

From electronic voting to AI: lessons from the Estonian Case on the transformation of digital democracy

Daniele Battista ¹

<https://orcid.org/0009-0005-8418-8374>

¹ University of Salerno, Salerno, IT, Italy

Abstract: The advancement of artificial intelligence is transforming the technological landscape and generating debates about its numerous effects. The integration of AI into the political sphere raises critical questions: can it enhance institutional transparency and decision-making processes, or does it promote a manipulative use of algorithms, violating ethical and legal norms? This study examines the implications of AI in the political arena, focusing on risks to citizens' privacy related to data use and the legal tools available to protect them in Europe. A case of particular interest is Estonia, a leader in the adoption of digital technologies in public governance. By analysing its experience, this research will explore how AI influences the electoral system and governance, with attention to the ethical, legal, and social consequences. The study will evaluate whether these initiatives are genuinely democratic or pose a threat to citizens' rights. The aim is to provide a critical and comprehensive overview of the complex dynamics related to the implementation of AI in politics, contributing to the understanding of the implications of this disruptive technology and its impact on democratic systems and European regulations.

Keywords: artificial intelligence; digital politics; legal implications; Estonia; electoral participation

1 Introduction

Non-human technologies possessing remarkable intellectual faculties, also known as Artificial Intelligence (AI), have permeated vast areas of the social, political, and economic system (Dwivedi *et al.*, 2021). AI is gradually reshaping the socio-technical system through the widespread adoption of interconnected devices (Makarius *et al.*, 2020). The integration of AI devices can also transform the current political paradigm by enabling access to broader and more extensive forms of communication and participation, beyond mere voting during sporadic

electoral events. On one hand, the importance of citizen participation and collective involvement in democratic processes is emphasized (Archibugi; Cellini, 2017). On the other, little is known about how intelligent systems can strengthen the civic fabric. The evolution of tools used for communicative processes is closely tied to this transformation, a focus that has become increasingly evident in recent decades due to technological dynamics. Artificial intelligence encompasses a variety of methods, algorithms, and technologies that allow software to exhibit cognitive abilities that, when observed from an external perspective, may resemble those of humans (Floridi, 2017).

These technologies are designed to perform complex tasks so that their behaviour can be interpreted as a form of artificial intelligence, even if they are not “intelligent” in the human sense of the term. This framework is significant but provides only a partial view, as it focuses on functionality or performance. Nowadays, it is essential to adopt a more comprehensive approach that considers the many facets of the phenomenon. This trajectory should address broader issues, such as the social, political, ethical, and legal contexts in which AI operates. In this landscape, artificial intelligence is seen not merely as a phenomenon limited to imitating human cognitive abilities but as one that influences various dynamics and makes significant decisions in a variety of contexts. Faced with these developments, it is crucial to provide a theoretical foundation that embraces not only the technical capabilities of AI to mimic human behaviour but also how it interacts with society and laws. This study adopts a theoretical framework that combines surveillance capitalism theory (Zuboff, 2023) with algorithmic governance (Yeung, 2018) to analyse how AI, through data processing, is reconfiguring the relationship between citizens and institutions.

This would lead to an integration between theory and law. It is evident that there are numerous consequences for the “person-voter” in this context, and rules are needed to rebalance the relationship between the right to privacy and the responsible and proper use of collected data and sensitive information, such as political preferences, occasionally in an illegal manner for electoral and

propagandistic purposes. In this regard, the Cambridge Analytica scandal is a fitting example, illustrating the vulnerability of the electorate and its self-determination. The deep learning capabilities of AI systems and the unstoppable progress we are witnessing raise enormous legal questions, starting with ensuring that development occurs within a regulatory framework with adequate levels of protection and security. These areas require a deeper assessment of AI's capacity to influence and shape the political sphere, as well as effective strategies to ensure informed and transparent debate in the AI era (Battista, 2024a).

The case of Estonia is a significant example in this context. The country is known to be at the forefront of the adoption of digital technologies in the political sphere, such as e-government platforms and e-voting. Estonia represents a unique laboratory of digital democracy. From compulsory digital signatures to e-voting (i-Voting), the country has experimented with AI tools in public management more extensively and systemically than other European states (Toots, 2019). This case allows for a concrete analysis of the benefits and limitations of AI in strengthening - or weakening - democratic processes.

2 Technopolitics and the democratic challenge

There is a need for a thorough assessment of the legal effects related to the protection of personal data and the potential for political manipulation. Therefore, Estonia can serve as a laboratory for analysing the risks and opportunities of using AI in developed political contexts. The aim of this study is to examine the potential of artificial intelligence (AI) within the current political context, particularly regarding the dynamics associated with democratization processes and public opinion building, as well as the legal risks concerning privacy and data protection, especially within the framework of European law.

In line with the discussion, an impartial and informed discourse is necessary, addressing the various challenges associated with this integration. This perspective underscores the importance of conducting a thorough and

balanced evaluation of the effects of AI on the political and legal spheres, as it helps to better understand this dynamic in all its complexity. The evolution of communication technologies has necessitated adjustments to the techniques of message dissemination. Significant social changes, such as the rise in social polarization (Kubin; Von Sikorski, 2021) and the covid-19 pandemic has accelerated the use of digital solutions in public administration, highlighting the need to assess the impact of AI on privacy and civil rights (Milan, 2020). The rapid digitalization caused by the pandemic has drastically altered daily habits and behaviours in urban settings (Gurvich *et al.*, 2021).

The need to modify message dissemination methods stems from a context in which social transformations and new technologies interact in complex ways, influencing both the manner and content of public communication. To address the new dynamics of participation and interaction in the contemporary digital and social landscape, these changes offer both an opportunity and a challenge. Today, both within and outside the scientific community, it is essential to consider the relationship between politics and artificial intelligence.

As this technology has the potential to significantly impact various levels of communication and participation, its manifestation in political events opens up a wide range of horizons. The highly innovative nature of artificial intelligence in shaping current political dynamics is evidenced by its ability to analyse complex data, process information in real-time, and adapt to individual preferences. It is no surprise that research has increasingly focused on how artificial intelligence, robotics, and automation impact the political world. These technologies can transform the way people receive, share, and engage with information, as well as participate in discussions on social media (Battista; Uva, 2023). According to Diakopoulos (2019), this phenomenon is known as “the era of algorithmic news,” which refers to the emergence of a new class of artificial intelligences. Such systems go beyond mere automation, presenting an intriguing concept.

