Legitimasi
Jurnal Hukum Pidana dan Politik Hukum
Vol. 15, No. 1, January-June 2026

ISSN:
2088-8813 (Print)
2579-5104 (Online)

The Urgency of Reformulating Election Criminal on the Use of Someone Else's Name Without Permission in Indonesia's Electoral Digitization System

Rofiqoh Pebrianti
Universitas Jambi, Indonesia

Usman
Universitas Jambi, Indonesia

Arfa'i
Universitas Jambi, Indonesia
Corresponding Author: razyummi1506@gmail.com

Submitted: November 24, 2025 Accepted: May 21, 2026 Published: June 29, 2026

Abstract: *This study highlights the rampant misuse of personal data without permission in the implementation of elections, particularly at the stage of political party registration and verification through the Political Party Information System (SIPOL). This condition shows the weak legal protection of citizens' privacy rights, considering that Law Number 7 of 2017 concerning Elections does not explicitly regulate sanctions for such violations. The research uses a normative juridical method with a legislative, conceptual, and case approach to examine regulations, criminal law doctrines, and electoral practices. The results of the study show that there are no comprehensive norms regulating the use of personal data without permission in the context of elections, which creates legal uncertainty and weakens the protection of citizens' rights. Therefore, it is necessary to reformulate election laws by integrating personal data protection provisions into Law Number 27 of 2022 and the new Criminal Code. The research recommendations include updating the Election Law by adding a special chapter on digital violations, strengthening Gakkumdu, auditing the security of the SIPOL and SIDALIH systems, and increasing public participation in data-based monitoring to maintain the integrity and transparency of digital elections in Indonesia*.
Keywords*: Electoral Criminal Law, Personal Data Protection, Unauthorized Data Use, Legal Reformulation, Electoral Integrity*

Abstrak: Penelitian ini menyoroti penyalahgunaan data pribadi secara masif tanpa izin dalam pelaksanaan pemilu, khususnya pada tahap pendaftaran dan verifikasi partai politik melalui Sistem Informasi Partai Politik (SIPOL). Kondisi ini menunjukkan lemahnya perlindungan hukum terhadap hak privasi warga, mengingat Undang-Undang Nomor 7 Tahun 2017 tentang Pemilu tidak secara tegas mengatur sanksi atas pelanggaran semacam itu. Penelitian ini menggunakan metode yuridis normatif dengan pendekatan legislatif, konseptual, dan studi kasus untuk mengkaji regulasi, doktrin hukum pidana, serta praktik pemilu. Hasil penelitian menunjukkan bahwa tidak ada norma yang komprehensif yang mengatur penggunaan data pribadi tanpa izin dalam konteks pemilu, sehingga menciptakan ketidakpastian hukum dan melemahkan perlindungan hak warga. Oleh karena itu, perlu merumuskan ulang undang-undang pemilu dengan mengintegrasikan ketentuan perlindungan data pribadi ke dalam Undang-Undang Nomor 27 Tahun 2022 dan Kitab Undang-Undang Hukum Pidana yang baru. Rekomendasi penelitian mencakup pembaruan Undang-Undang Pemilu dengan menambahkan bab khusus tentang pelanggaran digital, memperkuat Gakkumdu, mengaudit keamanan sistem SIPOL dan SIDALIH, serta meningkatkan partisipasi publik dalam pemantauan berbasis data untuk menjaga integritas dan transparansi pemilu digital di Indonesia.
Kata Kunci: Hukum Pidana Pemilu, Perlindungan Data Pribadi, Penggunaan Data Tanpa Izin, Perumusan Ulang Hukum, Integritas Pemilu

Introduction

The general election (Pemilu) is a fundamental instrument in Indonesia's democratic system as a manifestation of the people's sovereignty, in accordance with Article 1 paragraph (2) of the 1945 Constitution of the Republic of Indonesia. Through elections, citizens have the constitutional right to directly participate in determining national policies and leadership. Elections function not merely as a procedural mechanism but also as a constitutional means to establish a government that is politically and morally legitimate through public participation.[1]

Political parties play a strategic role as instruments of political recruitment and as intermediaries between public aspirations and state policies.[2] However, the dynamics of elections in the digital era bring new challenges to data governance and electoral ethics. The digitalization of electoral systems such as the Political Party Information System (SIPOL), Candidate Information System (SILON), and Voter Data Information System (SIDALIH) has accelerated administrative processes but simultaneously opened opportunities for misuse of citizens' personal data.

