ABUAD Law Journal (ALJ)
(2025). Vol. 13, No. 1, Pages 1-23 https://doi.org/10.53982/alj.2025.1301.01-j
Published by College of Law, Afe Babalola University Law Journal,
College of Law, Afe Babalola University, Km 8.5, Afe Babalola Way,
P.M.B. 5454, Ado Ekiti, Ekiti State, Nigeria ISSN: *2971-7027*
www.abuad.edu.ng, abuadlawjournal@abuad.edu.ng

DATA PROTECTION IN E-VOTING SYSTEMS: THE 2024 NIGERIAN BAR ASSOCIATION'S ELECTIONS IN RETROSPECT

Olumide Babalola*

Abstract

The adoption of e-voting systems in democratic processes necessitates a robust data protection framework to ensure voter privacy, electoral integrity, and compliance with data protection laws. This article critically examines data protection and privacy concerns in e-voting, with a focus on the 2024 Nigerian Bar Association (NBA) elections. Key issues explored include informed consent, confidentiality and integrity threats, cross-border data transfers, data minimization, data retention, and transparency. The article also highlights privacy and data protection challenges specific to NBA e-voting, such as the publication of the voters' list, post-election access to servers and application logs, and the consent of voters to the sharing of election transactions. To address these concerns, the article proposes practical recommendations, including proactive disclosure of voters' personal data usage, a multi-layered approach to combating identity theft and double voting, recognition of votes cast as personal data subject to Data Subject Access Requests (DSARs), enhanced protection of international users' data, and the need for auditable and transparent electoral processes. By advocating for a more accountable and privacy-conscious approach to e-voting, this article contributes to the ongoing discourse on balancing electoral transparency with data protection imperatives.

Keywords: Data protection, e-voting, NBA elections, and privacy.

* PhD Researcher, University of Portsmouth, United Kingdom. olumide@oblp.org.

https://doi.org/10.53982/alj.2025.1301.01-j

1.0 Introduction

Increasingly and as a crucial response to the continued technological incursion into almost all professional and personal activities of Nigerian lawyers, data protection is fast becoming an everyday subject in Nigerian legal circles. As a testimony of this new consciousness, in 2024, the Nigerian Bar Association (NBA) took its proactivity a step further by issuing privacy[1] and cybersecurity guidelines[2] for its members, even though the weight, application and empirical effect of such documents on the members' professional lives is another issue for discussion.

Remarkably, data protection has become a fundamental aspect of modern democratic governance, especially in an age marked by rapid technological progress and growing dependence on digital systems. This emerging phenomenon is particularly crucial in electoral processes, where the security, transparency, and integrity of (personal) data are essential to upholding free and fair elections. In Nigeria, where democracy is still maturing amidst various political, social, and economic challenges, ensuring both data protection and election transparency is of utmost significance. Nigerian legal professionals, fondly revered as 'ministers in the temple of justice', have a distinctive role in preserving the integrity of their own electoral processes, especially in relation to the use, accuracy, collection, management, and protection of personal data. Following the introduction of the Nigeria Data Protection Regulation (NDPR) in 2019, the passing of the Nigeria Data Protection Act in 2023, and increasing public awareness around privacy, it is crucial for legal professionals to actively engage with both the technical and regulatory frameworks that govern privacy and data protection in electing their leaders. This engagement is vital not only to protect their members' privacy rights but also to ensure that NBA elections remain transparent, secure, accurate and credible.

[1] Privacy Guidance for Lawyers in Nigeria issued by the NBA Section on Law Practice < https://nbaslp.org/wp-content/uploads/2024/08/PRIVACY-GUIDANCE-FOR-LAWYERS-IN-NIGERIA-Signed.pdf> accessed on 20 November, 2024.
[2] NBA Cyber Security Guidelines < https://nbaslp.org/wp-content/uploads/2024/09/NIGERIA-BAR-ASSOCIATION-CYBERSECURITY-GUIDELINE.pdf> accessed on 20 November, 2024.

https://doi.org/10.53982/alj.2025.1301.01-j

Undoubtedly, the fallout of the 2024 NBA elections, the arguments and counterarguments arising therefrom informed the topic of this paper which is, for ease of readership, structured into five parts. The first part introduces the purpose and focus of the paper as a real-time academic reaction to the biannual privacy and data protection issues arising from NBA national elections since the introduction of e-voting method in 2016. The second part broaches a general overview of privacy and data protection issues associated with e-voting systems i.e elections conducted on digital platforms. Since NBA elections is the focus of the paper, the third part draws on the theme of the paper by analysing the real-time privacy and data protection arguments for and against the 2024 NBA elections while the fourth part offers recommendations for future NBA elections from a privacy and data protection perspective. The fifth part concludes on the arguments made in the paper.

2.0 E-voting, Privacy and Data Protection

Electronic voting or e-voting[3] has been variously described or referenced as 'remote voting'[4] 'online voting'[5] 'Internet voting'[6] 'i-voting'[7] or 'cyber voting.[8]' Irrespective of the preferred nomenclature, e-voting has been simplistically defined as the election or voting system that relies on 'some electronic technology for their correct functionality,'[9] 'the use of electronic systems and technologies in elections to cast and count votes.'[10] More elaborately, Musa and Aliyu define e-voting as 'systems that allow the eligible voter to cast their votes via a

