure digital environment that safeguards the integrity of parliamentary operations, particularly as AI adoption increases. Attacks might target the AI models themselves, potentially introducing bias or subtly altering decision-making processes. AI systems employed for analysing and disseminating information could be exploited to propagate disinformation within a state or to negatively affect information retrieval. Therefore, it is essential not only to ensure the integrity of the data but also to protect the adopted AI models,[62] guaranteeing that these models possess reliability features such as human oversight and robustness.[63]

---

60 Consider the case of duplicate, ambiguous or inconsistent data, on which see *Inter-Parliamentary Union*, Guidelines for AI in parliaments, 116 ff.

61 For example, an environmental protection law based on inaccurate pollution statistics could target the wrong industries or fail to address the most pressing problems.

62 *Inter-Parliamentary Union*, Guidelines for AI in parliaments.

63 In the absence of specific standards for AI cybersecurity, several government agencies have published voluntary AI security *frameworks* aimed at helping stakeholders secure their AI systems, operations and processes. For instance, the EU Cybersecurity Agency (ENISA) has published a multilevel security framework for AI cybersecurity

Cyber-attackers can exploit the vulnerabilities of these systems and the data on which they are trained.[64] AI can magnify the types of attacks currently seen,[65] such as adversarial attacks,[66] those resulting in data poisoning,[67] and the well-known DDoS (Distributed Denial of Service)[68] attacks.

Security and data protection issues also affect another aspect of AI usage. In the parliamentary context, ensuring the secure processing of personal identification services is vital. Data sovereignty (the principle that data are subject to the laws of the country in which they are collected or stored) must also be considered.

To mitigate all the risks highlighted above, the literature suggests establishing processes and utilising IT systems and infrastructures generally through 'by-design' implementation. In the case of AI, this essentially in-

---

best practices (FAICP). Similarly, the US National Institute of Standards and Technology (NIST) has published an AI risk management framework to help organisations involved in the design, development, implementation or use of AI systems better mitigate the risks associated with AI and contribute to its reliable and responsible development and use.

64 Sometimes attackers can target the system that receives user input and, other times, the data itself. Attacks can occur at any stage, from data preparation to the development, implementation and operation of the AI system. From this, it can be understood how the entire life cycle of the AI system must be properly supervised to minimise unexpected behaviour.

65 *NIST*, NIST Identifies Types of Cyberattacks That Manipulate Behavior of AI Systems (2024).

66 This type of attack involves an attacker manipulating an AI system's input data to produce inaccurate, unexpected or incorrect responses. This type of attack often targets AI systems capable of image recognition, causing the system to recognise an image incorrectly. One can have the example of an attacker targeting a voting system that uses facial recognition technology, causing it to allow the attacker to vote as an MP mistakenly.

67 In this type of attack (data poisoning), the attacker adds data to the dataset used to train an AI model. The model learns from incorrect information, leading it to make erroneous decisions. For example, a system might misdiagnose a healthy patient as having a deadly cancer, or worse, misdiagnose a patient with cancer as healthy, preventing the person from receiving the right treatment. In a parliamentary context, a proposal could be sent to the wrong committee for discussion, or misinformation could be used to create misinformation.

68 In this type of attack, the attacker can flood a system with excessive requests. The goal is to make the system stop working, preventing any response or, at least, making it so slow that users cannot get a response from the system. When there is an attack of this kind, the victim, often a large company or an administration that provides services, suffers financial losses or damage to its reputation. In a parliamentary context, an attacker could destroy the AI chatbot designed to answer citizens' questions during a plenary session where an issue requiring broad citizen support is being discussed.

volves constructing systems whose data is trained and fine-tuned before usage in the parliamentary context.

IV. The Need for New Rules Governing AI in Parliaments

While AI offers numerous advantages in various aspects of parliamentary life, significant risks and concrete issues remain to be addressed. These include not only the inefficiencies of these tools but also concerns regarding IT security and compliance with data protection regulations.

Only recently has the issue of regulating the use of AI in the activities of elected assemblies been considered in political debate. However, the range of possible approaches, spanning from full integration of such systems to outright rejection of their effectiveness, is still under discussion.

The divergence emphasises that we are in the midst of an evolutionary process requiring the establishment of essential guidelines to direct parliaments in the use of AI responsibly.

A comprehensive investigation into the most effective rules for securing these systems could harness emerging strengths and opportunities. Two potential paths exist: non-binding documents (soft law), such as resolutions, codes of conduct, or guidelines, and legally binding instruments (hard law), such as regulations, directives, and rules. Institutions at the supranational and international levels have now pursued both paths.

