THE USE OF MODERN INFORMATION TECHNOLOGIES DURING ELECTIONS IN DEVELOPED COUNTRIES

Polotnianko Oksana

DOI: https://doi.org/10.61345/1339-7915.2024.6.13

Annotation. The article is devoted to the study of the use of modern information technologies during elections in developed countries, focusing on how digital innovations have transformed electoral processes. The research examined the adoption of electronic voting systems, biometric identification methods, blockchain-based platforms, and artificial intelligence-driven monitoring tools, highlighting their role in enhancing efficiency, transparency, and voter engagement. The integration of these technologies has led to significant changes in how elections are administered, addressing long-standing challenges related to vote counting accuracy, voter authentication, and combating disinformation.

Considered were the practical applications and challenges associated with deploying advanced technologies in electoral processes across different regions. The analysis revealed that electronic voting systems, particularly Direct Recording Electronic machines and optical scan devices, have improved vote tabulation speed and accuracy while raising cybersecurity concerns requiring robust mitigation strategies. Biometric technologies have been instrumental in reducing voter fraud by enabling quick and reliable voter verification, though they present ethical dilemmas regarding personal data protection.

Investigated were the pivotal success factors and recurring challenges that arise when integrating information technologies into electoral frameworks. Key determinants of successful technology adoption included the establishment of comprehensive legal frameworks that delineate stakeholder responsibilities, sustained financial investment in infrastructure modernization, and the implementation of public awareness campaigns to build voter confidence. The research highlighted how countries like Estonia have pioneered internet voting systems with strong cybersecurity safeguards, while others, such as the United States, have prioritized decentralized approaches with varying levels of technological sophistication across states.

Deserves special attention the ethical, legal, and practical considerations that accompany the digitalization of elections, as the increasing reliance on technology brings both unprecedented opportunities and complex risks. Cybersecurity threats, including hacking, malware attacks, and data manipulation, were identified as pervasive challenges requiring multilayered defense systems and continuous monitoring to safeguard electoral integrity.

Key words: electronic voting systems, blockchain technology, artificial intelligence, electoral processes, developed countries, cybersecurity, digital governance, voter engagement, disinformation monitoring, data privacy, election transparency.

1. Introduction.

The rapid development and integration of modern information technologies into electoral processes have fundamentally transformed how elections are conducted, particularly in developed countries where digital infrastructure and technological literacy are more advanced. The use of these technologies has become increasingly significant in enhancing voter participation, ensuring transparency, and improving the efficiency of electoral management systems. As societies become more digitized, traditional methods of voting and election monitoring have been supplemented—and in some cases replaced—by electronic voting systems, biometric identification technologies, blockchain-based transparency solutions, and artificial intelligence tools used for monitoring election integrity and combating disinformation. This shift toward digital elections is driven not only by technological advancements but also by the growing demands for more accessible, secure, and transparent electoral processes that can meet the challenges of modern governance and voter expectations.

The growing reliance on information technologies during elections raises important questions about the future of democratic participation and the role of digital innovation in shaping political engagement. As election authorities and policymakers continue to explore new ways to leverage technology for more efficient and transparent electoral processes, it is vital to assess both the opportunities and challenges these innovations present. This study not only aims to contribute to the academic discourse on electoral modernization but also seeks to provide practical recommendations for policymakers, election officials, and international organizations striving to develop technology-driven solutions that uphold electoral integrity while enhancing voter confidence and inclusivity.

2. The methodological basis of the study.

The methodological basis of the study was a combination of general scientific and special research methods. The comparative legal method was used to analyse electoral technologies in developed countries, while the systematic approach helped to identify key relationships between technological innovations and electoral integrity. Case studies, content analysis of regulatory documents, and statistical data analysis were used to assess the effectiveness of the use of information technology in elections. The study also paid special attention to scientists (Antonyan T., Davtyan S., Kentros S., Kiayias A., Michel L., Nicolaou N., Russell A., Shvartsman A.A., Ibáñez E., Galdámez N., Estrebou C., Pasini A., Chichizola F., Rodríguez I., Pesado P., Zheng Z., Xie S., Dai H., Chen X., Wang H., Ferrara E., Teslim B., Baringer A., Herron M.C., Smith D. A., Mildebrath H., Shahandashti S.F., Hao F., Kumar S., Walia E., Ilechukwu M., Uzoka E., Madubike B., Ijagbemi A., Chukwu C.) who have studied the introduction of new technologies in the electoral process.