[3] In this paper, the terms e-voting and electronic voting are used interchangeably.
[4] Filip Zagórski and others, 'Remotegrity: Design and Use of an End-to-End Verifiable Remote Voting System' in Michael Jacobson and others (eds), *Applied Cryptography and Network Security* (Springer 2013).
[5] Mieke Loncke and Jos Dumortier, 'Online Voting: A Legal Perspective' (2004) 18 International Review of Law, Computers & Technology 59.
[6] Joe Mohen and Julia Glidden, 'The Case for Internet Voting' (2001) 44 Commun. ACM 72.
[7] Stuart J Turnbull-Dugarte and Daniel Devine, 'Support for Digitising the Ballot Box: A Systematic Review of *i-Voting* Pilots and a Conjoint Experiment' (2023) 86 Electoral Studies 102679.
[8] Tunbosun Oladoyinbo, 'The Effect of Data Information Security In Digital Voting and Electoral Processes' [2024] IOSR Journal of Computer Engineering 11.
[9] J Paul Gibson and others, 'A Review of E-Voting: The Past, Present and Future' (2016) 71 Annals of Telecommunications 279.
[10] Ghizlane Ikrissi and Tomader Mazri, 'Electronic Voting: Review and Challenges' in Mohamed Ben Ahmed and others (eds), *Innovations in Smart Cities Applications Volume 7* (Springer Nature Switzerland 2024).

https://doi.org/10.53982/alj.2025.1301.01-j

computer normally connected to the internet or intranet from anywhere like home or office.'[11] and 'a system of voting where the voters cast their votes from a remote Internet-enabled computer or another access device.'[12] Despite the international 'political race'[13] surrounding who introduces e-voting first[14], in 2005, Estonia became the first country in the world to introduce the electoral system[15] even though some other source claims Brazil led the way in this regard thus: "In 2000, this country completed the first completely automated elections using DREs (electronic voting terminals)."[16]Generally, e-voting like other activities performed on digital platforms, is faced with some privacy and data protection concerns.

2.1Privacy concern

The right to private and family life guaranteed by the Nigerian Constitution[17] embodies the freedom to vote for the candidate of choice and the autonomy to keep such decisions private, especially in secret balloting. The Court of Appeal in *Nwali v EBSIEC* confirms the nexus between elections and the right to privacy thus:

[11] Mahdi Alhaji Musa and Farouk Muhammad Aliyu, 'Design of Electronic Voting Systems for Reducing Election Process' (2013) 2.
[12] Piret Ehin, 'Internet Voting in Estonia 2005–2019: Evidence from Eleven Elections' (2022) 39 Government Information Quarterly 101718.
[13] CD Mote, 'Report of the National Workshop on Internet Voting: Issues and Research Agenda', *Proceedings of the 2000 annual national conference on Digital government research* (Digital Government Society of North America 2000).
[14] The first implementation of electronic voting was in the 90s. David Yeregui Marcos del Blanco, David Duenas-Cid and Héctor Aláiz Moretón, 'E-Voting System Evaluation Based on the Council of Europe Recommendations: nVotes' in Robert Krimmer and others (eds), *Electronic Voting* (Springer International Publishing 2020).
[15] Ülle Madise and Tarvi Martens, 'E-Voting in Estonia 2005. The First Practice of Country-Wide Binding Internet Voting in the World.' (2006).
[16] Roger Jardí-Cedó and others, 'Study on Poll-Site Voting and Verification Systems' (2012) 31 Computers & Security 989.
[17] The marginal note to section 37 guarantees the right to privacy as the 'right to private and family life'. This specie of privacy is wider and it embodies many if not all aspects of human life. See Maris Burbergs, 'How the Right to Respect for Private and Family Life, Home and Correspondence Became the Nursery in Which New Rights Are Born: Article 8 ECHR' in Eva Brems and Janneke Gerards (eds), *Shaping Rights in the ECHR: The Role of the European Court of Human Rights in Determining the Scope of Human Rights* (Cambridge University Press 2014) <https://www.cambridge.org/core/books/shaping-rights-in-the-echr/how-the-right-to-respect-for-private-and-family-life-home-and-correspondence-became-the-nursery-in-which-new-rights-are-born/8125388A74F5A394D002CE3B0F669B0B> accessed 1 October 2024.

https://doi.org/10.53982/alj.2025.1301.01-j

"… the privacy of his choice of that candidate and the privacy of his voting for that candidate constitute part of his "privacy" as a citizen. The appellant was entitled to the privacy of his decision to vote for a particular candidate, his choice of that candidate and his casting his vote for that candidate. Therefore requiring or compelling him to vote openly in the public watch and knowledge by queuing in front of the poster carrying the portrait of the candidate he has decided to vote for intrudes into, interferes with, and invades the privacy of his said decision, choice and voting, completely removing that privacy, therefore amounting to a clear violation of his fundamental right to the privacy of a citizen guaranteed him and protected by section 37 of the 1999 Constitution."[18]

Voter anonymity is an essential expectation in every given democratic process, ensuring that the electorate expresses their decisions through votes cast freely, without fear of retribution or coercion. While anonymity is relatively easier to achieve in paper-based elections where voters are physically accredited and authenticated at the polling station, but once the ballot is cast into the box, the ballot papers are immediately separated from their identity. This procedural disconnection between the electorate and the votes cast ensures privacy and protects the individual from potential external manipulation or surveillance. In an e-voting system, it is practically impossible to digitally to separate voters from the respective votes. E-voting employs robust systems for authenticating voters while simultaneously ensuring that the actual vote cast remains anonymous all through the process. If this balance is not achieved, the privacy of voters can be compromised, undermining trust in the election process and potentially leading to voter manipulation or intimidation.

2.2 Data protection concern

For data protection, while the 'concerns' are in the mould of obligations[19] and duties for data controllers and processors regulating or operating the electoral platforms on one hand, they

[18] Hon. Peter Nwali v. Ebonyi State Independent Electoral Commission (2014) LPELR–23682(CA).
[19] Like other controllers, the electoral body must comply with the principles of data processing including ensuring the integrity and confidentiality of the voting platforms; fulfil other obligations like providing access to data subjects' rights, appointment of data protection officers, data protection impact assessment, conduct and file compliance audit where necessary etc. For further reading on obligations, see Olumide Babalola and Paolo Balboni, *Annotated Nigeria Data Protection Act 2023* (Noetico Repertum, Lagos).

https://doi.org/10.53982/alj.2025.1301.01-j

represent rights and entitlements of the users/electorate whose personal data are processed by the platforms and their handlers.[20]