[1]Muhammad Syafei and Muhammad Rafi Darajati, "Design of General Election in Indonesia," *Law Reform: Jurnal Pembaharuan Hukum* 16, no. 1 (2020), https://doi.org/10.14710/lr.v16i1.30308; Jimly Asshiddiqie, *Konstitusi Dan Pemilu Dalam Perspektif Demokrasi* (Jakarta: Rajawali Pers, 2011), 117; Gede Karya et al., "Big Data Integration Design for General Election in Indonesia," in *2020 5th International Conference on Informatics and Computing, ICIC 2020*, 2020, https://doi.org/10.1109/ICIC50835.2020.9288657; Stefan Eklöf, "The 1997 General Election in Indonesia," *Asian Survey* 37, no. 12 (1997), https://doi.org/10.2307/2645765.

[2]Saiful Risky, Sholahuddin Al-Fatih, and Mabarroh Azizah, "Political Configuration of Electoral System Law in Indonesia from State Administration Perspective," *Volksgeist: Jurnal Ilmu Hukum Dan Konstitusi* 6, no. 1 (2023), https://doi.org/10.24090/volksgeist.v6i1.7940; Yves Mény and Andrew Knapp, *Government and Politics in Western Europe: Britain, France, Italy, Germany* (Oxford: Oxford University Press, 1998), 112; Yves Mény and Andrew Knapp, *Government and Politics in Western Europe: Britain, France, Italy, Germany* (Oxford: Oxford University Press, 1998).

The phenomenon of identity theft, or the use of another person's name without consent in political party registration, demonstrates the weakness of data protection mechanisms in election administration. The Indonesian Election Supervisory Agency (Bawaslu) has recorded several public reports regarding unauthorized use of names in SIPOL, including the identities of civil servants, village officials, and even election organizers who are legally prohibited from affiliating with political parties.[3]

This condition highlights a gap between technological advancement and regulatory readiness. The Republic of Indonesia's Law No. 7 of 2017 on General Elections does not explicitly regulate prohibitions or sanctions against the unauthorized use of personal data in electoral processes.[4] As a result, such acts cannot be categorized as electoral crimes but can only be prosecuted under general criminal law, such as Article 378 of the Criminal Code (KUHP) on fraud, or Article 67 of Law No. 27 of 2022 on Personal Data Protection. Yet, these acts clearly violate citizens' constitutional right to privacy, as guaranteed by Article 28G, paragraph (1), of the 1945 Constitution.

The absence of specific criminal provisions in the Election Law addressing unauthorized use of personal data creates a legal vacuum. Criminal law formation must always be responsive and anticipatory to social changes, including the emergence of new forms of crime resulting from technological progress.[5] In line with Sudarto, criminal law has two main functions: repressive, to punish violations, and preventive, to deter crimes that harm society.[6]

The urgency of electoral law reform becomes more pressing when personal data misuse threatens the integrity of democracy and public trust in electoral institutions such as the General Election Commission (KPU) and Bawaslu. In the digital society, "code is law," meaning that digital systems also carry normative power that must be legally regulated to prevent abuse.[7] Thus, electoral regulations must be restructured to be more adaptable to the digital context, incorporating personal data protection norms into electoral crimes.

This approach aligns with the principle of *lex specialis derogat legi generali*, whereby specific laws (Law No. 7 of 2017 on General Elections) should contain explicit

[3]Putra Perdana Ahmad Saifulloh, Beni Kurnia Illahi, and Sonia Ivana Barus, "Legal Standing to the Corruption Eradication Commission as a Applicant for the Dissolution of a Political Party at the Constitutional Court," *Jurnal Konstitusi* 20, no. 2 (2023), https://doi.org/10.31078/jk2028.

[4]Moody Rizqy Syailendra, "Personal Data Protection Law In Indonesia: Challenges And Opportunities," *Indonesia Law Review* 14, no. 2 (2024), https://doi.org/10.15742/ilrev.v14n2.4; Erman I. Rahim et al., "Personal Data Protection in Political Party Information Systems in the Organization of General Elections: Concept and Law Reform Recommendations," *Journal of Law and Legal Reform* 6, no. 3 (2025), https://doi.org/10.15294/jllr.v6i3.12942.