3. The aim of the work is to analyze how developed countries utilize modern information technologies during elections, examine the benefits and risks associated with their implementation, and assess the implications for electoral integrity and democratic participation.

4. Review and discussion.

Modern elections have increasingly incorporated innovative information technologies with the goal of enhancing efficiency, accuracy, and public confidence in democratic processes, yet numerous challenges tied to security, privacy, and accessibility continue to arise alongside these developments. Various digital tools have transformed traditional balloting techniques and offered new avenues for promoting transparency, creating a dynamic landscape that demands ongoing refinement of legal, technical, and administrative frameworks.

Electronic voting systems are among the most prominent innovations in the electoral sphere, since they rely on digital interfaces to capture, tabulate, and transmit voters' choices. Several configurations exist, including Direct Recording Electronic machines that register selections on touch-screen displays and optical scan devices that read marks on paper ballots through digital imaging [1]. These systems can expedite vote counting and reduce human errors in tallying, making them appealing in jurisdictions that contend with vast electoral constituencies or stringent time constraints. The reliance on software, however, magnifies the threat of cyberattacks and technical failures that could undermine voter trust or skew election outcomes. Some regions mandate the use of voter-verified paper audit trails in an attempt to address these concerns, because physical ballot records can enable transparent recounts and cybersecurity analyses, thus reinforcing confidence in final results.

Biometric technologies that analyze unique physical or behavioral traits represent another essential component of contemporary voter identification processes, particularly in settings characterized by historical issues related to identity fraud, inflated registration rolls, or prevalent impersonation. Fingerprint, iris, or facial recognition devices can confirm a voter's identity in seconds, thereby reducing the likelihood of multiple ballots cast by a single individual [2]. These technologies often interface with centralized databases that store the biometric profiles of registered citizens, enabling swift and reliable authentication procedures at polling locations. Implementing such solutions raises ethical concerns regarding personal data management and civil liberties, due to the potentially invasive nature of collecting highly sensitive information that might be misused by unauthorized actors. Robust encryption, strict access controls, and regulatory oversight are typically cited as vital safeguards when employing these systems in large-scale elections.

Blockchain-based voting platforms have also attracted attention as promising avenues for guaranteeing the integrity and transparency of electoral processes, given that decentralized ledgers secured by cryptographic protocols allow tamper-resistant and publicly auditable records. Every ballot transaction, once verified through consensus algorithms across a distributed network, is almost impossible to alter or delete without alerting multiple stakeholders [3]. Numerous test cases highlight the potential for improved voter confidence by eliminating single points of failure and central authority vulnerabilities, although challenges remain in the form of computational overhead and bandwidth limitations that could pose barriers to widespread adoption. These considerations underscore the need to balance resilience and user-friendliness, particularly when designing blockchain solutions capable of serving large electorates.

Artificial intelligence has gradually assumed a significant role in monitoring election-related activities and identifying disinformation tactics that threaten to erode public trust. Advanced algorithms can automatically assess vast volumes of digital content, including multimedia assets that may be doctored to mislead potential voters, thereby detecting and flagging suspicious materials with remarkable speed. Social media sentiment analyses, combined with deep learning techniques, can unmask viral campaigns orchestrated to spread inflammatory rhetoric or divisive narratives, ultimately contributing to a more evidence-driven response against malicious efforts aimed at manipulating public opinion [4]. Critics caution that AI-based oversight carries distinct pitfalls stemming from the risks of algorithmic biases, false positives, and inadvertent censorship. Systems designed to protect civic discourse might mistakenly block legitimate content or reinforce existing prejudices within datasets, revealing a delicate tension between fostering accuracy and respecting fundamental freedoms of expression.

The interplay among electronic voting systems, biometric identification, blockchain-based platforms, and AI-driven surveillance illustrates the complexity of delivering credible and inclusive elections in a connected global environment. Each approach offers distinct advantages, such as speed, data security, and robust audit capabilities, while simultaneously raising concerns connected to civil liberties, system vulnerabilities, and computational costs [5]. Establishing comprehensive standards and regulatory mechanisms requires coordinated action by governments, software developers, cybersecurity professionals, election officials, and civil society groups. Trust in outcomes ultimately hinges on striking a careful balance between the transformative potential of new tools and the preservation of voter privacy, fairness, and democratic principles, ensuring that technological progress does not come at the expense of transparency and accountability.