2.2.1 Obtaining informed consent

Consent is one of the legal bases for the processing of personal data. Where data is processed based on consent, the subjects of such processing must understand the intricacies of the activities to which they voluntarily and explicitly agree. In electronic voting systems, seeking and obtaining informed and explicit consent is not only a legal requirement but also crucial for maintaining the integrity of the democratic process.[21]

Inherently, consent is tricky, but it becomes even more problematic in e-voting systems.[22] For consent to be valid, voters must be fully informed of the use their personal data would be put to and then given the opportunity to agree or disagree – this latitude underscores the complexity of consent in digital environments, i.e the e-voting platforms. Moreover, consent in the context of e-voting must be freely given in an environment where the voters are aware of their choices. Any coercion or undue influence to consent to the process could potentially undermine the fairness of the election. Statutorily, voters, like other data subjects, must also have the option to withdraw consent, although, in the case of electronic voting, this can be problematic or procedurally impracticable, once a vote is cast, as it is practically irreversible to ensure election integrity. Ultimately, the voting system must balance the need for free, informed consent within the technical constraints of vote finality.

2.2.2 Confidentiality and integrity threats

A cardinal twin principle of data protection is confidentiality and integrity.[23] For e-voting, the principle mandates the electoral umpire to ensure the protection of voters' personal data by

[20] Adrià Rodríguez-Pérez, 'My Vote, My (Personal) Data: Remote Electronic Voting and the General Data Protection Regulation', *Electronic Voting: 5th International Joint Conference, E-Vote-ID 2020, Bregenz, Austria, October 6–9, 2020, Proceedings* (Springer-Verlag 2020) <https://doi.org/10.1007/978-3-030-60347-2_11> accessed 1 October 2024.
[21] Wouter Bokslag and Manon de Vries, 'Evaluating E-Voting: Theory and Practice' (arXiv, 8 February 2016) <http://arxiv.org/abs/1602.02509> accessed 1 October 2024.
[22] Chris Jay Hoofnagle, 'Designing for Consent' (2018) 7 Journal of European Consumer and Market Law 162.
[23] For further reading on confidentiality and integrity, see Olumide Babalola, Privacy and Data Protection Law in Nigeria (Noetico Repertum, 2021).

https://doi.org/10.53982/alj.2025.1301.01-j

ensuring that voter identities and their choices remain private and secure from unauthorised access, manipulation, alteration or destruction. A breach of confidentiality and integrity may result in unauthorized access or disclosure of voter's personal data or voting preferences, potentially leading to voter coercion, manipulation, or loss of trust in the electoral process. Integrity in the context of e-voting, on the other hand, refers to the reliability of the voting platform warehousing the electorate's personal data. The principle demands that the votes cast are accurately captured, recorded, transmitted, and counted correctly, without alterations or manipulations. In e-voting systems, the breach of data integrity invariably leads to manipulation of election results, casting doubt on the legitimacy of the outcomes. Since the principle of confidentiality and integrity forms the spine of safe and trustworthy e-voting systems, they are potentially under attack by cybercriminal activities, hence the necessity for robust security mechanisms.

2.2.3 Cross-border data transfers

By their inherent nature, e-voting systems are digital, hence they are hosted on the Internet and often rely on cloud storage services, data processing centres, and other IT infrastructures that are usually spread across multiple geographic locations.

As the technology used for these electoral processes are sophisticated and not yet universally available, many countries do not have the capacity to locally develop and host e-voting systems instead they resort to global technology providers for partial support or holistic delivery. Invariably, these providers routinely store or process voter data in data centers located in other countries, particularly in large cloud hubs like the United States, Europe, or Asia. This decentralization of infrastructure introduces the challenge of cross-border data transfers, where voter data flows across national boundaries for storage, processing, or backup. While this globalized infrastructure can increase the efficiency and scalability of e-voting systems, it also introduces legal, privacy, and security risks. These cross-border data flows raise the issues of data sovereignty, adequacy of level of protection, jurisdictional complexities, third-party vendor compliance and associated risks, data security threats, and foreign interference. etc.

https://doi.org/10.53982/alj.2025.1301.01-j

2.2.4 Data minimization

Data minimization is a precautionary principle of data protection that stems from the risks of big data. The principle essentially demands that only the necessary personal data needed to fulfill the purpose of processing be collected and processed. In the context of e-voting, adherence to this principle limits the quantity and categories of personal data required and/or collected to what is strictly required for the voting process, such as verifying voter eligibility and preventing fraud. Electoral umpires deploying e-voting platforms may be legitimately swayed to collect a wide range of personal information, including demographic data, device identifiers, and voting patterns, to improve functionality or ensure security. However, collecting unnecessary personal data increases the risk of privacy breaches.

2.2.5 Data retention

Storage limitation is a principle of data processing requiring personal data to be stored within a certain time limit – as long as it is necessary for the initial purpose of collection or otherwise processing. Data retention refers to the period during which personal data is stored and the processes by which it is deleted or anonymized after it is no longer needed. In e-voting, the length of time voter data is retained can have significant privacy implications i.e increased vulnerability to data breaches. On one hand, retaining data may be necessary to verify the legitimacy of election results or to investigate potential fraud. On the other hand, prolonged retention increases the risk of data breaches, compromise and misuse. E-voting systems often store personal information (such as voter IDs and login details) to verify election results or for audit purposes. Retaining this data for extended periods creates vulnerabilities, especially in the event of a cyberattack or unauthorized access. While it is important to ensure the integrity of the election, retaining detailed voting records could expose sensitive information, such as how individuals voted, undermining voter privacy.

2.2.6 Transparency

In the context of e-voting, the principle of transparency mandates the electoral umpire manning the voting platforms to provide lucid and comprehensive information to the users of

https://doi.org/10.53982/alj.2025.1301.01-j

the platforms especially details of the entire life cycle of personal data vis a vis its processing. Various categories of personal data are processed by the e-voting systems, hence the (joint)controllers of the e-voting systems ought to proactively provide information to the users on the functionality of the platforms especially as it relates to the use, purpose(s), transmission, security and retention of the personal data collected. E-voting systems are complex and not easily understandable by the general public or even election administrators. This creates a "black box"[24] problem where voters, candidates and observers cannot easily see how their votes are processed.