This shift in focus has led to growing interest in a variety of issues arising from the combination of technology and democratic decision-making methods (Battista, 2024b). It is worth noting that, while they may appear to be merely rhetorical exercises, artificial intelligence technologies carry the risk of introducing distortions, manipulation, and misinformation, despite their vast potential to enhance knowledge and social relationships (Aïmeur; Amri; Brassard, 2023). Consequently, addressing the issue solely from a theoretical perspective is insufficient (Hajli *et al.*, 2022), as it raises the “art of illusion”. The proposed approach aims to understand not only the technological dynamics of AI but also how AI influences society, institutions, and democracy. This profound conflict underscores once again the close connection between the adoption of such technologies and highlights the importance of employing a critical and reflective approach to mitigate potential negative effects and promote conscious and ethical use. Nevertheless, it is undeniable that AI within democratic institutions reflects political choices and technological architectures that favor certain actors over others, thanks to rapid technological progress and growing public acceptance (Nemitz, 2018).

Governmental strategies and communications support this argument, describing artificial intelligence (AI) as an inevitable and profoundly transformative technological advancement with favourable economic prospects (Zeng; Chan; Schäfer, 2022). This positioning reflects the perception of AI as a catalyst for significant transformations, including in economic models, highlighting both emerging opportunities and profound implications across various sectors, within the so-called platform capitalism (Srnicek, 2017) – a model based on the collection and monetization of data by major digital platforms. In this rapid evolution, the impact of AI on the political arena cannot be overlooked, as it can significantly influence legislative processes, decision-making flows, and global interactions. The aspiration to assign political responsibilities to AI-based systems reflects the idea that technology is an effective and rational tool capable of impartially guiding decisions and policies. This trend raises important questions about trust in automation in political

leadership and how mechanical and human expertise shapes the future of governmental institutions.

When considering new models of political engagement, replacing decision-making elements traditionally associated with political representatives has emerged as an intriguing and controversial perspective. The concept of humans realizing the will of a non-human entity requires deep reflection on the characteristics and limits of representative democracy. Viewing humans as intermediaries or spokespersons for a non-human entity creates overarching scenarios that require critical analysis of the dynamics of representation, democratic consensus, and fairness in decision-making processes.

The unexpected possibility of physical humans being replaced by AI suggests a stronger link between human actors operating within the political fabric and artificial entities (Auriemma; Battista; Quarta, 2023). This challenge disrupts established paradigms and opens new frontiers for study and reflection in the field of technology and the relationships between society and technology. There is an urgent need to gain public consensus in the electoral marketplace, marked by increasingly unstable controversies and widespread disillusionment with idealistic principles. The opportunity to intensify interactions and dialogues with the public base proves valuable in a context where politics is perceived as distant and where rapid, immediate responses to questions are sought. Political communication supported by non-political actors is crucial for rebuilding connections with the traditional political sphere (Van Aelst *et al.*, 2017).

The collaboration between democratic participation and artificial intelligence not only enhances citizen engagement but also helps in better understanding political issues, outlining a perspective where technology enhances the democratic experience. This awareness emphasizes the importance of active citizen participation in governance, as it is widely acknowledged that dialogue between rulers and the ruled helps promote high standards within a democratic system. The consensus on this consideration is that citizen participation is fundamental to sustaining the vitality and validity of democratic institutions. Understanding this logic provides a means to promote and support

civic aggregation activities to preserve and strengthen the foundations of democracy in contemporary societies. It is a theoretical imperative to rethink and reformulate the traditional paradigm of political participation, considering legal implications.

Finally, the progressive and experimental approach of some projects, such as those cited, suggests a heightened awareness of the difficulties associated with implementing AI in politics in all its forms. The indisputable point is that the path toward the harmonious integration of artificial intelligence into political decision-making processes will require open discussions, strict regulations, and constant ethical monitoring to ensure that these advancements have a positive impact on democracy and political life.

3 Artificial Intelligence and law: challenges and opportunities in the digital society

The social system and the democratic sphere will only be able to coexist if society is able to orient the legal approach to AI, particularly in terms of risks, and with a multidisciplinary method on the one hand, and if a shared global value system emerges that can translate effective rules at the planetary level. This is because the phenomenon under analysis has a scope that transcends traditional boundaries.

Despite its limitations in institutional structure, the European Union serves as a catalyst in regulating the phenomenon, as we will discuss later. However, the attempt must first be political and ethical, and then legal. Only if the implementation of an artificial intelligence system poses potential risks to the violation of a person's integrity and dignity will its use be considered acceptable. Indeed, it has been widely acknowledged that although artificial intelligence is not a person, in the public sphere it raises significant risks for privacy, surveillance and algorithmic discrimination (Eubanks, 2018). Since AI uses a large amount of data to function, this link is necessary: the data known as Big Data (Devins *et al.*, 2017).

Most devices that extract information from the physical and digital world automatically collect the enormous amount of data contained. The real strength of such a large volume of data is not simply the quantity, but its potential usefulness, which includes the possibility of using it for “analytical” purposes, making predictions, and finding relationships. Since AI uses a large amount of data to function, this connection is necessary: data known as Big Data (Devins *et al.*, 2017). Most devices that extract information from the physical and digital world automatically collect the enormous amount of data contained therein. The real strength of such a mass of data is not simply its quantity, but its potential usefulness, which includes the possibility of using it for ‘analytical’ purposes, making predictions and finding relationships. In addition to this, a central value emerges, namely that they are able to generate useful information that can be applied to strategic decisions, a concept that also shifts the focus from the quantity to the quality of the information extracted (Gallo; Fenza; Battista, 2022).