Developed nations have made considerable strides in implementing information technologies within their electoral frameworks, resulting in diverse outcomes that reflect variations in legal structures, political cultures, and public attitudes toward digital governance. The United States has frequently been at the forefront of technological experimentation, illustrated by the deployment of electronic poll books and automated ballot scanners in multiple states, as well as the adoption of online voter registration portals designed to enhance accessibility for citizens residing abroad or in remote areas [6]. These platforms have often operated under strict federal and state guidelines, including mandatory security audits and certification procedures, in an effort to minimize vulnerabilities linked to malware, hacking, or user negligence. The national landscape nevertheless remains highly decentralized, given that each state retains considerable discretion in electoral administration, leading to uneven implementation of advanced technologies across the country. In parallel, high-profile instances of attempted foreign interference have driven policy discussions around strengthening cybersecurity protocols, improving oversight of third-party vendors, and maintaining robust paper-based contingencies, often known as voter-verified paper audit trails, to ensure that every recorded ballot can be independently reviewed and authenticated in the event of a contested outcome.

European Union member states have also embraced forward-looking solutions aimed at modernizing electoral operations, although their approaches differ based on unique constitutional traditions and administrative structures. Some nations maintain e-voting pilot programs that integrate internet-based mechanisms, facilitating remote casting of ballots and real-time monitoring of turnout trends. Others have focused on digital voter registration systems that incorporate secure electronic signatures and government databases for identity verification, thereby expediting the enrollment process and reducing the risk of clerical errors [7]. Estonia is frequently referenced as a pioneer of nationwide internet voting solutions, having refined a digital infrastructure anchored in cryptographic safeguards, citizen identity cards, and transparent auditing procedures. Adoption rates for electronic ballots in such jurisdictions have grown in tandem with public confidence, although concerns persist regarding the potential exclusion of individuals who lack reliable internet access or sufficient digital literacy. Similarly, debates continue around the need to guarantee secrecy and anonymity during electronic voting sessions, a particularly sensitive issue in the context of remote ballot submission from personal devices.

The Asia-Pacific region has witnessed a surge in technological innovations geared toward enhancing voter engagement and administrative efficiency, although levels of sophistication vary considerably. Some jurisdictions have introduced mobile applications that disseminate real-time updates on polling station congestion, thereby enabling voters to plan visits at off-peak hours and reduce queue times. Others have leveraged biometrics to streamline voter identification, a process that mitigates imposture risks and curbs the incidence of duplicate registrations. Certain governments have likewise developed interactive platforms that encourage voter education through digital forums, automated reminders, and targeted campaigns, aiming to boost turnout among younger citizens [8]. These efforts occasionally intersect with broader digital initiatives, such as the integration of electoral data with national identification systems that consolidate multiple government services under a single secure platform. Nonetheless, many countries in this region face challenges related to the heterogeneity of rural populations, linguistic diversity, and the sheer scale of logistical planning required to serve expansive voter bases, particularly during national elections.

A comparative analysis of these cases highlights several pivotal success factors that transcend regional boundaries, including a clear legal framework that delineates responsibilities for security and reliability, consistent funding for infrastructure modernization, and sustained communication campaigns that foster trust among citizens who might be wary of digital solutions. Moreover, cross-jurisdictional collaboration and knowledge exchange appear crucial to surmounting technical roadblocks, as practices that prove advantageous in one nation can be adapted to the institutional realities of another [9]. Remaining challenges tend to revolve around cybersecurity vulnerabilities, potential breaches of voter privacy, and the digital divide that can exclude marginalized populations from fully reaping the benefits of technological progress. In view of these patterns, investments in secure systems, transparent auditing processes, and inclusive policy design appear to be critical for striking a balance between innovation and the ethical obligations inherent in administering modern elections in advanced democracies.

Modern electoral processes that integrate cutting-edge digital tools must contend with a broad spectrum of risks, challenges, and ethical dilemmas, necessitating rigorous oversight and careful deployment strategies. Cybersecurity vulnerabilities represent one of the most pervasive threats in this domain, given that malicious actors can exploit software weaknesses, phishing schemes, or distributed denial-of-service campaigns to disrupt voting infrastructure or manipulate sensitive data. Many election-management bodies have instituted multi-layered defense systems that incorporate robust encryption protocols, intrusion detection mechanisms, and frequent patch updates to servers and other critical components, although these measures demand continuous adaptation in response to rapidly evolving threats and techniques [10]. Information sharing among government agencies, cybersecurity professionals, and private-sector partners has gained momentum, providing opportunities for intelligence exchange regarding emerging attack vectors. In addition, comprehensive contingency plans that include paper backups and manual audits can safeguard the integrity of final vote counts even when digital systems come under attack, mitigating the risk of severe operational breakdowns.