If the public and election stakeholders cannot comprehend the technology or how it works, they are less likely to trust the results. This lack of transparency can fuel scepticism and conspiracy theories. Transparency is breached when the vulnerabilities of voting platforms are downplayed or not fully disclosed to the public. When security vulnerabilities are kept secret or poorly communicated, voters cannot be sure that their votes are safe from manipulation. This fosters mistrust in the system.

3.0 Privacy and data protection challenges in NBA e-voting

The NBA adopted e-voting for its general elections for the first time in 2016 under the leadership of Augustine Alegeh, SAN. The outcome of the election was reportedly challenged because many eligible lawyers were allegedly disenfranchised owing to some functional irregularities. Since 2016 till date, the successive outcomes of the electronic elections conducted by the NBA have been challenged on similar grounds including the repeated requests for post-election audit exercise.

The outcome of the 2024 NBA elections added a twist. The election was conducted on Election Buddy Inc. – a Canadian platform that describes itself as "online voting software ensures your electronic voting is accurate and secure." After the elections and declaration of results, the 1st and 2nd runners-up (the complainants) called for an audit of the elections on the

[24] Matt Bishop and others, 'E-Voting and Forensics: Prying Open the Black Box' Proceedings of the 2009 USENIX/ACCURATE Electronic Voting Technology Workshop (2009).

https://doi.org/10.53982/alj.2025.1301.01-j

grounds of double voting, identity theft, and manipulation of votes, but that was not the twist. In a 28-paged robust response to the letters written by the complainant, NBA's electoral body – the Electoral Committee of the Nigerian Bar Association (ECNBA) or (the Umpire), declined the request for an audit with reasons – chief of which are the enforcement of privacy and data protection rights of voters and other non-NBA users of the e-voting platform. In this part, I briefly analyse some of the issues bordering on privacy and data protection as decipherable from ECNBA's letter dated 25th July 2024 titled 'Re: Request for Access to Critical Information Regarding The 2024 NBA National Elections.'[25]

3.1. Publication of voters list

The umpire declined a publication of the voters register/list because, according to their letter relying on the Nigeria Data Protection Act 2023 (NDPA), they cannot lawfully "publish, particularly without the consent of the data subject."[26] While it is undeniable that consent is a lawful basis to process personal data, it is not the only ground for such processing under the NDPA.[27] In this context, personal data can be processed on the grounds of NBA and the complainants' joint or several legitimate interests[28] in the integrity, freeness and fairness of the elections and also in the public interest[29] in the rule of law, orderliness and uprightness of the Nigerian bar – an association whose members populate the third arm of government. More so, the publication of the voters' register is a legal requirement of a valid electoral process imposing a legal obligation on the umpire which itself is a ground for processing such data under the NDPA. Hence, where other lawful grounds exist, consent is no longer required for the processing of personal data – the voters' details in this context.

---

[25] NBA Communication Officer, 'RE: REQUEST FOR ACCESS TO CRITICAL INFORMATION REGARDING THE 2024 NBA NATIONAL ELECTIONS' (*NBA BLOG*, 27 July 2024) <https://blog.nigerianbar.org.ng/2024/07/27/re-request-for-access-to-critical-information-regarding-the-2024-nba-national-elections/> accessed 8 October 2024.
[26] Paragraph 5, page 3 of the ECNBA's letter dated 25th July 2024.
[27] Section 25 of the NDPA provides six grounds or bases for the lawful processing of personal data to wit: consent; entry into or performance of contract; legal obligation; legitimate interest; public interest and vital interest. For further reading, see Olumide Babalola and Paolo Balboni, 'Annotated Nigeria Data Protection Act, 2023' (Noetico Repertum, 2023.
[28] NDPA, section 25(1)(b)(v).
[29] NDPA, section 25(1)(b)(iv).

https://doi.org/10.53982/alj.2025.1301.01-j

In their response, the umpire references the GDPR – a European enactment, hence resort may be had to some foreign resources for guidance on this issue. In 2022, rather than prohibit access to voter lists on the grounds of data protection, the Council of Europe acknowledges its legality and gives some policy advisory/directives on its handling and management thus:

"Where political campaign organisations legally acquire the official voters list from the election regulatory body to assist their campaigns, the law should stipulate who is entitled to access these data, and for what purposes, limited to what is necessary for engaging with the electorate with clear prohibitions and appropriate sanctions for using the data for any other purposes….Unless specifically approved by law, contact data from the official voters' list should not be combined with other sources of personal data to create profiles of voters for micro-targeting purposes."[30]

On the same wavelength, the UK Information Commissioner's Office confirms that: "Registered political parties, candidates and campaigners are entitled to receive copies of the full electoral register which includes eligible voters' names and addresses."[31] Interestingly, Election Buddy, is based in Canada as acknowledged by the umpire, where electoral candidates are legally given access to the voter lists under the authority of the Canada Elections Act.[32] Even in Europe, the distribution of voter lists to candidates is allowed subject to restrictions on its use. Ultimately, in any case, lawyers' names, years of call and SCN numbers are publicly available on https://www.nigerianbar.org.ng/find-a-lawyer hence they cannot enjoy the suggested expectation of privacy within the context of NBA elections as proposed by the umpire.[33]

[30] Council of Europe, Guidelines on the Protection of Individuals With Regard to the Processing of Personal Data by and for Political Campaigns' (2022).
[31] Information Commissioner's Office, 'Use of the Electoral Register' (20 June 2024) <https://ico.org.uk/for-organisations/direct-marketing-and-privacy-and-electronic-communications/guidance-for-the-use-of-personal-data-in-political-campaigning-1/use-of-the-electoral-register/> accessed 4 October 2024.
[32] Colin J Bennett, 'Voter Databases, Micro-Targeting, and Data Protection Law: Can Political Parties Campaign in Europe as They Do in North America?' (2016) 6 International Data Privacy Law 261.
[33] This is not in any way suggesting that publicly available personal data do no enjoy expectation of privacy. See Brandon T Crowther, '(Un)Reasonable Expectation of Digital Privacy Comment' (2012) 2012 Brigham Young University Law Review 343.