But Big Data constitutes the fuel of artificial intelligence: it enables the training of predictive models capable of identifying behavioural trends and policy orientations (Tufekci, 2014). In the context of digital democracy, this analytical capacity translates into microtargeting tools and automation of political communication, transforming the way citizens are reached, influenced and engaged. Finally, variability highlights the challenge of data consistency and reliability, as they may present anomalies or be influenced by dynamic factors (Sagiroglu; Sinanc, 2013). These dimensions make Big Data a complex but essential resource for driving innovation, and in fact, these features position them as the fundamental resource for the emerging digital market. The phenomenon of the data-driven and algorithmic society (Comunello, 2020), which has led to the continuous daily use of network-connected devices, has created an obvious narrowing between the public and private spheres. This is because every interaction is tracked, and even though the data is anonymous, the latest biometric techniques allow identification of the true owner.

In contrast, the devastating impact of such intelligent systems on individuals' privacy is so significant that legal scholars and policymakers must consider how to strike a necessary balance that ensures both data circulation and privacy protection. In this regard, it has recently been asserted that an existential right related to the permanence of individuals is needed in the face of the danger posed by the all-encompassing perspective of the machine's dominance over humans.

4 AI and data protection: a difficult balance

Daily life is now influenced by AI across various aspects and levels: personal, commercial, political-electoral, sexual, and social. Consequently, the legal aspect as well. Indeed, Article 12 of the Universal Declaration of Human Rights (United Nations, 1948) and Article 8 of the European Convention on Human Rights (Council of Europe, 1950) state that every person has the right to legal protection against arbitrary interference in their private life, family life, home, and correspondence, and that everyone has the right to be protected by the law.

However, it is believed that behavioural information regarding interests, preferences, and personality traits are the most important in the context of Big Data. Algorithmic profiling techniques (Fasan, 2020, p. 11) create an individual behavioural profile of individuals, allowing market operators not only to "[...] tailor each proposal by conforming and packaging it based on the specific character traits of customers". In fact, human activity on electronic devices like smartphones and computers, web browsing, or social media use leaves traces and data. This allows third parties to invade the personal sphere while creating targeted messages to manipulate people's behaviour for political purposes (Benkler; Faris; Roberts, 2018).

This is especially true with machine learning technologies, which can automatically learn, analyze, and deduce new personal information, modify the algorithm, and improve performance based on the data input (Shariff *et al.*, 2024). In this case, it has been correctly observed that extracting and deleting

specific data becomes impossible because they are now part of an algorithm automatically created based on the data entered the system (Battista, 2023).

In this regard, the regulations established by the European Regulation 2016/679 (European Parliament and Council, 2016) concerning the processing, protection, and transmission of personal data have been violated. As a result, the fundamental nature of personal data risks being lost when it is associated with AI systems to constitute the resource of the new digital economy. In this way, the legal expert, particularly the European legislator, seeks to reconcile two requirements that are, in fact, opposite and antithetical, namely the protection of individuals' privacy and the growth of the digital market governed by AI. Despite tentative regulatory efforts in the Old Continent, the law is still unprepared for this complex and epochal challenge. The General Data Protection Regulation (GDPR) was created to find a way to balance data transmission and privacy protection. This is because modern economy is an inescapable fact that the science of law cannot and should not shy away from. The European Regulation on Artificial Intelligence (EU 2024/1689) (European Parliament and Council, 2024), which recognizes the importance of protecting personal data and promoting the circulation that fuels the digital market, seeks to prevent European companies from losing competitiveness compared to those operating in non-European markets.

In this sense, there is a clear distinction between the circulatory and financial function of European legislation and what should have the character of exclusivity, which is a fundamental right of personality. Thus, once again, the market prevails over the individual, fundamental rights, and political choices, meaning that the law prevails. However, this happens only when regulation lacks a global impact and there is a need to act quickly to prevent the collapse of the economic system and its competitiveness. To reaffirm the centrality of human beings in the dynamics of exchange and profit, which should serve rather than objectify those who are subjects, a global constitutive moment must be represented by strengthening the United Nations and its recognition as a global legislative body capable of setting rules on issues whose effects have no borders

and whose solutions can, therefore, be global. The essential nature of the right to privacy is clearly diminished when applied at the regional or continental level.

This is due both to the protection of the digital market and the willingness of individuals to use the powerful technological tools at their disposal in any situation. In the absence of an effective global regulatory proposal, individuals prefer to relinquish the sovereignty of their privacy between the convenience of a world at their fingertips and the defence of a right deemed essential only in Treaties and conference proclamations. The provisions of Article 2 of the AI Act, entitled “Scope” (Edwards, 2021) might make this last consideration seem superfluous, as it provides for the regulation’s application to individuals organizations and providing goods and services within the single market based in a third country outside the Union’s territory. However, since this provision only applies to the “general purposes” of the Union, which are not defined in paragraph 1, letter a, the reference to the applicability of the rules in an extraterritorial context is ambiguous and may be interpreted differently. Adding to this the absence of practical sanctions for violations of the regulation, the legal expert gets the sense that there is little anthropocentrism, with a rhetorical reference to fundamental rights. The point is that the market and the distribution of data are now fundamental to the profits of a few. As a result, human fundamental rights may be instrumentalized and overlooked, especially in a society where “the so-called meta-narratives typical of the great ideologies of the twentieth century are being replaced by a culture of performativity, where reality, expectations, and values are constructed around the effectiveness of achieving results rather than implementing a specific vision of the world.

A world that is changing at a dizzying pace, and the internet in this intricate framework represents the first thing humanity has built that it doesn’t understand, the greatest experiment in anarchy we’ve ever had, to use the words of Eric Schmidt (former CEO of Google). A reality that reveals how this vast vortex of data makes its management difficult. In fact, it is no secret that the so-called big data have made the issue more complex today: it is a massive

accumulation of data that floods the world with information like never before and continues to grow at an uncontrollable pace.

The European Union, for its part, has taken significant steps to try to balance the new needs of the digital market with the protection of its citizens' personal data. First, with the approval of Regulation 2016/679 (European Parliament and Council, 2016), and later, with the addition to the Artificial Intelligence Code: the first global regulation on artificial intelligence. The scope of its regulation is defined as follows in Article 3 of the same:

[...] an automated system designed to operate with varying levels of autonomy and that may present adaptability after deployment and that, for explicit or implicit objectives, deduces from the input received how to generate outputs such as predictions, content, recommendations, or decisions that can affect physical or virtual environments (Almada, 2025, p. 80).