[5]Barda Nawawi Arief, *Bunga Rampai Kebijakan Hukum Pidana: Perkembangan Penyusunan Konsep KUHP Baru* (Jakarta: Kencana Prenada Media Group, 2011), 5; Afdhal Ananda Tomakati, "Konsepsi Teori Hukum Pidana Dalam Perkembangan Ilmu Hukum," *Jurnal Hukum Pidana Dan Kriminologi* 4, no. 1 (2023), https://doi.org/10.51370/jhpk.v4i1.99.

[6]Sudarto, *Hukum Pidana Dan Perkembangan Masyarakat* (Bandung: Sinar Baru, 1983); O. H Eddy, *Asas Legalitas Dan Penemuan Hukum Dalam Hukum Pidana* (Jakarta: Erlangga, 2009).

[7]Lawrence Lessig, *Code and Other Laws of Cyberspace* (New York: Basic Books, 1999), 6.

provisions regarding violations related to electoral processes, including personal data misuse. Such reformulation must be harmonized with the Personal Data Protection Law (Law No. 27 of 2022) and the new Criminal Code (Law No. 1 of 2023), which, in Article 281, recognizes the right to privacy and personal data as part of human rights.

The study of criminal law policy has long been discussed by classical scholars who emphasize that criminal law policy must be designed rationally, functionally, and oriented toward the values of justice. Punishment does not merely serve as a means of retribution but also as an instrument of prevention and protection of societal interests, including citizens' rights to personal data.[8] This view is consistent with Bassiouni's opinion, which states that criminal law must function repressively, preventively, and restoratively.[9]

The concept of criminal law policy is essentially part of social policy aimed at protecting society from various forms of crime and social deviance. Over time, criminal law policy has not only been directed toward combating conventional crimes but also toward addressing new forms of crime emerging from developments in information technology. Therefore, the formulation of criminal law must be capable of adapting to societal dynamics and technological advancements in order to remain effective in providing legal protection for both individual and public interests.[10]

In the context of personal data protection, criminal law policy plays an important role as an *ultimum remedium* instrument used to create a deterrent effect against perpetrators of personal data misuse. The protection of personal data constitutes part of human rights protection, particularly the right to privacy, which is recognized in various national and international legal instruments. Consequently, the misuse of personal data should not merely be regarded as an administrative violation but may also be categorized as an act that infringes upon the constitutional rights of citizens.[11]

In the context of electoral law, elections are not merely procedural mechanisms but also constitutional instruments for establishing a government with political and moral legitimacy.[12] Political parties serve as intermediaries between public aspirations and state policies.[13] Nevertheless, electoral regulations as stipulated in Law Number 7 of 2017 on General Elections have not fully accommodated issues concerning personal data protection, thereby creating a legal vacuum in addressing digitally based violations.

---

[8]Sudarto, *Hukum Pidana Dan Perkembangan Masyarakat*.

[9]M. Cherif Bassiouni, *Introduction to International Criminal Law* (Leiden: Brill, 2003).

[10]Barda Nawawi Arief, *Masalah Penegakan Hukum Dan Kebijakan Hukum Pidana Dalam Penanggulangan Kejahatan* (Jakarta: Kencana Prenada Media Group, 2018); Muladi and Barda Nawai Arief, *Teori-Teori Dan Kebijakan Pidana* (Bandung: Alumni, 1992).

[11]United Nations Development Programme (UNDP), *Universal Declaration of Human Rights* (New York: United Nations Development Programme (UNDP), 1948); John Tobin, "Teaching Human Rights," in *The Struggle for Human Rights*, 2021, https://doi.org/10.1093/oso/9780198868064.003.0013.

[12]Asshiddiqie, *Konstitusi Dan Pemilu Dalam Perspektif Demokrasi*.

[13]Knapp, *Government and Politics in Western Europe: Britain, France, Italy, Germany*.