https://doi.org/10.53982/alj.2025.1301.01-j

3.2. Access to servers and application logs

The umpire denied the complainants 'access to server and application log files used during the election period' because it is contrary to the GDPR, NDPA/NDPR and 'Election Buddy Inc provides its services to tons of organization and nations globally using the same servers and application files, hence giving one user access clearly compromises the entire credibility of their servers carrying other users' data.'[34] Curiously, the umpire's letter does not contain any specific provision of the referenced laws that would be violated if the complainants are granted access to the servers and application logs but the starting point is a confirmation of the nature of personal data borne by the servers and application logs on one hand and the use of such information on the other hand. Are they personal data, anonymised or pseudonymised data?.

From a data protection perspective, this is part of the information that should have been proactively provided to the users of Election Buddy's e-voting systems and the members of the NBA before personal data are migrated to the platforms for electioneering purposes. Under the GDPR[35] and NDPA[36] alike, at the point of collection of personal data, data controllers (Election Buddy[37] and ECNBA) are duty-bound to provide certain information about the nature of the data collected, its use and entire governance.

While the GDPR does not expressly state how this obligation is to be fulfilled, its Nigerian counterpart specifically provides for the use of a privacy policy to convey this set of information.[38] On Election Buddy's website, their privacy policy interestingly states that they use personal data for "Investigating and protecting against fraudulent, harmful, unauthorized,

[34] See page 14 of ECNBA's letter.
[35] GDPR, art. 13(1) and (2).
[36] NDPA, section 27.
[37] In their privacy policy accessible at: https://electionbuddy.com/privacy-policy, Election Buddy admits that there are instances where they act as controllers with respect to voters' information.
[38] NDPA, section 27(3) expressly provides that: "The information referred to in subsection (1) shall be contained in a privacy policy and expressed in clear, concise, transparent, intelligible, and easily accessible format, taking into consideration the class of data subjects targeted by the data processing."

https://doi.org/10.53982/alj.2025.1301.01-j

or illegal activity."[39] The complainants have alleged identity theft, double voting, electoral manipulation etc. All these point towards illegality – and they have called for an investigation in the mould of an audit, hence the ECNBA and Election Buddy have valid and lawful grounds to grant access to servers and application logs to unravel the alleged illegalities (if any).

Situating this within the relevant provisions of the GDPR, data protection rights and controllers' obligations are restricted for the investigation and detection of crime[40] and 'the prevention, investigation, detection and prosecution of breaches of ethics for regulated professions.'[41] The legal profession is a highly regulated one, hence any allegation of manipulation of its general elections is worth investigating. Under the NDPA, certain data protection rules and obligations are not applicable to the processing of data necessary for the establishment of legal claims whether in court or regulated out-of-court settlements.[42]

Legitimate interest is one of the lawful grounds on which controllers can rely to process personal data. The lawful basis allows organizations to process personal data without needing explicit consent from the data subjects where the former has a compelling reason or "legitimate interest" to do so, provided that it does not adversely prejudice the data subjects' rights and freedoms. Legitimate interest is not defined under the NDPR, however the GDPR gives a little bit of clarity on the concept. This legal basis concerns the processing of data for the purpose of interests legitimately pursued a 'controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child.'[43]

Ferretti broadly defines or describes legitimate interest in the following terms:

---

[39] The Privacy Policy is found at < https://electionbuddy.com/privacy-policy/?_gl=1*1jdxk5a*_up*MQ..*_ga*MjEwMTg2MzAwMS4xNzI3OTczNTI4*_ga_FKSSZ1SH00*MTcyODA0MDU5Mi4yLjEuMTcyODA0MDU5Mi42MC4wLjE2MDc2NzYwNDg.> accessed on 4 October 2024.
[40] GDPR, article 23(1)(d).
[41] GDPR, article 23(1)(g).
[42] NDPA, section 3(2)(d).
[43] GDPR, art. 6(1)(f); for further reading of the concept of legitimate interest, see Dolenc Dubravka, 'Legitimate Interest as Legal Grounds for Processing Personal Data' (2020) 49 Bankarstvo 145.

https://doi.org/10.53982/alj.2025.1301.01-j

"The legitimate interest of data controllers or that of third parties is known as the "balance of interest" clause…Therefore, the legitimate interest clause is considered the criterion upon which the majority of personal data processing takes place, at times the default position, especially for commercial transactions. Under this condition, the processing must be necessary for the purpose, which must be a legitimate interest of the controller or a third party to whom the data is disclosed, provided that such legitimate interests do not impinge upon the fundamental rights and freedoms of individuals.[44]

To rely on legitimate interest, the three-part test ought to be applied by asking the salient questions: (a) Purpose test – is there a legitimate interest behind the processing? (b) Necessity test – is the processing necessary for that purpose? and (c) Balancing test – is the legitimate interest overridden by the individual's interests, rights or freedoms.?[45]

In the context of the impugned elections, the complainants have only demanded access to the server and application logs pertaining to NBA elections. Considering the weighty allegations, both ECNBA, Election Buddy and the complainants (as third parties)[46] have legitimate interests in preventing electoral fraud by establishing credibility and accuracy of the elections results by granting access to the information required for this proof – the purpose. Secondly, this is necessary to build voter trust, ensure transparency in the succession procedure of the association and to prevent the subversion of Nigerian lawyers choice of their leaders – the necessity. In balancing the competing interests, the duty of the Association towards holding credible elections and entrenching the rule of law overrides an individual's right to privacy on one hand and it is the expectation and hope of every member of the NBA that the election results reflect the true wishes of the electorate, hence they are not averse to election audits confirming accuracy of such results.