Technological inequality and voter exclusion pose equally pressing concerns, since some populations face barriers in accessing devices, stable internet connections, or digital literacy resources. Marginalized groups residing in rural locales may be disproportionately affected by insufficient infrastructure, which can prevent full participation in electronic or internet-based voting procedures. Elderly citizens and individuals unfamiliar with digital interfaces may also hesitate to engage with new systems that replace traditional ballot methods, potentially lowering turnout in critical demographics. Although outreach efforts, public education campaigns, and the design of user-friendly platforms can narrow these gaps, policymakers must remain attentive to bridging the digital divide and ensuring that innovations do not inadvertently marginalize large segments of the electorate. In that vein, investments in accessible hardware, dedicated training sessions, and simplified interfaces can help modern election systems become more inclusive for those with limited exposure to technology.

Ethical dilemmas relating to data privacy and surveillance arise whenever advanced information technologies intersect with electoral activities, since the accumulation of personal details can create opportunities for invasive data mining or unauthorized monitoring of citizens. Political parties, state authorities, and private entities might harvest voter records and online behavior profiles with the intention of refining campaign strategies, raising questions about consent and the erosion of personal autonomy. Legal frameworks frequently require that any data collected during voter registration or biometric authentication remain secure, with limitations imposed on usage, retention, and third-party sharing. Encryption protocols, access control measures, and transparent oversight mechanisms are indispensable for maintaining public trust in these processes, yet the tension between efficient electoral administration and individual rights persists. Concerns that widespread surveillance could influence voting behavior or foster self-censorship underscore the importance of balancing innovation with robust protections that preserve democratic values.

The integration of modern technologies in electoral systems also brings forth legal and regulatory challenges, including discrepancies between federal and regional jurisdictions, gaps in existing statutes, and the need for specialized technical expertise among lawmakers. Legislative bodies are frequently compelled to revise election codes and enact data protection regulations that address emerging risks connected to remote voting platforms, biometric authentication procedures, or machine-learning algorithms employed for disinformation detection. Clear guidelines on responsibility allocation are vital: vendors, election officials, and government agencies must be aware of their respective obligations in safeguarding infrastructure, maintaining transparency, and upholding fundamental civil liberties. International cooperation often proves advantageous in this realm, with transnational bodies adopting joint standards or sharing proven tactics for preventing hacking incidents, data leaks, and system malfunctions. Nevertheless, the rapid pace of technological advancement can outstrip the capacity of legal systems to respond promptly, which underscores the necessity of ongoing legislative review, adaptive governance practices, and multi-stakeholder collaboration to mitigate potential damage and ensure that digital innovation remains consistent with the core principles underpinning fair and equitable elections.

5. Conclusions.

The expanding integration of modern information technologies into electoral processes has illuminated both the potential for enhanced efficiency, accuracy, and transparency, as well as the variety of risks, ethical dilemmas, and logistical barriers that can impede successful implementation. Policymakers, election administrators, and diverse stakeholders in the private and public sectors have recognized the necessity of adopting frameworks that address cybersecurity and data protection, while embracing innovations such as electronic voting interfaces, biometric verification, and blockchain-based platforms. Findings in this domain suggest that seamless coordination across governmental layers and the promotion of digital literacy among voters represent fundamental prerequisites for fostering inclusive participation, minimizing inequalities, and mitigating threats of intrusion by malicious actors. Ensuring the trustworthiness and reliability of advanced systems requires a delicate balance between technical rigor, user-friendly design, and robust legal measures that protect civil rights and uphold democratic principles, even in the face of accelerating technological change.

Future research avenues may center on refining governance models that harmonize new digital methods with well-established electoral practices, with particular attention paid to reconciling international standards and local requirements. The interplay between emerging technologies and the safeguarding of core democratic values remains a fertile area for empirical investigation, especially regarding the ways in which artificial intelligence, biometrics, and distributed ledger solutions can bolster accountability and voter confidence without undermining privacy or transparency. Continual re-evaluation of hardware and software components, ongoing analysis of real-world pilot programs, and collaborative research efforts to harness cross-border expertise can yield further insights into the dynamic relationship between cutting-edge innovation and electoral integrity.

