**International Journal of Political Science (IJPS)**
*Volume 11, Issue 1, 2025, PP 21-27*
*ISSN 2454-9452 (Online)*
*https://doi.org/10.20431/2454-9452.1101003*
*www.arcjournals.org*

# Electronic Voting and Personal Data

**Dr. Aikaterini Pipilou**

*Department of Political Science and International Relations, School of Social and Political Sciences, University of the Peloponesse, Greece*

***Corresponding Author:** ***Dr. Aikaterini Pipilou,*** *Department of Political Science and International Relations, School of Social and Political Sciences, University of the Peloponesse, Greece*

**Abstract:** *The protection of personal data in electronic voting is a complex issue that depends on legislation and ensuring the security of citizens. This process provides ease of participation for voters but raises concerns about the leakage of personal data and votes, discouraging some from participating. Voting is a fundamental right in a democracy, and the leakage of personal data can undermine its functioning. In electronic voting, voter data is stored in databases and is accessible to third parties, increasing the risk of leaks. Furthermore, the confidentiality of the vote, which is linked to individuals' political beliefs, must be protected. Personal data familiarizes citizens with the acceptance of its management by responsible entities without giving them full control over its protection. To address the above issues, strict adherence to legislation is required, along with the use of appropriate technological means to protect the data. The systems must ensure the non-leakage of personal data and the confidentiality of the vote. Additionally, the human resources involved must be suitably trained to handle the processes and identify any potential issues. Furthermore, conducting pilot voting sessions is important to identify weaknesses in the technical systems before their final implementation.*

**Keywords:** *Protection of personal data, Electronic voting, Legislation, Security of citizens, Voter participation, Data leakage, Vote confidentiality*

## 1. Introduction

A reference to the major issues that may arise during the implementation of electronic voting in various electoral contests and procedures, particularly regarding the personal data of voters, as well as a reference to the methods and techniques that can be employed to address and manage these problems effectively, could be of a great scientific interest.

Initially, it is essential for all parties involved to rigorously adhere to the applicable laws, as defined at the national, European, and international levels. As can easily be understood, if the foundation for the protection of personal data during electronic voting has not been adequately secured, such as when the greatest possible effort has not been made to comply with personal data protection legislation, no further protective measures can be enforced. This is because the law itself provides the necessary safeguards for personal data protection in a comprehensive and clear manner, ensuring that its absolute and unconditional application would suffice to guarantee the protection of voter data without requiring additional action, methods, or techniques.

Moreover, the implementation of appropriate technological tools and systems for electronic voting presents a significant challenge, especially considering the dual objective of ensuring valid voting results while protecting the personal data of voters. The technical quality of these tools is inherently linked to the successful execution of electronic voting, making the selection and deployment of the right technology crucial for achieving secure outcomes.

## 2. The Main Issues Arising in the Conduct of Electronic Voting in Relation to the Personal Data of Voters

The protection of personal data can by no means be considered an issue that can be addressed in a one-dimensional manner. On the contrary, it presents various dimensions and is linked both to the relevant laws in force at any given time and to the different requests made by citizens for additional legislative regulations, as well as to the sense of security that should accompany citizens whenever

their personal data is collected, managed, or processed[1]. The electoral process is the highest form of expression of the people's will and is one of the fundamental aspects of democratic governance. Therefore, it is easily understood that the credibility and validity of electronic voting, as well as the sense of security for the citizens participating in it, must be ensured, so that we can talk about the proper functioning of the democratic system in modern societies.

Although electronic voting makes it easier for a larger number of voters to participate in each electoral process and contest, there is still widespread concern about potential leaks of personal data or even the voters' actual choices made through their votes, which discourages some citizens from participating in electronic voting. Voting is a fundamental right for the citizens of a democratically organized state[2]. Therefore, the harm that democracy could suffer if its institutions fail to adequately protect voters' personal data during electronic voting may be significant and serious[3].

It is well known that in the context of conducting electronic voting, the personal data of those participating in the process is stored in specific databases. More specifically, all voters, during the electronic voting process and in order to have the right to participate, call upon and retrieve their personal data from the existing electronic system where it is stored in encrypted and digital form. After identification, they complete the voting process. Therefore, it is understood that these data are not only accessible to the individual to whom they belong, but also to third parties, meaning they are available to the system administrator(s)[4].