---

[44] Federico Ferretti, 'Data Protection and the Legitimate Interest of Data Controllers: Much Ado about Nothing or the Winter of Rights?' (2014) 51 Common Market Law Review <https://kluwerlawonline.com/api/Product/CitationPDFURL?file=Journals\COLA\COLA2014063.pdf> accessed 19 June 2023.
[45] Paolo Balboni and others, 'Legitimate Interest of the Data Controller New Data Protection Paradigm: Legitimacy Grounded on Appropriate Protection' (2013) 3 International Data Privacy Law 244.
[46] Under both GDPR and NDPR, controllers can also process personal for the purpose of legitimate interest pursued by third parties. See GDPR, article 6(1)(f) and NDPA, section 25(1)(v).

https://doi.org/10.53982/alj.2025.1301.01-j

3.3. Consent of voters to the sharing of election transactions

In response to allegations of identity theft leading to double voting, the umpire requests the complainants to seek and obtain the consent of their supporters that alleged identity theft so the umpire 'can also unveil their said privately cast votes for transparency in our investigation.' Again, while answering a request for voting transactions, the umpire responds that the provision of such information is a violation of voter privacy except the complainants provide 'consent letters of the voters' concerned. These answers have repeatedly elevated 'consent' above all other legal bases and statutorily allowed derogations. From a privacy or data protection perspective, the umpire is not required to rely on voters' consent before processing their data to defend the integrity and accuracy of the elections it conducted. This much is confirmed in Election Buddy's privacy policy thus: "For operational and legal purposes, we may share your personal information with certain entities as outlined below:… Authorities and others: Law enforcement, government authorities, and private parties, as we believe in good faith to be necessary or appropriate for the compliance and protection purposes described above." As argued earlier, relying on legitimate interest and public interest, the ECNBA can validly disclose the voting transactions to the complainants without voters' consent as contemplated by the relevant data protection legislation.

4.0 The Way forward: Recommendations

The 2024 e-elections have come and gone but like their predecessors, vestiges of allegations of electoral malpractices continue to linger, especially in the light of the documented pushbacks from the electoral umpire. For future elections i.e the ones conducted on digital platforms, the NBA ought to sincerely consider the following suggestions:

4.1 Proactive information on voters' personal data

https://doi.org/10.53982/alj.2025.1301.01-j

One of the data subjects' rights guaranteed by the NDPA is the right to be informed on the processing of personal data.[47] Since the ECNBA acknowledges that some "critical" personal information are fed to the e-voting platforms towards the elections, the NBA as controllers ought to proactively provide full, lucid, comprehensive and understandable information to the voters on the entire life cycle of their personal data for the electoral process i.e from collection to migration to the e-voting platforms and post-election use (if any). For clarity, the ECNBA must provide information on the data flow of the entire electoral cycle. For example, when you register to vote, where is the data recorded, after voting where are the votes digital receipts stored? etc. The NDPA expressly requires information on recipients of personal data, in this case, the e-voting platform, the period of retention, the sub-recipients from the e-voting platform and most importantly the rights of users.

4.2 Adopt a multi-level approach towards curbing Identity theft and double-voting

It is rather too simplistic for the ECNBA to conclude that inaccurate voter records is not its "issue." The duty to ensure the accuracy and update of personal data is a shared responsibility between the controller (ECNBA) in the context of elections and the voters. Interestingly, the NDPA puts this responsibility squarely at the NBA/ECNBA's doorstep to ensure the accuracy of personal data and keep it up to date.[48] The NBA does not have to wait till the election period before cleaning up the members' personal data since the obligation to ensure accuracy and updated records is a recurrent duty. The NBA has an existing database of members which has members' emails and telephone numbers, which can be used as a benchmark for the voters list to flag inconsistencies ahead of time.

4.3 Votes cast are the personal data of contestants accessible by DSAR

[47] NDPA, section 27.
[48] NDPA, section 24(1)(e).

https://doi.org/10.53982/alj.2025.1301.01-j

The complainants' request for the election transaction is to compare the number of votes cast in their favour with the results recorded for them in order to establish their allegations of manipulations and other electoral malpractices. In elections, votes cast in favour of a candidate represent the electorates' endorsement and expression of their preference for the candidate concerned. These votes double as electorates' and contestants' personal data. Both the GDPR and NDPA define personal data identically as information relating to an individual directly or indirectly identifiable.[49] From whatever prism one looks at it, election results, e-ballots and voting transactions relate to the candidates since they give clear information on the votes allegedly won and lost, hence they constitute the candidates' personal data within the context of election outcomes. Admittedly, there are no direct authorities supporting this novel argument however, election computation and results could be likened to examination marking and grading on which a court decision exists. In *Peter Nowak v Data Protection Commissioner,*[50]a trainee accountant who failed an open book professional examination made a data subject access request for all his personal data held by the examination body. The body obliged the request but refused to share his examination scripts on the grounds that it did not contain personal data but when the matter went to the Court of Justice of the European Union (CJEU), the court found that:

"Contrary to what the Data Protection Commissioner appears to argue, it is of no relevance, in that context, whether the examiner can or cannot identify the candidate at the time when he/she is correcting and marking the examination script. It is also undisputed that, in the event that the examiner does not know the identity of the candidate when he/she is marking the answers submitted by that candidate in an examination, the body that set the examination, in this case, the CAI, does, however, have available to it the information needed to enable it easily and infallibly to identify that candidate through his identification number, placed on the examination script or its cover sheet, and thereby to ascribe the answers to that candidate. First, the content of those answers reflects the extent of the candidate's knowledge and competence in a given field and, in some cases, his intellect, thought processes, and judgment. In the case of a handwritten script, the answers contain, in addition, information as

[49] See article 4(1) GDPR and section 65 of the NDPA.
[50] C-434/16 delivered by the Court of Justice of the European Union on the 20th day of December 2017.

https://doi.org/10.53982/alj.2025.1301.01-j

to his handwriting. Second, the purpose of collecting those answers is to evaluate the candidate's professional abilities and his suitability to practice the profession concerned. Last, the use of that information, one consequence of that use being the candidate's success or failure at the examination concerned, is liable to have an effect on his or her rights and interests, in that it may determine or influence, for example, the chance of entering the profession aspired to or of obtaining the post sought."