The generality and broadness of the definition are believed to have been intended to reduce the risk that the rule and its scope would quickly become obsolete (Dreier, 2022). In fact, when rules are generalized, the opposite effect occurs it makes them inapplicable because the norm does not have a truly prescriptive scope for behaviour, and the violation does not follow a clear and satisfactory sanction to remedy the infringement of a right. For example, consider the first consideration and Article 1 of the regulation, which emphasize the anthropocentric goal of the regulation in promoting artificial intelligence to protect fundamental human rights. However, the only remedies available for an individual whose fundamental rights have been violated are filing a complaint with the supervisory authority and the right to an explanation under Articles 85 and 86 of the AI Act. Furthermore, it is necessary to highlight another factor that creates doubts and legal knots that are difficult to solve: the relationship between the AI Act and the GDPR. The former is an essential reference because AI systems must operate with a large amount of data. Article 22 of Regulation 2016/679 (European Parliament and Council, 2016) is one of the most important points of contact, in addition to the principles; it states that the data subject has the right not to be subject to decisions based solely on automated processing,

including profiling, unless such processing is necessary for the conclusion or execution of a contract, authorized by EU or member state law, and based on the data subject's consent.

The interaction between the two regulations creates application conflicts because, currently, there is no procedural coordination mechanism, which risks reducing the extent of protection provided to citizens. Additionally, the interaction between the two regulations creates application conflicts because of the principles of consent, data minimization, purpose limitation, transparency, accessibility, and understandability of the GDPR. For example, consider anonymous data, which are widely used by AI and cannot be regulated by a law governing the circulation of personal data of identified or identifiable individuals. Moreover, AI systems that use algorithms to make automated decisions do not operate with the logic of consent, which is the foundation of the Data Protection Regulation. In this sense, it has been observed that, as mentioned earlier, the purpose of processing and the potential use of data may not be determined at the time of collection or, in any case, in advance, thus preventing informed consent and leaving the issue of users' informational asymmetry due to the complexity of AI.

The Regulation for the protection of personal data is unable to uphold privacy principles with respect to artificial intelligence systems, which can bypass the fragile limits imposed by European legislation. Similarly, the European legislator has chosen to adopt AI legislation that has no anthropological or applicative scope in relation to the principles and the deterrent and remedial effectiveness foreseen. The logic of the regulation is always based on personal data concerning which a decision is made by an individual. The data subject controls and, in some cases, manages the data. Self-determination is the cultural foundation of the Regulation, more than the legal foundation. Even though responsibility is reduced, this logic cannot be used for big data, and it will not be possible to imagine individual data management based on consent.

5 The electronic voting system in Estonia: a case study on the integration of Artificial Intelligence in democracy

Estonia is a country internationally recognized as one of the most competitive in the field of digital technologies and e-governance. Since 2007, it has implemented an electronic voting system, becoming a pioneer in the use of new digital technologies to promote citizen participation in political life. Over the years, the Estonian system has evolved, incorporating artificial intelligence (AI) and other advanced technologies to enhance the efficiency and security of the electoral process. For these reasons, it is worth analysing the political, social, and ethical implications of the Estonian electronic voting system, examining the benefits and challenges it entails, with particular attention to voter privacy and institutional transparency (Drechsler; Madise, 2004).

The existing electronic voting system, known as e-Voting, allows voters to cast their vote via the Internet, using an electronic identity card (ID) and a personal password. This system was introduced to facilitate citizen participation and make voting more accessible, particularly for those living abroad or in remote areas of the country. The security of Estonia's electronic voting is based on a complex infrastructure that includes data encryption and multi-factor authentication. In Estonia, internet voting is considered a viable alternative to traditional voting at polling stations: a dual-track system where voters maintain the option to vote using the traditional paper-based system but can also vote electronically in the days leading up to polling day. Online voting is available only during the early voting period, while on election day, voters can only cast their vote using the paper-based ballot. A voter who has opted for home voting can still go to the polling station on election day and vote normally, invalidating their previous internet vote. In general, Estonia has invested heavily in the verifiability of the vote, guaranteed by the fact that the electronic voter can verify their preference via a QR code accessible through an application directly from their smartphone.

In recent years, the implementation of AI has improved the ability to detect anomalies in the electoral process, increasing the security and reliability

of the system (Novelli; Sandri, 2024). AI algorithms are used to monitor voting behaviour, identify potential fraud attempts, and ensure that the electoral process remains impartial and free from external manipulation (Singh; Chatterjee, 2018). Focusing on efficiency and accessibility, the integration of AI into the electronic voting system has enhanced the efficiency of the electoral process. Algorithms can quickly manage and analyses many electoral transactions, reducing vote counting times and facilitating the processing of results in real time.

Undoubtedly, Estonia's electronic voting system has increased democratic participation, especially for Estonian citizens living abroad. According to official data, the adoption of electronic voting has seen a significant increase in voter turnout, particularly among younger people and those with mobility difficulties. Of course, while the use of AI may improve accessibility, it would also raise several significant ethical and legal concerns. On the other hand, the protection of personal data is one of the main concerns associated with the use of electronic voting. Although Estonia's electronic voting system adopts strict encryption standards, the collection of sensitive information, such as voters' identities and their political preferences, poses a risk to privacy (Al-Maaitah; Qatawneh; Quzmar, 2021). The use of AI to monitor voter behaviour could lead to privacy violations, raising questions about the management and storage of personal data. However, although AI can help identify anomalies in the electoral process, there is a risk that the algorithms themselves could be vulnerable to manipulation (Taş; Tanrıöver, 2021). Furthermore, despite advanced security measures, the electronic voting system remains vulnerable to potential cyber-attacks, particularly from external actors.

The integration of AI does not eliminate the risk of attacks by hackers who could compromise the integrity of electoral data or manipulate results. The continuous evolution of attack technologies requires constant updates to security systems and the adoption of new measures to protect the digital infrastructure. The adoption of AI in electronic voting also raises legal issues regarding the protection of voters' fundamental rights. In Europe, the General Data Protection Regulation (GDPR) provides a legal framework for the protection of personal

data, requiring institutions using AI to respect individuals' privacy rights. European legislation mandates that citizens have control over their data and that sensitive information be treated with the utmost respect and transparency. Additionally, the European Union has developed a set of guidelines for the ethical use of AI, including algorithmic transparency, non-discrimination, and accountability in the adoption of digital technologies in the public sector.