Another significant concern is the potential leakage of this data, even by mistake, given its mass digital storage[5]. Hence, great care is needed from those responsible to ensure that this data remains strictly and exclusively within the records of the specific electronic system.

Furthermore, in the context of voting through electronic means, the issue of safeguarding the secrecy of the voter's choice is particularly prominent. An individual's political beliefs[6] are among the most vulnerable personal data, and the expressed political opinion through voting could become a target[7]. For this reason, these data require increased protection from the state during voting with technological means.

Another notable issue in electronic voting is the relativization of personal data. Electronic voting requires conducting the entire electoral process using technological tools, which implies, on one hand, that citizens become accustomed to the idea of granting access and management of their personal data to the responsible processors, as well as the idea of having their data stored in a database over which they have no control. On the other hand, citizens accept the realization of their right to vote through an electronically formatted platform, without being able to know with certainty who has access to their vote. Both of these factors are crucial indicators of the relativization of personal data, as they reflect a decrease in individuals' concern about maintaining the confidentiality of their personal data, which is the core characteristic of this concept[8].

## 3. THE ASSESSMENT OF THE ADEQUACY OR INADEQUACY OF THE LEGISLATIVE FRAMEWORK FOR THE PROTECTION OF PERSONAL DATA DURING THE IMPLEMENTATION OF ELECTRONIC VOTING

At a next level, it is necessary to discuss the specific aspect of ensuring adequate protection of personal data during the implementation of electronic voting, which relates to the adequacy of the legislative framework that can be identified in this regard.

[1]Skinner, G. (2007). Multi-Dimensional Privacy Protection for Digital Collaborations. *International Journal of Security*, 1(1), pp. 22-31.
[2]Brennan, J. (2016). *The Ethics and Rationality of Voting*. [online] Available at: https://plato.stanford.edu/entries/voting/
[3]AEDH. (2017). *Electronic voting: a threat to democracy?* [online] Available at: http://www.aedh.eu/en/electronic-voting-a-threat-to-democracy/
[4]Rexha, B., et al. (2012). Improving authentication and transparency of e-Voting system – Kosovo case. *International Journal of Computers and Communication*, 1(6), pp. 84-91.
[5]Corse, A. (2018). *The Cyberthreats That Most Worry Election Officials*. [online] Available at: https://www.wsj.com/articles/the-cyberthreats-that-most-worry-election-officials-1537322820
[6]Wilson, J.P. & Rule, N. (2014). Perceptions of Others' Political Affiliation Are Moderated by Individual Perceivers' Own Political Attitudes. *PLOS ONE, doi.org/10.1371/journal.pone.0095431*
[7]Bund, J. (2016). Cybersecurity and democracy: Hacking, leaking, and voting. *European Union Institute for Security Studies (EUISS)*, 30(2016), pp. 1-4.
[8]Cheng, L., et al. (2017). Enterprise data breach: causes, challenges, prevention, and future directions. *WIREs Data Mining and Knowledge Discovery*, 7(5), pp. 1211-1225.

Initially, at a primary level, it should be noted that, with the European Regulation No. 679/2016, as mentioned earlier in a previous chapter of this thesis, there has been a stronger and more comprehensive protection in relation to the protection of personal data in general. Therefore, given the generalization and intensification of the processes to safeguard the elements that fall under the concept of personal data, one could conclude that the relevant legislative protection is now adequate. However, the situation is quite different and far from the aforementioned conclusion[9].

### 3.1. Examples of the Inadequacy of the Legislative Framework Fort Protection of Personal Data during the Implementation of Electronic Voting

Furthermore, in order to deepen the above, it is worth specifically mentioning and noting the fact that it is common and even recorded today, even after the implementation of the European Regulation 679/2016, direct violations of the personal rights of individuals during their participation in cases of electronic voting. Therefore, of particular interest at this point is the documentation and presentation of specific examples through which the inadequacy of the legislative framework for the protection of personal data during the implementation of electronic voting is clearly proven.

A first related example, which should be specifically mentioned and referenced here, is that of electronic voting conducted in Estonia, which was the first country to adopt the system of electronic voting in 2005[10]. In the context of conducting this first election, as well as in subsequent years during similar elections, it became apparent that the existing and applicable legislative framework was not able to secure the personal data of Estonian citizens participating in electronic voting. This was because the legislation had not foreseen the necessary safeguards.