Relating the finding above to the complainants' request, the election transactions reflect the performances of the candidates in the election, and their suitability as decided by the electorate with consequences on their rights and interests in the leadership of the NBA. The totality of these considerations leads to an aggregate of election transactions as information relating either directly or indirectly to the candidates (the complainants) – the falls under the expansive definition of personal data. This position finds support in the European decision of *Patrick Breyer v Germany*[51] where the court acknowledges that information relating to a data subject may not contain all the identifiers, but an aggregate of other information makes such information qualify as personal data.[52] In the complainants' case, any vote cast in their favour directly relates to them while the other votes arguably indirectly relate to them as well. In any case, all the votes form part of the election transactions and they holistically relate to the complainants, in terms of the electorate's endorsement or disapproval. Having settled the nature of votes as contestants' personal data as well, then such transactions are accessible by exercising data subjects' access request. As part of the rights guaranteed by the NDPA, data subjects can request copies of their personal data in a controller's possession.[53] Relying on this provision, the complainants are within their rights to demand copies of the election transactions and the ECNBA is duty-bound under the NDPA to oblige without incurring any liability.

4.4 Masking/protecting other international users' data

[51] Application no. 50001/12: Patrick Breyer v Germany delivered by the European Court of Human Rights on the 20th day of January 2020.
[52] W Gregory Voss and Kimberly A Houser, 'Personal Data and the GDPR: Providing a Competitive Advantage for U.S. Companies' (2019) 56 American Business Law Journal 287.
[53] NDPA, section 34(1)(a) –(b).

https://doi.org/10.53982/alj.2025.1301.01-j

Part of the ECNBA's reluctance to grant access is the apprehension of exposing other international service users' personal data in the process. First, if this excuse was given by Election Buddy, then it is an indictment on them since elections on their platform are meant to be uniquely protected and encrypted. Application servers are not like physical rooms where personal data can be carelessly displayed. They are the software link between users' browsers and the host's database and internal legacy systems. They facilitate 'online interactions by dynamically generating catalogs, accepting and processing orders, updating customer or employee data, and retrieving and presenting other requested information.'[54] So access to the servers used for a particular election transaction does not necessarily expose data used in other election transactions not associated with the one concerned.

Secondly, the kind of data displayed on servers are codes which may not necessarily be personal data if they do not directly or indirectly identify users. Third, to circumvent privacy breaches, other users' personal data can be masked or redacted while granting access to the relevant election transaction. In *Michael J. Durant v Financial Services Authority*[55] a bank customer made requests to his bank seeking disclosure of personal data held by it, both electronically and in manual files. The FSA provided him with some copies of documents relating to him but some of the documents were redacted so as not to disclose the names of others but he wanted more files. When the matter got to the English Court of Appeal, the court notes the need for redaction and when consent will be dispensed with as follows: "It is important to note that section 7(4) leaves the data controller with a choice of whether to seek consent; it does not oblige him to do so before deciding whether to disclose the personal data sought or, by redaction, to disclose only part of it."[56]

Under relevant data protection laws, access can validly be granted to servers where a legal basis exists. In this case, the controllers can validly rely on legal obligation, legitimate interest or public interest to grant access for elections audit thereby dispensing with the

[54] Jesse Feiler, *Application Servers: Powering the Web-Based Enterprise* (Elsevier Science & Technology Books 2000).
[55] Michael John Durant v Financial Services Authority [2003] EWCA Civ 1746. Delivered in 2003 by the UK Court of Appeal.
[56] Ibid.

https://doi.org/10.53982/alj.2025.1301.01-j

requirement for voters' consent.[57] For the Nigerian lawyers, the bases of legal obligation and legitimate interest are grounded in the NBA's Constitutional provision of electoral transparency thus:

"The ECNBA shall display openness and transparency in all its activities and in its relationship with all members, particularly the candidates for the election, and shall ensure the following: …Establish a system that allows interested parties to access, in a timely manner, all critical information, documents, and databases used in an election process, or used in the normal operation of the election administration."[58]

This provision was inserted in the Constitution to protect the rights of the complainants as a derogation from voters privacy recognised under section 45 of the Nigerian Constitution which subjugates certain fundamental rights at the expense of laws made for public order and protecting others' rights. In interpreting how section 45 of the Nigerian Constitution relates to rules made by associations like the NBA in this case, the Supreme Court in *Mbanefo v Molokwu*[59] ruled that: "Section 45 provides that nothing in Section 40 of the 1999 Constitution shall invalidate any law that is reasonably justifiable in a democratic society, in the interest of defence, public safety, public Order, public morality or public health etc … This may be an appropriate stage to state loud and clear that the interpretation of "law" as prescribed under section 45 of the Constitution cannot be restricted only to the statutes of parliament. It would include rules and regulations guiding communities in maintenance of peace and tranquillity. This will minimize those anti-social behaviours which spill over to the outside specific boundaries creating a breakdown of law and order thereby overloading the security agencies beyond their tour of duty."[60] In this case, section 45 trumps any privacy arguments that may be used to shield electoral inaccuracies and malpractices in the circumstance.