These regulations are essential to ensure that the use of AI in electronic voting does not undermine citizens' trust in the electoral system. The Estonian electronic voting system represents a pioneering example of how artificial intelligence can be integrated into politics to improve efficiency, security, and democratic participation. However, the adoption of AI in this context raises significant challenges, particularly in terms of privacy, security, and potential algorithmic biases. It is crucial that the use of AI in the electronic voting system be constantly monitored and regulated to prevent abuse and ensure that voters' rights are respected. International cooperation and the adoption of common ethical and legal standards will be essential to preserve trust in digital democracy. In the 2019 Estonian parliamentary elections, 44.2% of voters used electronic voting, marking an increase compared to previous elections.

This rise highlights growing trust in the i-Voting system and greater democratic participation facilitated by technology. Before the introduction of electronic voting, voter participation in parliamentary elections was lower. For example, in the 2003 elections, the participation rate was 58.9%, while in 2007, the year electronic voting was introduced, participation increased to 61.9%. This increase can be attributed to the introduction of electronic voting, which made the electoral process more accessible and convenient for citizens. The adoption of electronic voting in Estonia has had a positive impact on electoral participation, facilitating access to voting and increasing citizens' trust in the democratic process. The integration of AI has further improved the efficiency and security of the system, helping to consolidate digital democracy in the country. Here is a table showing the trend in voter participation in Estonia's

parliamentary elections, comparing traditional voting with electronic voting, highlighting the increase in participation.

Table 1 - Electoral participation in Estonia: traditional vs. electronic voting

Year	Type of election	Participation (%)	Electronic voting (%)	Increase in participation (%)
2003	Parliamentary Elections	58.9	/	/
2007	Parliamentary Elections	61.9	5.5	3.0
2011	Parliamentary Elections	60.4	24.3	-1.5
2015	Parliamentary Elections	64.2	30.9	+3.8
2019	Parliamentary Elections	63.7	44.2	-0.5

Fonte: Prepared by the author.

Description of Table 1: The table shows participation rates, percentages of electronic voting, and changes in participation for five parliamentary elections between 2003 and 2019. Participation increased most significantly in 2015 (+3.8%) and decreased in 2011 and 2019. Electronic voting began in 2007 and increased steadily, reaching 44.2% in 2019.

The introduction of electronic voting in 2007 led to an immediate increase in voter participation (+3.0%), reaching an initial peak. In subsequent elections, electronic voting participation gradually increased (reaching 44.2% in 2019), but the rate of growth slowed compared to the early years. Overall voter participation in elections with electronic voting was still higher than in traditional elections before 2007. Electronic voting, therefore, had a positive impact on participation, especially among Estonian citizens abroad or those with mobility difficulties. The steady growth in the use of i-Voting is evidence of the growing public trust in the security and reliability of the system. The Estonian electronic voting system, introduced in 2005, has had a significant impact on voter participation, contributing to greater inclusivity and accessibility of the democratic process. The adoption of electronic voting, now supported by artificial intelligence, has facilitated voter participation, particularly for those living abroad or in remote areas, increasing convenience and reducing physical and logistical barriers to voting. Data analysis shows that although overall

participation has varied in different elections, electronic voting has had a long-term positive effect, contributing to a general increase in participation. Specifically, the introduction of electronic voting in 2007 led to an immediate increase of about 3% in participation, with electronic voting reaching a peak of 44.2% in 2019.

However, despite the benefits in terms of accessibility and participation, the adoption of new technologies also brings challenges. Protection of personal data and system security remain key concerns, particularly regarding voter privacy and the risk of manipulation. Despite the implementation of strict security standards and the ongoing evolution of systems, vulnerabilities related to cyberattacks and algorithmic biases still need to be monitored. In conclusion, the Estonian experience demonstrates that the introduction of electronic voting and AI can enhance democratic participation, but it requires constant attention to ensure that voters' rights are protected, the system remains secure and transparent, and ethical and legal concerns are properly addressed.

The adoption of similar technologies in other countries could benefit from Estonia's experience, adapting it to their own needs and ensuring a balance between innovation and civil rights protection. The introduction of electronic voting in Estonia undoubtedly represented a significant step towards modernizing the electoral process, but not without encountering a range of challenges. Although the system has been widely appreciated for its efficiency and its ability to increase democratic participation, difficulties related to data protection, security, and potential digital inequalities have emerged as issues that need to be addressed constantly and rigorously. One of the main challenges concerns the protection of voter privacy. The adoption of an electronic system involves the collection of a significant amount of sensitive data, such as personal identification information and political preferences. Although Estonia implements strict encryption and authentication measures, there remains a risk that this data could be vulnerable to security breaches, such as cyberattacks or unauthorized access. The implementation of a digital identification system through an electronic ID card raises concerns about possible abuses of the

authentication system or identity theft. In an international context, the use of sensitive data could also raise concerns at the European level and beyond, especially regarding compliance with different regulations. Another crucial challenge is cybersecurity. Despite Estonia having developed one of the most advanced protection systems in the world, electronic voting remains a potential target for cyberattacks, both from malicious internal and external actors.

The growing threat of attacks by cybercriminals or foreign states is a constant concern, particularly in a period when digital election manipulation is a globally discussed issue. For instance, during the 2019 elections, the Estonian government had to take rigorous measures to monitor and defend the system against potential DDoS (Distributed Denial of Service) attacks and other forms of digital interference. Although the defence against these attacks was effective, the existing vulnerabilities require continuous updates to security measures and the training of experts to counter new forms of threats. An example of another risk is the possibility that data collected during the electoral process may be used to segment voters based on political preferences, age, gender, or geographic location. This type of manipulation could influence political messaging through social media or other platforms, creating unrepresentative voter bases or even reinforcing informational bubbles. Finally, another challenge is digital inequality, as not all citizens have equal access to the necessary technologies to participate in electronic voting, such as mobile devices, internet access, or adequate digital literacy.