References:

1. Antonyan, T., Davtyan, S., Kentros, S., Kiayias, A., Michel, L., Nicolaou, N., Russell, A., & Shvartsman, A.A. (2009). State-wide Elections, Optical Scan Voting Systems, and the Pursuit of Integrity. IEEE Transactions on Information Forensics and Security, 4(4), 597–610. Retrieved from https://voter.engr.uconn.edu/reports-publications/state-wide-elections-optical-scan-voting-systems-and-the-pursuit-of-integrity/ [in English].

2. Ibáñez, E., Galdámez, N., Estrebou, C., Pasini, A., Chichizola, F., Rodríguez, I., & Pesado, P. (2015). Biometric Identification in Electronic Voting Systems. *Journal of Computer Science & Technology*, 15(2), 45–56. Retrieved from https://host170.sedici.unlp.edu.ar/server/api/core/bitstreams/f2a69eb0-2bb6-4949-a72a-1638cf0ff026/content [in English].

3. Zheng, Z., Xie, S., Dai, H., Chen, X., & Wang, H. (2017). An Overview of Blockchain Technology: Architecture, Consensus, and Future Trends. *IEEE International Congress on Big Data*, 557–564. Retrieved from https://ieeexplore.ieee.org/document/8029379 [in English].

4. Ferrara, E. (2017). Disinformation and Social Bot Operations in the Run Up to the 2017 French Presidential Election. *Interorganizational Networks & Organizational Behavior eJournal*. Retrieved from: https://www.semanticscholar.org/paper/Disinformation-and-Social-Bot-Operations-in-the-Run-Ferrara/7a6823d16a1dc680c9bdfe03dc4caccbe2e944b6 [in English].

5. Teslim, B. (2024). Integrating Artificial Intelligence with Blockchain Voting. *ResearchGate*. Retrieved from: https://www.researchgate.net/publication/384569869_INTEGRATING_ARTIFICIAL_INTELLIGENCE_WITH_BLOCKCHAIN_VOTING [in English].

6. Baringer, A., Herron, M.C., & Smith, D.A. (2020). Voting by Mail and Ballot Rejection: Lessons from Florida for Elections in the Age of the Coronavirus. *Election Law Journal: Rules, Politics, and Policy*, 19(3), 289–320. Retrieved from https://doi.org/10.1089/elj.2020.0658 [in English].

7. Mildebrath, H. (2024). The Arrival of E-Voting and Campaign Technologies in Europe: Promise, Perils, and Preparedness. *European Parliamentary Research Service*, PE 762.321. Retrieved from https://www.europarl.europa.eu/RegData/etudes/BRIE/2024/762321/EPRS_BRI(2024)762321_EN.pdf [in English].

8. Shahandashti, Siamak F. and Hao, Feng (2016) DRE-ip:A Verifiable E-Voting Scheme without Tallying Authorities. In: ESORICS 2016: Computer Security – ESORICS 2016. European Symposium on Research in Computer Security, 26-30 Sep 2016, GRC, pp. 223-240. Retrieved from: https://eprints.whiterose.ac.uk/117997/ [in English].

9. Kumar, S., & Walia, E. (2011). Analysis of Electronic Voting System in Various Countries. *International Journal on Computer Science and Engineering*, 3(5), 1825–1830. Retrieved from: https://www.

researchgate.net/publication/267235287_ANALYSIS_OF_ELECTRONIC_VOTING_SYSTEM_IN_VARIOUS_COUNTRIES [in English].

10. Ilechukwu, Michelle & Uzoka, Esther & Madubike, Blossom & Ijagbemi, Ayokunle & Chukwu, Chibuzor. (2024). A Comparative Analysis of Cybersecurity Challenges and Solutions in Electronic Voting Systems. Retrieved from: https://www.researchgate.net/publication/387534174_A_Comparative_Analysis_of_Cybersecurity_Challenges_and_Solutions_in_Electronic_Voting_Systems [in English].

Oksana Polotnianko,
PhD in Economics,
Associate Professor of the Department
of Administrative, Financial and Banking Law,
of the PJSC «Higher Educational Institution
«Interregional Academy of Personnel Management»
E-mail: ksenijapolo21@gmail.com
ORCID: 0009-0008-7319-421X