Democratic elections require guarantees of honesty, fairness, transparency, and accountability. As the use of information technology in electoral administration continues to increase, new challenges related to data security and the protection of citizens' identities have emerged. While the digitalization of electoral processes offers significant advantages in terms of administrative efficiency and effectiveness, it simultaneously increases the risk of personal data misuse if not accompanied by adequate regulatory frameworks and supervisory mechanisms.[14]

Several contemporary studies have also examined similar issues. Kusnaldi et al. highlight the challenges of data leakage within digital electoral systems, though their study primarily focuses on administrative aspects.[15] Syailendra et al. discuss the opportunities and obstacles in implementing the Personal Data Protection Law, but do not directly connect the issue to electoral criminal law.[16] Meanwhile, Attidhira and Permana emphasize the weaknesses of personal data protection regulations in Indonesia in general, without specifically addressing the context of digital elections.[17]

Based on the review of previous studies, it can be observed that most existing research focuses either on personal data protection in general or on the administrative aspects of digital electoral administration. Studies specifically examining the relationship between personal data misuse, electoral crimes, and the need for the reformulation of criminal law policy remain relatively limited. Therefore, there is a need for research that integrates the perspectives of criminal law and electoral law within a comprehensive analytical framework.

This study seeks to fill this gap through an integrative approach that combines criminal law and electoral law perspectives, particularly in the context of personal data misuse within digital systems such as SIPOL and SILON. The focus of this research is to examine the urgency of reformulating electoral criminal law in response to the challenges of digitalization while ensuring legal certainty, justice, and the protection of citizens' constitutional rights.

This study employs a normative legal research method with a normative juridical approach. This method positions law as a set of norms or rules that prevail within society and serve as guidelines for regulating human behavior. Normative legal research focuses on the examination of legislation, legal principles, legal doctrines, legal theories, and court decisions related to the legal issues under investigation. In this study, the normative juridical approach is utilized to analyze the legal framework

[14]Rina Shahriyani Shahrullah, Jihyun Park, and Irwansyah, "Examining Personal Data Protection Law of Indonesia and South Korea: The Privacy Rights Fulfilment," *Hasanuddin Law Review* 10, no. 1 (2024).

[15]Rahim et al., "Personal Data Protection in Political Party Information Systems in the Organization of General Elections: Concept and Law Reform Recommendations."

[16]Kukuh Dwi Kurniawan et al., "Criminal Sanctions and Personal Data Protection in Indonesia," *Lex Publica* 11, no. 2 (2024), https://doi.org/10.58829/lp.11.2.2024.255.

[17]Mladen Milošević, "Personal Data Protection In Criminal Law," *Journal of Criminology and Criminal Law* 59, no. 2 (2021), https://doi.org/10.47152/rkkp.59.2.7; Mia Puteri Deviana, Poppy Hermaya, and Yusuf Abdul Rahman, "Kajian Yuridis Perlindungan Data Pribadi Masyarakat Yang Dicatut Calon Peserta Pemilu 2024," *PALAR (Pakuan Law Review)* 9, no. 3 (2023).

governing the unauthorized use of personal identity in electoral processes and the legal liability arising from such acts.

The normative juridical approach limits the scope of the research to the formulation of legal issues, the object of study, and the legal scholarly tradition that is oriented toward the examination of positive law. Normative legal science has the primary functions of describing, systematizing, interpreting, analyzing, and evaluating the positive law applicable within society.[18] Therefore, this study not only identifies the applicable legal norms but also examines their adequacy in providing legal protection for citizens' rights within the electoral context.

To obtain a comprehensive analysis, this study employs three principal approaches, namely the statute approach, the conceptual approach, and the case approach. *First*, the statute approach is used to examine various laws and regulations relevant to the object of the study. Through this approach, the researcher identifies, inventories, and analyzes legal norms governing election administration, personal data protection, and criminal liability for identity misuse. The regulations examined include the 1945 Constitution of the Republic of Indonesia, Law Number 7 of 2017 concerning General Elections, Law Number 27 of 2022 concerning Personal Data Protection, the Indonesian Criminal Code (KUHP), as well as various regulations issued by the General Election Commission (KPU) and the Election Supervisory Agency (Bawaslu).[19]

Second, the conceptual approach is employed to examine legal concepts, theories, doctrines, and principles related to personal data protection, the right to privacy, criminal liability, cybercrime, and electoral offenses. This approach aims to provide a theoretical foundation for understanding the legal position of personal identity misuse within the Indonesian legal system. Furthermore, the conceptual approach is used to connect criminal law theories with the principles of public ethics and democracy. Criminal law should be directed toward protecting public interests, maintaining social order, and upholding the moral values that exist within society.[20]

Third, the case approach is utilized to examine court decisions, jurisprudence, and cases relevant to the misuse of personal identity in electoral processes and other offenses involving personal data. The analysis of cases is conducted to understand how judges interpret legal norms, evaluate evidence, and apply principles of justice in

[18]D Meuwissen, *Pengantar Ilmu Hukum* (Jakarta: UI Press, 2002).