### 3.2. Protection of the Subject/Voter in the Event of a Breach of their Personal Data during the Implementation of Electronic Voting

At this point of the voting procedure, what should be attempted is the clarification of the conceptual content of the term "protection" of the individual participating in electronic voting as a voter, always in relation to the protection of personal data. This protection, therefore, could be described as reflecting, according to a significant group of scholars, the sense of security that the citizen/voter has before and during the conduct of electronic voting. In this light, it is observed that the concept of protection takes on a more introspective meaning and relates to the way in which it is experienced by the subject, thus constituting an emotionally charged boundary. According to the view of those who support this interpretation of the concept, this particular aspect of the term is of major importance, given the fact that it largely determines the choice of citizens/voters to participate in electronic voting, a choice that is closely connected with the exercise of their right to participate in the electoral process and, consequently, with the proper functioning of the democratic system[11].

### 3.3. The Protection of the Subject/Voter in the Event of a Breach of their Personal Data during the Implementation of Electronic Voting in the Period Leading Up to its Conduct

As can easily be understood, the period preceding the conduct of electronic voting is extremely critical regarding the protection of personal data, for two main reasons.

The first reason is that during this period, a whole process of collecting, processing, and managing personal data takes place, so the citizen/voter must enjoy the corresponding protection. Specifically, during the process of compiling the electoral rolls, on the basis of which the voting is conducted, and which occurs before the voting itself, each voter must have the ability to ensure that their personal information is not leaked[12].

---

[9]Mendelson, D. (2018). The European Union General Data Protection Regulation (EU 2016/679) and the Australian My Health Record Scheme – A Comparative Study of Consent to Data Processing Provisions. *Journal of Law and Medicine, 26(2018), pp. 23-38*

[10]Springall, D., et. al. (2014). *Security Analysis of the Estonian Internet Voting System*. [online] Available at: http://delivery.acm.org/10.1145/2670000/2660315/p703springall.pdf?ip=178.59.222.240&id=2660315&acc=OA&key=4D4702B0C3E38B35%2E4D4702B0C3E38B35%2E4D4702B0C3E38B35%2E638B5282305ABE89&__acm__=1549903887_f956a55326df2f5360b5cca40875fc8f

[11]uiderveen Borgesius, F., et. al. (2018). Online Political Microtargeting: Promises and Threats for Democracy. *Utrecht Law Review, 14(1), pp. 82-96*

[12]Abramson, M. & Means, G. (Eds). (2001). *E-government 2001*. Lanham: Rowman & Littlefield

The second reason is that during the same period, the voter—participating in electronic voting—must enjoy protection for their personal data embedded in the electronic voting system, from potential exploitation for various purposes, which may be commercial, political, or of any other nature. Therefore, in light of the above, and especially during this period leading up to electronic voting, the issue of protecting the subject/voter becomes a major concern. Given that the stricter European Regulation 679/2016 is now in force, the intensification and strengthening of protective measures become legally imperative[13].

### 3.4. The protection of the subject/voter in the event of a breach of their personal data during the implementation of electronic voting in the period of its conduct

Furthermore, the moment of conducting the electronic voting is undoubtedly the most important for the protection of the personal data of citizens/voters. This is easy to understand, given the fact that at this stage, not only their personal data, those that individualize them, are exposed to various forms of management and processing, but additionally, the issue of protecting the confidentiality of the vote, or their choice within the framework of electronic voting, becomes particularly critical. Undoubtedly, this element constitutes one of the most essential personal data and requires the highest level of protection[14].

However, and in any case, what must be particularly emphasized here is the fact that the sense of security among voters, as detailed above, is placed at the center of this stage of electronic voting, as it, on the one hand, highlights the proper functioning of the democratic system in practice, and on the other hand, determines the future participation of the voter in subsequent electronic elections[15].

### 3.5. Techniques for Addressing Problems Arising in the Context of Electronic Voting Regarding Voters' Personal Data

Initially, particular care is required from all involved parties to strictly adhere to the applicable legislation, as it is found at national, European, and international levels[16]. Being easily understood, in the case where the basis for the entire process of protecting personal data during electronic voting is not ensured, that is, if the utmost effort has not been made to ensure the observance and application of relevant data protection legislation, no further protective process can be demanded. This is because the law itself offers all the necessary guarantees for the protection of personal data, clearly and comprehensively, so that its absolute and unconditional implementation would ensure this protection without the need for any additional action, method, or technique[17].