Although Estonia has heavily invested in digital education and infrastructure, there are still segments of the population, particularly the elderly or people living in rural areas, who may not be able to use the electronic voting system. This digital inequality could reduce the inclusivity of electronic voting and contribute to unequal voter participation, especially if measures are not taken to ensure all citizens have equal opportunities to access the necessary technologies. In summary, although electronic voting in Estonia represents a significant innovation and has brought concrete advantages in terms of participation, the challenges it poses are not negligible. Protection of privacy,

security against cyberattacks, the risk of algorithmic biases, inequality in access to technologies, and the need to maintain trust in the system are central issues that need to be addressed. The continuous evolution of technologies and strengthening of data protection regulations, alongside promoting equitable and informed access, are essential to ensuring that the electronic voting system can grow securely, inclusively, and ethically.

6 Conclusion

The advancement of artificial intelligence (AI) is inevitably reshaping the technological and political landscape, presenting opportunities for significant improvements in governance and democratic participation (Dufresne, 2019). However, the integration of AI into the political sphere raises a series of critical questions, particularly regarding the use of personal data and the risk of algorithmic manipulation. The fundamental question that arises is whether the adoption of AI can promote greater transparency and more efficient decision-making processes, or if it poses dangers related to privacy violations and the distortion of the democratic system. In this context, Estonia, which introduced electronic voting in 2005 and integrated AI into its governance system, serves as a valuable case study. The Estonian experience has shown that the use of AI in the electoral system can enhance democratic participation, especially for those living abroad or for citizens with mobility challenges.

The introduction of electronic voting, supported by an advanced digital infrastructure, has helped increase voter turnout, but not without raising concerns regarding security, privacy protection, and equitable access to technology (Barbosa *et al.*, 2021). Estonia has implemented stringent security measures, including authentication via electronic ID cards and the use of encryption, but the system remains vulnerable to cyberattacks, raising questions about its long-term resilience. Moreover, the growing digitalization brings with it issues related to digital inequality, which could limit the inclusivity of electronic voting. Fragmentation in access to the necessary technologies could undermine equal participation, especially among vulnerable segments of the

population. The challenges related to cybersecurity and data protection, along with the need to ensure that the system does not favour political manipulation or algorithmic discrimination, present significant obstacles that must be addressed to avoid potential abuses. Regarding the legal tools for protecting personal data, Europe has implemented advanced regulations such as the General Data Protection Regulation (GDPR), which represents an important step in safeguarding citizens' privacy. However, the continuous evolution of technologies requires constant updating of laws and regulations to effectively address the new challenges posed by AI and new forms of digital surveillance.

Legal implications involve not only data protection but also the need to ensure transparency in the use of algorithms, so that they can be traceable and accountable in the case of automated political decisions. Despite the progress, it is important to emphasize that we are still in the early stages of integrating AI into democratic and political systems. Although technology can be a powerful tool for democracy, it cannot fully replace traditional methods of political participation (Mergel, 2019). The use of electronic voting, while useful for promoting inclusivity and improving the efficiency of the electoral process, should never replace the human and political dimension of democracy.

AI can certainly play an important role in enhancing access to voting and managing political information, but it is crucial that its use does not compromise fundamental principles of freedom, equality, and justice. In conclusion, while AI and digital technologies have the potential to transform democracy and electoral processes, it is crucial that the adoption of these technologies is managed with caution, in respect of citizens' fundamental rights and in accordance with international regulations on privacy and data protection. Democracy cannot be reduced to a mere automated process; it must remain a system that promotes inclusion, transparency, and active participation.

References

AÏMEUR, Eleni; AMRI, Sara; BRASSARD, Gilles. Fake news, disinformation and misinformation in social media: a review. **Social Network Analysis and**

Mining, New York, v. 13, n. 30, p. 1-36, 2023. Disponível em:
<https://doi.org/10.1007/s13278-023-01028-5>. Acesso em: 13 May 2025.

ALMADA, Marco. European Union. What is an artificial intelligence system, really? Notes on the European Commission's guidelines on Article 3 (1) of the AI Act. **Journal of AI Law and Regulation**, Berlin, v. 2, n. 1, p. 76-81, 2025. Disponível em: <https://doi.org/10.21552/aire/2025/1/9>. Acesso em: 13 May 2025.

AL-MAAITAH, Shadi; QATAWNEH, Mohammed; QUZMAR, Anwar. E-voting system based on blockchain technology: a survey. *In*: INTERNATIONAL CONFERENCE ON INFORMATION TECHNOLOGY, 2021. **Proceedings** [...]. New York: IEEE, 2021. p. 200-205.

ARCHIBUGI, Daniele; CELLINI, Marco. The internal and external levers to achieve global democracy. **Global Policy**, New Jersey, v. 8, n. S6, p. 65-77, 2017. Disponível em: <https://doi.org/10.1111/1758-5899.12490>. Acesso em: 13 May 2025.

AURIEMMA, Vincenzo; BATTISTA, Daniele; QUARTA, Serena. Digital embodiment as a tool for constructing the self in politics. **Societies**, Basel, v. 13, n. 12, p. 261, 2023. Disponível em: <https://doi.org/10.3390/soc13120261>. Acesso em: 13 May 2025.

BARBOSA, Manuel; BARTHE, Gilles; BHARGAVAN, Karthikeyan; BLANCHET, Bruno; CREMERS, Cas; LIAO, Kangjie; PARNO, Bryan. SoK: computer-aided cryptography. *In*: IEEE SYMPOSIUM ON SECURITY AND PRIVACY, 2021. **Proceedings** [...]. New York: IEEE, 2021. p. 777-795.

BATTISTA, Daniele. For better or for worse: politics marries pop culture (TikTok and the 2022 Italian elections). **Society Register**, Poznan, v. 7, n. 1, p. 117-142, 2023. Disponível em: <https://doi.org/10.14746/sr.2023.7.1.06>. Acesso em: 13 May 2025.

BATTISTA, Daniele. Political communication in the age of artificial intelligence: an overview of deepfakes and their implications. **Society Register**, Poznan, v. 8, n. 2, p. 8-23, 2024a. Disponível em: <https://doi.org/10.14746/sr.2024.8.2.01>. Acesso em: 13 May 2025.

BATTISTA, Daniele. Comunicazione politica e intelligenza artificiale: un bilancio tra manipolazione e partecipazione. **Rivista di Digital Politics**, Bologna, v. 4, n. 1, p. 71-90, 2024b. Disponível em: <https://www.rivisteweb.it/doi/10.53227/113721>. Acesso em: 13 May 2025.