Firstly, the European Union's AI Regulation (No 2024/1689), commonly called the AI Act, imposes several obligations on developers and distributors that adopt a risk-based approach. These obligations include conducting a fundamental rights impact assessment (FRIA) for high-risk applications in the public domain. The regulation also classifies certain applications of AI systems in the parliamentary domain as high-risk and specifies obligations related to those applications.

Secondly, the Council of Europe has finalised the 'Framework Convention on AI, Human Rights, Democracy and the Rule of Law'. This Convention represents the first legally binding instrument the Council of Europe issued on these matters. However, it does not impose additional obligations on parliaments regarding using AI technologies.[69]

69 The road to this convention was paved in 2020, when the Parliamentary Assembly of the Council of Europe (PACE) adopted resolutions and recommendations exploring the implications of the Al on human rights, democracy and the rule of law.

Thirdly, the UN General Assembly adopted a resolution in March 2024 to direct the use of AI for the global good. The resolution aims to promote safe, secure, and reliable AI systems, thus accelerating progress towards fully realising the 2030 Agenda for Sustainable Development. This resolution, like the Universal Declaration of Human Rights, is not legally binding, although regional and national normative documents can use it as a compass to achieve the overall goals.

Despite these significant measures, no comprehensive guidelines or binding legal instruments currently systematically regulate the uses and risks of AI implementation within legislative assemblies. However, various AI systems have been used within these institutions for several years, not merely on an experimental basis.

In anticipation of further integration of AI tools and services in the parliamentary workspace, numerous organisations are endeavouring to develop guidelines and regulations. In these pages, we primarily address the safeguards necessary to preserve not only the sovereignty of the infrastructure but also to prevent the intrusion of external actors, safeguarding data ownership to ensure the traceability and legitimacy of parliamentary activities.

However, these considerations necessitate further requirements from a holistic perspective regarding the proper implementation of these technologies in legislative work. Indeed, it must also be ensured that the AIs employed in parliaments align with democratic principles and social needs, remain free from any form of bias and error, are proprietary yet open systems characterised by technological neutrality, and that those implementing such systems do so by fostering awareness among all users, including both politicians and staff of representative institutions.

If the general objective is to prevent machines from replacing human beings, it is necessary not to make humans excessively dependent on machines, even allowing them to exercise a right to rethink the use of machines or even return to using traditional tools.

Finally, because of the typical structure of representative assembly activities and the specific limitations associated with LLMs, the unauthorised and amateurish use of these tools must be discouraged by limiting their use within a framework of strategies and guidelines drawn up by each institution. It is precisely the inappropriate use of these technologies that carries the most significant risks at all levels, from the individual to the public.

Autonomy, freedom, the ability to make informed choices, democracy, respect for the rule of law, and sustainability are some of the values that should guide parliaments' digital transformation, according to the guidelines that have now become the common heritage of European institutions thanks to the work carried out in constructing the "Digital Decade".[70]

V. Concluding remarks

This study seeks to contribute to the expanding body of research on the impact of AI within legislative assemblies. Worldwide, AI is increasingly being deployed in various ways to enhance the efficiency and effectiveness of public administration. Legislatures are following this trend by adopting AI-driven tools to streamline legislative processes while maintaining the deliberative integrity of democratic debate. The goal is to accelerate democratic procedures without compromising the quality of democratic deliberation or undermining fundamental principles of representation and accountability.

In the near future, AI systems are likely to play an even greater role in parliamentary proceedings, assisting legislators in their work while preserving the primacy of human agency. AI-driven applications could include automated legislative analysis to ensure compliance with current legal frameworks, as well as AI-enhanced monitoring of political discourse on digital platforms. However, for these advancements to be realised, AI systems must be designed to support – not replace – human judgment, ensuring that decision-making processes remain transparent, reliable, and democratically accountable.

As AI use expands, so do the associated risks in parliamentary settings. These risks encompass threats to data security, vulnerabilities in cybersecurity, and institutional and reputational challenges. To tackle these concerns, comprehensive safeguards must be established before AI can be reliably integrated into legislative processes. This necessitates the adoption of robust governance frameworks, cybersecurity measures, and preliminary risk assessments.

Ultimately, the deployment of AI in legislative assemblies must align with democratic principles, institutional values, and fundamental rights.

70 One of the highlights of this transformation is the "European Declaration on Digital Rights and Principles for the Digital Decade (2023)".

If implemented responsibly, AI can strengthen legislative efficiency and foster greater citizen engagement. However, without adequate oversight and regulation, AI may pose significant threats to the integrity of democratic institutions. As AI evolves, legislative assemblies must proactively shape its governance, ensuring that these technologies serve democracy rather than undermine it.