Indeed, the data protection legislation, particularly as it is defined today after the enactment of the European Union Regulation No. 2016/679, is complete and absolute, ensuring that no further procedures are necessary, as the protective framework addresses both the prevention and suppression of any action related to the violation of citizens' personal data[18].

Moreover, within the context of conducting electronic voting, a significant challenge lies in finding and choosing the technological tools and means that will be used, both from the perspective of ensuring smooth execution in a way that results in valid outcomes and from the perspective of protecting the personal data of those participating. This is because the issue of ensuring the high technological quality required for the electronic voting process is intrinsic to the very possibility of conducting such a vote. Thus, alongside the provision of most regulations accompanying electronic

[13]Petrucco, F. (2018). *The Right to privacy and new technologies: between evolution and decay*. UK: Media Laws

[14]Thi, A. & Dang, T. (n.d.). *Privacy preserving in electronic voting*. [online] Available at: https://pdfs.semanticscholar.org/5c4c/08411f7d811ad5420df72b40f8a50a3b4a53.pdf

[15]European Parliament. (2018a). *Prospects for e-democracy in Europe. Part II: Case studies*. Brussels: European Union

[16]Mostert, M., et al. (2017). From Privacy to Data Protection in the EU: Implications for Big Data Health Research. *European Journal of Health Law, 25*(1), pp. 43-55.

[17] Cavoukian, A. (2011*). Privacy by Design in Law, Policy, and Practice: A White Paper for Regulators, Decision-makers, and Policy-makers*. Ontario: Information and Privacy Commissioner.

[18]Tikkinen-Piri, C., et al. (2018). EU General Data Protection Regulation: Changes and Implications for Personal Data Collecting Companies. *Computer Law & Security Review, 34*(1), pp. 134-153.

voting, particular importance lies in determining, by experts, how the electronic tools to be used will ensure the protection of voters' personal data[19].

Following the above, it can be noted that the achievements of technology, including both the electronic media as physical tools and the intangible programs that define the operation of the electronic tools to be used, are capable of creating a secure environment for conducting electronic voting with respect to personal data. This observation is of great importance because only if all the above elements function correctly can the protection of voters' personal data during the voting process be achieved in practice.

Regarding the technological and electronic tools to be used during electronic voting[20], it should be especially emphasized that these tools must be equipped with mechanisms and programs designed to prevent any possible interference with voters' personal data[21]. These systems inherently guarantee the non-leakage of personal data and the secrecy of the vote[22].

Furthermore, special mention should be made of the human resources that will staff the entire electronic voting process, that is, those who will contribute to its smooth execution. This is because the electronic voting process is not a simple, systematic process; rather, it is a complex operation in all its stages, including preparation, execution, and result extraction, where human involvement can play a decisive role[23].

Indeed, as demonstrated by international practice, assigning the appropriate tasks to the right people in cases where electronic voting occurs significantly contributes to the protection of voters' personal data[24]. This is because selecting the appropriate personnel based on their scientific knowledge and training enables the prediction of potential problems or malicious actions that could lead to violations of personal data[25]. Even in cases where there is no issue of error or malicious action, proper handling by these individuals of all the processes directly related to electronic voting can serve as an important safeguard for the protection of voters' personal data[26].

Additionally, voters' personal data protection within the framework of electronic voting can be ensured through the conduct of a pilot voting process using electronic means prior to the final vote[27]. It is therefore understood that a necessary prerequisite for ensuring the proper functioning of all utilized electronic tools and systems, so that electronic voting is conducted smoothly, is the prior conduct of a trial vote, identical to the actual one, using the same electronic and technological tools and software. The various data used in this process must, of course, be protected[28].