BATTISTA, Daniele; UVA, Gabriele. Exploring the legal regulation of social media in Europe: a review of dynamics and challenges-current trends and future developments. **Sustainability**, Basel, v. 15, n. 5, p. 1-11, 2023. Disponível em: <https://doi.org/10.3390/su15054144>. Acesso em: 13 May 2025.

BENKLER, Yochai; FARIS, Robert; ROBERTS, Hal. **Network propaganda: manipulation, disinformation, and radicalization in american politics**. Oxford: Oxford University Press, 2018.

COMUNELLO, Francesca. **La società degli algoritmi e dei dati: riflessioni sulla platform society, sul ruolo degli algoritmi e sull'immaginario algoritmico**. Tecnologie della comunicazione e forme della politica. Padova: Fondazione Centro studi filosofici di Gallarate, 2020.

COUNCIL OF EUROPE. **European convention on Human Rights**. Rome: Council of Europe, 4 Nov. 1950. Article 8.

DEVINS, Caryn; FELIN, Teppo; KAUFFMAN, Stuart; KOPPL, Roger. The law and big data. **Cornell Journal of Law and Public Policy**, Ithaca, v. 27, n. 2, p. 357-413, 2017.

DIAKOPOULOS, Nicholas. **Automating the news: how algorithms are rewriting the media**. Cambridge: Harvard University Press, 2019.

DRECHSLER, Wolfgang; MADISE, Ülle. Electronic voting in Estonia. In: KERSTING, Norbert; BALDERSHEIM, Harald (ed.). **Electronic voting and democracy: a comparative analysis**. London: Palgrave Macmillan, 2004. p. 97-108.

DREIER, Thomas. The Deontic power of the Internet-access controls and the obsolescence of legal norms. In: DREIER, Thomas; Tiziana Andina (ed.). **Digital Ethics**. Baden-Baden: Nomos, 2022. p. 297-322.

DUFRESNE, Todd. **The democracy of suffering: life on the edge of catastrophe, philosophy in the Anthropocene**. Canada: McGill-Queen's Press, 2019.

DWIVEDI, Yogesh Kumar *et al.* Artificial Intelligence (AI): multidisciplinary perspectives on emerging challenges, opportunities, and agenda for research, practice and policy. **International Journal of Information Management**, Amsterdam, v. 57, p. 1-47, 2021. Disponível em: <https://doi.org/10.1016/j.ijinfomgt.2019.08.002>. Acesso em: 13 May 2025.

EUBANKS, Virginia. **Automating inequality: how high-tech tools profile, police, and punish the poor**. New York: St. Martin's Press, 2018.

EDWARDS, Lilian. The EU AI Act: a summary of its significance and scope. **Artificial Intelligence (the EU AI Act)**, [s. l.], v. 1, p. 25, 2021.

EUROPEAN PARLIAMENT AND COUNCIL. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free

movement of such data (General Data Protection Regulation). **Official Journal of the European Union**, [s. l.], L 119, p. 1-88, 4 May 2016.

EUROPEAN PARLIAMENT AND COUNCIL. Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence and amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828 (Artificial Intelligence Act). **Official Journal of the European Union**, [s. l.], OJ L 1689, 12 July 2024. CELEX 32024R1689.

FASAN, Michele. Intelligenza artificiale e pluralismo: uso delle tecniche di profilazione nello spazio pubblico democratico. **BioLaw Journal-Rivista di BioDiritto**, Trento, v. 1, p. 345-366, 2020.

FLORIDI, Luciano. **La quarta rivoluzione**: come l'infosfera sta trasformando il mondo. Milano: Raffaello Cortina, 2017.

GALLO, Manuela; FENZA, Giuseppe; BATTISTA, Donato. Information Disorder: what about global security implications? **Rivista di Digital Politics**, Bologna, v. 2, n. 3, p. 523-538, 2022. Disponível em: <https://www.rivisteweb.it/doi/10.53227/106458>. Acesso em: 13 May 2025.

GURVICH, Carolyn *et al.* Coping styles and mental health in response to societal changes during the covid-19 pandemic. **International Journal of Social Psychiatry**, Thousand Oaks, v. 67, n. 5, p. 540-549, 2021. Disponível em: <https://doi.org/10.1177/0020764020961790>. Acesso em: 13 May 2025.

HAJLI, Nick; SAEED, Usman; TAJVIDI, Maryam; SHIRAZI, Fariba. Social bots and the spread of disinformation in social media: the challenges of artificial intelligence. **British Journal of Management**, New Jersey, v. 33, n. 3, p. 1238-1253, 2022. Disponível em: <https://doi.org/10.1111/1467-8551.12554>. Acesso em: 13 May 2025.

KUBIN, Eszter; VON SIKORSKI, Christian. The role of (social) media in political polarization: a systematic review. **Annals of the International Communication Association**, London, v. 45, n. 3, p. 188-206, 2021. Disponível em: <https://doi.org/10.1080/23808985.2021.1976070>. Acesso em: 13 May 2025.

MAKARIUS, Erin E.; MUKHERJEE, Debmalaya; FOX, John D.; FOX, Allison K. Rising with the machines: a sociotechnical framework for bringing artificial intelligence into the organization. **Journal of Business Research**, Amsterdam, v. 120, p. 262-273, 2020. Disponível em: <https://doi.org/10.1016/j.jbusres.2020.07.045>. Acesso em: 13 May 2025.

MERGEL, Ines. Digital service teams in government. **Government Information Quarterly**, Amsterdam, v. 36, n. 4, p. 1-16, 2019. Disponível em: <https://doi.org/10.1016/j.giq.2019.07.001>. Acesso em: 13 May 2025.

MILAN, Stefania. Techno-solutionism and the standard human in the making of the covid-19 pandemic. **Big Data & Society**, Thousand Oaks, v. 7, n. 2, p. 1-17, 2020. Disponível em: <https://doi.org/10.1177/2053951720966781>. Acesso em: 13 May 2025.

NEMITZ, Paul. Constitutional democracy and technology in the age of artificial intelligence. **Philosophical Transactions of the Royal Society A: Mathematical, Physical and Engineering Sciences**, London, v. 376, p. 1-14, 2018. Disponível em: <https://doi.org/10.1098/rsta.2018.0089>. Acesso em: 13 May 2025.