[57] See the case of Bernh Larsen Holding v. Norway (Case 24117/08) delivered by the European Court of Human Rights (ECtHR) in 2003 where access to servers was granted even where it exposed others' personal data.
[58] The Constitution of the Nigerian Bar Association, 2021, second schedule, Part 2, paragraph 8(c) at page 40.
[59] Mbanefo v Molokwu (2014) LPELR-22257(SC).
[60] Ibid.

https://doi.org/10.53982/alj.2025.1301.01-j

4.5 Choice of service provider and access to terms of engagement

As part of the recruitment process for an e-voting service provider, the preferred vendor's privacy practices must be reviewed to ensure compliance with Nigerian data protection legislation. The service level agreement must be accessible to contestants to pre-inform them of their data subjects' rights especially access to election transactions, and the rectification of inaccurate or misleading election records/results which are all guaranteed by the Nigeria Data Protection Act 2023.[61]

4.6 Opening the black box and auditable elections

Transparency is vital to fostering trust in any electoral process. The adoption of e-voting in the NBA elections must turn out a better option than the erstwhile paper-based system in terms of transparency, security and accountability. The crux of the complainants' post-election umbrage is the umpire's refusal to allow them to audit the elections through the voting platforms. The ECNBA's letter discloses that the conduct of what appears to be a self-audit which falls short of the complainants' request, and what is more, Election Buddy favours election audits thus:

"It doesn't matter if your organization is a small homeowners association electing officers in an intimate election or if you're tallying votes for a large-scale industry association—you want to be sure the process is uncorrupted and fair. If the integrity of your elections comes into question, this is when election audits take place. Election audits occur when there is suspicion or evidence of discrepancies or inaccuracies in the voting process. These audits aren't just reserved for elections involving the government. They can be applied to industries and organizations. Auditing your election can instil voter confidence and ensure your organization follows all proper procedures… While online voting is generally secure and accurate, audits are just as necessary for digital voting as physical ballot submissions. Both methods can work together to ensure accurate results... Currently, manually reviewing and

[61] See section 34 of the NDPA.

https://doi.org/10.53982/alj.2025.1301.01-j

recounting through an objective third party is the best way to audit elections and ensure an accurate vote count."[62]

Accuracy is a cardinal principle of data protection. The NDPA requires personal data (election results in this case) to be accurate, not misleading and in the event of inaccuracy, it must be corrected and updated to reflect current reality.[63] This accuracy can only be ensured after a proper audit exercise has been conducted on the election. On the essentiality of audits, it has been advised that: "Appropriate audits can be used to enable trust in the accuracy of election outcomes even if the integrity of software, hardware, personnel, or other aspects of the system on which an election is run were to be questioned."[64]

In similar terms, Mello-Stark and Lamagna rightly argue that: "In order for an election system to be trusted, it needs to be verifiable. Methods must exist to check that the votes are cast as intended by the voters. There must be strong evidence that the machines function as they are supposed to function. Voters should feel confident that the election is conducted fairly and accurately."[65] Driving further their advocacy for e-voting audits, the authors suggest, the following types of audits: receipts audits, tally audits and system self-checking audits using various methods.[66] In a much recent research paper, Khlaponin et al confirmed the necessity and option of 'building a system of secret Internet voting, in which a full-fledged audit is available to all voters and their proxies. A full-fledged audit should be understood as such an audit, in which everything that may
be in doubt is checked.'[67]

---

[62] electionbuddyadmin, 'Do Elections Get Audited?' (*ElectionBuddy*, 24 May 2023) <https://electionbuddy.com/blog/2023/05/24/do-elections-get-audited/> accessed 5 October 2024.
[63] NDPA, section 24(1)(e) and 34(1)(c).
[64] National Academies of Sciences, Engineering, and Medicine *'Securing the Vote: Protecting American Democracy' at NAP.Edu* <https://nap.nationalacademies.org/read/25120/chapter/7> accessed 5 October 2024.
[65] Suzanne Mello-Stark and Edmund A Lamagna, 'The Need for Audit-Capable E-Voting Systems', *2017 31st International Conference on Advanced Information Networking and Applications Workshops (WAINA)* (2017) <https://ieeexplore.ieee.org/document/7929736/?arnumber=7929736> accessed 8 October 2024.
[66] ibid.
[67] Yuriy Khlaponin, Volodymyr Vyshniakov and Oleg Komarnytskyi, 'Proof of the Possibility for a Public Audit of a Secret Internet Voting System' (19 January 2023) <https://papers.ssrn.com/abstract=4330966> accessed 8 October 2024.

https://doi.org/10.53982/alj.2025.1301.01-j

From the foregoing intervention, conducting audits on e-voting systems is not only necessary but essential for the integrity, transparency, and trustworthiness of electoral processes. Audits serve as a crucial mechanism to verify the accuracy of votes, ensure compliance with legal and regulatory standards, and identify any irregularities or security risks. Moreover, the credibility of NBA elections hinges on its members' confidence in the electoral process. Regular audits can help to reassure stakeholders—including voters, political parties, and regulatory bodies—that the e-voting system operates as intended, free from manipulation or technical failures. By systematically assessing the security, functionality, and overall accuracy of these systems, audits can enhance accountability and contribute to a more robust democratic process. In summary, the implementation of comprehensive audits is vital not only for safeguarding electoral integrity but also for fostering NBA members' trust in the democratic process.

5.0 Conclusion

The 2024 Nigerian Bar Association's elections together with its post-election controversies provide a valuable case study for the practical and academic assessment of the intersection of data protection and e-voting systems. As technology continues to transform electoral processes across the World, the importance of safeguarding personal data, ensuring voter privacy and ascertaining the accuracy and credibility of voting platforms has never been more pronounced. This retrospective analysis highlights the pre- and post election intrigues, emphasizing the need for robust data protection measures including the respect for voters/candidates' rights. Effective data protection in e-voting systems is not merely a regulatory requirement but a cornerstone of public trust in the electoral process. The lessons learned from the 2024 elections underscore the necessity for continuous improvement in the security and transparency of e-voting systems. Moving forward, it is imperative that future elections incorporate best practices in data protection, including regular audits, stakeholder engagement, and adherence to established standards. As we advance into an increasingly digital future, the commitment to protecting voter data will play a pivotal role in fostering confidence and ensuring that bar elections remain fair, transparent, and secure.

BABALOLA

Data Protection in E-Voting Systems: The 2024 Nigerian Bar Association's Elections in Retrospect

https://doi.org/10.53982/alj.2025.1301.01-j