The great importance of this pilot implementation of electronic voting is self-evident, as it allows testing both the technical capabilities of the tools to be used and the electronic programs to identify any weaknesses or errors and to correct them before the final implementation in the actual voting

[19] Norwegian Ministry of Local Government and Regional Development. (2006). *Electronic Voting – Challenges and Opportunities*. Norway: MLGRD, pp. 20-98.
[20] Russell, M. & Zamfir, I. (2018). *Digital Technology in Elections: Efficiency versus Credibility*. [online] Available at: http://www.europarl.europa.eu/RegData/etudes/BRIE/2018/ 625178/EPRS_BRI (2018)625178_ EN.pdf.
[21] Committee of Ministers – Council of Europe. (2017). *1289th Meeting, 14 June 2017: Democracy and Political Questions*. [online] Available at: https://rm.coe.int/1680726c0b
[22]Jenke, L. & Huettel, S. (2016). Issues or Identity? Cognitive Foundations of Voter Choice. *Trends in Cognitive Sciences Journal, 20*(11), pp. 794–804.
[23]Goldsmith, B. & Ruthrauff, H. (2013). *Implementing and Overseeing Electronic Voting and Counting Technologies*. USA: USAID, pp. 153-211.
[24]Jones, D. (2001). *Problems with Voting Systems and the Applicable Standards*. [online] Available at: http://homepage.divms.uiowa.edu/~jones/voting/congress.html.
[25] The Carter Center. (2012). *Observing Electronic Voting*. Atlanta: One Copenhill, pp. 29-94.
[26] Frangakis, N. (2007). Digital Democracy and Threats to Privacy. *Human Rights, 34*(2007), pp. 459-470.
[27] Root, D. & Kennedy, L. (2017). *9 Solutions to Secure America's Elections*. [online] Available at: https://www.americanprogress.org/issues/democracy/reports/2017/08/16/437390/9-solutions-secure-americas-elections/.
[28] Kumar, S. & Walia, E. (2011). Analysis of Electronic Voting System in Various Countries. *International Journal on Computer Science and Engineering (IJCSE), 3*(5), pp. 1825-1830.

process. After all, there are certain technical and operational issues that can only emerge during the implementation of the process, which cannot be anticipated or derived theoretically[29].

## 4. CONCLUSION

From what has been presented one way conclude that the protection of personal data in electronic voting is a multifaceted issue that requires careful consideration at every stage of the voting process. Ensuring the confidentiality, integrity, and security of voters' personal data is paramount to maintaining the credibility of the electoral process and safeguarding democratic values. While technological advancements offer the potential for more efficient and accessible voting, they also introduce significant risks, including data breaches and the compromise of voter privacy. To address these challenges, strict adherence to existing data protection legislation, the implementation of secure technological solutions, and the involvement of well-trained personnel are essential. Furthermore, conducting pilot trials before the actual voting process can help identify and correct any vulnerabilities. In addition, only through a comprehensive approach that combines legal, technical, and human resource strategies can the integrity of electronic voting systems be ensured, fostering public trust in the democratic process. Finally, the need for new legislative interventions regarding the protection of personal data during the implementation of electronic voting is now deemed crucial.

## REFERENCES


[1] Abramson, M. & Means, G. (Eds). (2001). *E-government 2001*. Lanham: Rowman & Littlefield.

[2] AEDH. (2017). *Electronic voting: a threat to democracy?* [online] Available at: http://www.aedh.eu/en/electronic-voting-a-threat-to-democracy/.

[3] Brennan, J. (2016). *The Ethics and Rationality of Voting*. [online] Available at: https://plato.stanford.edu/entries/voting/.

[4] Bund, J. (2016). Cybersecurity and democracy: Hacking, leaking, and voting. *European Union Institute for Security Studies (EUISS)*, 30(2016), pp. 1-4.

[5] Cavoukian, A. (2011*). Privacy by Design in Law, Policy, and Practice: A White Paper for Regulators, Decision-makers, and Policy-makers.* Ontario: Information and Privacy Commissioner.

[6] Cheng, L., et al. (2017). Enterprise data breach: causes, challenges, prevention, and future directions. *WIREs Data Mining and Knowledge Discovery*, 7(5), pp. 1211-1225.

[7] Committee of Ministers – Council of Europe. (2017). *1289th Meeting, 14 June 2017: Democracy and Political Questions*. [online] Available at: https://rm.coe.int/1680726c0b.

[8] Corse, A. (2018). *The Cyberthreats That Most Worry Election Officials*. [online] Available at: https://www.wsj.com/articles/the-cyberthreats-that-most-worry-election-officials-1537322820.

[9] European Parliament. (2018a). *Prospects for e-democracy in Europe. Part II: Case studies*. Brussels: European Union.

[10] Frangakis, N. (2007). Digital Democracy and Threats to Privacy. *Human Rights, 34*(2007), pp. 459-470.