NOVELLI, Claudio; SANDRI, Giulia. Digital democracy in the age of artificial intelligence. **arXiv**, Ithaca, p. 1-27, 2024. Disponível em: <https://doi.org/10.48550/arXiv.2412.07791>. Acesso em: 13 May 2025.

SAGIROGLU, Seref; SINANC, Duygu. Big data: a review. *In*: INTERNATIONAL CONFERENCE ON COLLABORATION TECHNOLOGIES AND SYSTEMS, 2013. **Proceedings** [...]. New York: IEEE, 2013. p. 42-47.

SHARIFF, Mohammed A.; VIMAL, Siva P.; GOPI, Bharathi; ANBARASI, Anandhi; THARUN, Ramesh; SRINIVASAN, Chandrasekaran. Enhancing text input for motor disabilities through IoT and machine learning: a focus on the swipe-to-type algorithm. *In*: INTERNATIONAL CONFERENCE ON COMPUTER, COMMUNICATION AND CONTROL, 2., 2024. **Proceedings** [...]. New York: IEEE, 2024. p. 1-5.

SINGH, Ajay; CHATTERJEE, Krishnendu. SecEVS: secure electronic voting system using blockchain technology. *In*: INTERNATIONAL CONFERENCE ON COMPUTING, POWER AND COMMUNICATION TECHNOLOGIES, 2018. **Proceedings** [...]. New York: IEEE, 2018. p. 863-867.

SRNICEK, Nick. **Platform capitalism**. New Jersey: Wiley, 2017.

TAŞ, Remzi; TANRIÖVER, Ömer Ö. A manipulation prevention model for Blockchain-Based E-Voting systems. **Security and Communication Networks**, New Jersey, v. 2021, n. 1, p. 1-16, 2021. Disponível em: <https://doi.org/10.1155/2021/6673691>. Acesso em: 13 May 2025.

TOOTS, Maarja Olesk. Why e-participation systems fail: the case of Estonia's Osale.ee. **Government information quarterly**, Tartu, v. 36, n. 3, p. 546-559, 2019. Disponível em: <http://dx.doi.org/10.1016/j.giq.2019.02.002>. Acesso em: 13 May 2025.

TUFEKCI, Zeynep. Engineering the public: Big data, surveillance and computational politics. **First Monday**, Chicago, v. 19, n. 7, p. 1-39, 2014. Disponível em: <http://dx.doi.org/10.5210/fm.v19i7.4901>. Acesso em: 13 May 2025.

UNITED NATIONS. **Universal Declaration of Human Rights**. Paris: United Nations, 10 Dec. 1948. Article 12.

VAN AELST, Peter; STRÖMBÄCK, Jesper; AALBERG, Toril; ESSER, Frank; DE VREESE, Claes; MATTHES, Jörg; STANYER, James. Political communication in a high-choice media environment: a challenge for democracy? **Annals of the International Communication Association**, Abingdon, v. 41, n. 1, p. 3-27, 2017. Disponível em: <https://doi.org/10.1080/23808985.2017.1288551>. Acesso em: 13 May 2025.

YEUNG, Karen. Algorithmic regulation: a critical interrogation. **Regulation & Governance**, New Jersey, v. 12, n. 4, p. 505-523, 2018. Disponível em: <https://doi.org/10.1111/reg.12158>. Acesso em: 13 May 2025.

ZENG, Jinghan; CHAN, Chung-hong; SCHÄFER, Mike S. Contested Chinese dreams of AI? Public discourse about artificial intelligence on WeChat and People's Daily Online. **Information, Communication & Society**, London, v. 25, n. 3, p. 319-340, 2022. Disponível em: <https://doi.org/10.1080/1369118X.2020.1776372>. Acesso em: 13 May 2025.

ZUBOFF, Shoshana. The age of surveillance capitalism. In: LONGHOFER, Wesley; WINCHESTER, Daniel (ed.). **Social theory re-wired**. London: Routledge, 2023. p. 203-213.

Do voto eletrônico à IA: lições do caso da Estônia sobre a transformação da democracia digital

Resumo: O avanço da inteligência artificial está transformando o cenário tecnológico e gerando debates sobre seus inúmeros efeitos. A integração da IA na esfera política levanta questões críticas: ela pode aumentar a transparência institucional e os processos de tomada de decisão ou promove o uso manipulador de algoritmos, violando normas éticas e legais? Este estudo examina as implicações da IA na arena política, com foco nos riscos à privacidade dos cidadãos relacionados ao uso de dados e às ferramentas legais disponíveis para protegê-los na Europa. Um caso de particular interesse é a Estônia, líder na adoção de tecnologias digitais na governança pública. Ao analisar sua experiência, esta pesquisa explorará como a IA influencia o sistema eleitoral e a governança, com atenção às consequências éticas, legais e sociais. O estudo avaliará se essas iniciativas são genuinamente democráticas ou

representam uma ameaça aos direitos dos cidadãos. O objetivo é fornecer uma visão geral crítica e abrangente da dinâmica complexa relacionada à implementação da IA na política, contribuindo para a compreensão das implicações dessa tecnologia disruptiva e seu impacto nos sistemas democráticos e nas regulamentações europeias.

Palavras-chave: inteligência artificial; política digital; implicações legais; Estônia; participação eleitoral

Authorship and Responsibility Statement

Conception and design of the study: Daniele Battista

Data collection: Daniele Battista

Data analysis and interpretation: Daniele Battista

Writing: Daniele Battista

Critical review of the manuscript: Daniele Battista

Data availability statement

Not applicable.

Corresponding authorship

Daniele Battista

dbattista@unisa.it

Editor-in-chief

Thiago Henrique Bragato Barros

How to cite

BATTISTA, Daniele. From electronic voting to AI: lessons from the Estonian Case on the transformation of digital democracy. **Em Questão**, Porto Alegre, v. 31, e-145465, 2025. <https://doi.org/10.1590/1808-5245.31.145465>

Open peer review:

<https://doi.org/10.1590/1808-5245.31.145465A>

<https://doi.org/10.1590/1808-5245.31.145465B>

Received: 28/01/2025

Accepted: 27/05/2025