[11] Goldsmith, B. & Ruthrauff, H. (2013). *Implementing and Overseeing Electronic Voting and Counting Technologies*. USA: USAID, pp. 153-211.

[12] Jenke, L. & Huettel, S. (2016). Issues or Identity? Cognitive Foundations of Voter Choice. *Trends in Cognitive Sciences Journal, 20*(11), pp. 794–804.

[13] Jones, D. (2001). *Problems with Voting Systems and the Applicable Standards*. [online] Available at: http://homepage.divms.uiowa.edu/~jones/voting/congress.html.

[14] Kumar, S. & Walia, E. (2011). Analysis of Electronic Voting System in Various Countries. *International Journal on Computer Science and Engineering (IJCSE), 3*(5), pp. 1825-1830.

[15] Mendelson, D. (2018). The European Union General Data Protection Regulation (EU 2016/679) and the Australian My Health Record Scheme – A Comparative Study of Consent to Data Processing Provisions. *Journal of Law and Medicine, 26(2018), pp. 23-38.*

[16] Mostert, M., et al. (2017). From Privacy to Data Protection in the EU: Implications for Big Data Health Research. *European Journal of Health Law, 25*(1), pp. 43-55.

[17] Norwegian Ministry of Local Government and Regional Development. (2006). *Electronic Voting – Challenges and Opportunities*. Norway: MLGRD, pp. 20-98.

[18] Petrucco, F. (2018). *The Right to privacy and new technologies: between evolution and decay.* UK: Media Laws.


[29] The Carter Center. (2007). *Developing a Methodology for Observing Electronic Voting*. Atlanta: One Copenhill, pp. 13-17.

[19] Rexha, B., et al. (2012). Improving authentication and transparency of e-Voting system – Kosovo case. *International Journal of Computers and Communication*, 1(6), pp. 84-91.

[20] Root, D. & Kennedy, L. (2017). *9 Solutions to Secure America's Elections*. [online] Available at: https://www.americanprogress.org/issues/democracy/reports/2017/08/16/437390/9-solutions-secure-americas-elections/.

[21] Russell, M. & Zamfir, I. (2018). *Digital Technology in Elections: Efficiency versus Credibility*. [online] Available at: http://www.europarl.europa.eu/RegData/etudes/BRIE/2018/625178/EPRS_BRI(2018)625178_EN.pdf.

[22] Skinner, G. (2007). Multi-Dimensional Privacy Protection for Digital Collaborations. *International Journal of Security*, 1(1), pp. 22-31.

[23] Springall, D., et. al. (2014). *Security Analysis of the Estonian Internet Voting System*. [online] Available at: http://delivery.acm.org/10.1145/2670000/2660315/p703-springall.pdf?ip=178.59.222.240&id=2660315&acc=OA&key=4D4702B0C3E38B35%2E4D4702B0C3E38B35%2E4D4702B0C3E38B35%2E638B5282305ABE89&__acm__=1549903887_f956a55326df2f5360b5cca40875fc8f.

[24] The Carter Center. (2007). *Developing a Methodology for Observing Electronic Voting*. Atlanta: One Copenhill, pp. 13-17.

[25] The Carter Center. (2012). *Observing Electronic Voting*. Atlanta: One Copenhill, pp. 29-94.

[26] Thi, A. & Dang, T. (n.d.). *Privacy preserving in electronic voting*. [online] Available at:https://pdfs.semanticscholar.org/5c4c/08411f7d811ad5420df72b40f8a50a3b4a53.pdf.

[27] Tikkinen-Piri, C., et al. (2018). EU General Data Protection Regulation: Changes and Implications for Personal Data Collecting Companies. *Computer Law & Security Review, 34*(1), pp. 134-153.

[28] Wilson, J.P. & Rule, N. (2014). Perceptions of Others' Political Affiliation Are Moderated by Individual Perceivers' Own Political Attitudes. *PLOS ONE, doi.org/10.1371/journal.pone.0095431.*

[29] Zuiderveen Borgesius, F., et. al. (2018). Online Political Microtargeting: Promises and Threats for Democracy. *Utrecht Law Review, 14(1), pp. 82-96.*

**Citation:** *Dr. Aikaterini Pipilou. "Electronic Voting and Personal Data" International Journal of Political Science (IJPS), vol 11, no. 1, 2025, pp. 21-27. doi: https://doi.org/10.20431/2454-9452.1101003.*