[19]Republic of Indonesia, "Undang-Undang Nomor 7 Tahun 2017 Tentang Pemilihan Umum [Law No. 7 of 2017 Concerning General Elections], State Gazette of the Republic of Indonesia Year 2017 No. 182, Supplement to the State Gazette of the Republic of Indonesia No. 6109)." (Jakarta: State Secretariat, 2017); Republic of Indonesia, "Undang-Undang Nomor 27 Tahun 2022 Tentang Pelindungan Data Pribadi [Law No. 27 of 2022 on Personal Data Protection], State Gazette of the Republic of Indonesia Year 2022 No. 196, Supplement to the State Gazette of the Republic of Indonesia No. 6820" (Jakarta: State Secretariat, 2022); Republic of Indonesia, "Undang-Undang Nomor 1 Tahun 2023 Tentang Kitab Undang-Undang Hukum Pidana [Law No. 1 of 2023 on the Criminal Code], State Gazette of the Republic of Indonesia Year 2023 No. 1, Supplement to the State Gazette of the Republic of Indonesia No. 6842" (Jakarta: State Secretariat, 2023).

[20]Anisya Ines Safitri, Aldo Andrieyan Putra Makaminan, and Mujiono Hafidh Prasetyo, "Kebijakan Hukum Pidana Dalam Upaya Penanggulangan Tindak Cyber Prostitution," *Jurnal Pembangunan Hukum Indonesia* 3, no. 1 (2021), https://doi.org/10.14710/jphi.v3i1.70-79.

resolving disputes. Consequently, this approach provides insight into the implementation of law in practice and helps identify potential legal gaps or inconsistencies between legal norms and their application.[21]

The legal materials used in this study consist of primary, secondary, and tertiary legal materials. Primary legal materials include legislation, court decisions, and official documents related to elections and personal data protection. Secondary legal materials comprise legal textbooks, scholarly journal articles, previous research findings, expert opinions, and other academic works relevant to the research topic. Meanwhile, tertiary legal materials include legal dictionaries, legal encyclopedias, and other reference sources that facilitate the understanding of primary and secondary legal materials.

The collection of legal materials is conducted through library research by reviewing and compiling legal documents, academic literature, and other legal sources relevant to the research focus. Subsequently, the collected legal materials are analyzed using a qualitative method with a descriptive-analytical approach. The analysis is carried out through the processes of inventorying, classifying, interpreting, and systematizing legal materials in order to obtain a comprehensive understanding of the issues under examination.

Through the combination of the statute, conceptual, and case approaches, supported by qualitative analysis of relevant legal sources, this study is expected to produce an in-depth examination of the misuse of personal identity in electoral offenses. Furthermore, the study seeks to provide legal recommendations for addressing existing legal vacuums and strengthening personal data protection within the administration of elections in Indonesia, thereby contributing to the realization of an honest, fair, and integrity-based democratic process.

One of the Crucial Issues in Electoral Digitalization

One of the crucial problems arising in the era of electoral digitalization is the unauthorized use of another person's name or identity by political parties or individual candidates, particularly during the registration process through the Political Party Information System (SIPOL) and the Candidate Information System (SILON). This practice is often carried out to fulfill administrative requirements such as the minimum number of party members, women's representation quotas, or public support requirements. Numerous cases have shown that citizens only become aware that their names have been misused after the verification process has been completed, indicating the weakness of personal data protection within digital-based electoral systems.[22]

This phenomenon demonstrates the existence of a legal vacuum in Law Number 7 of 2017 on General Elections, as there are no provisions that explicitly classify identity misuse as an electoral crime. Although such conduct violates Law Number 27

[21]Pengadilan Negeri, "Putusan Pengadilan Negeri Jakarta Pusat No. 123/Pid.Sus/2020/PN.Jkt.Pst [Central Jakarta District Court, Decision No. 123/Pid.Sus/2020/PN.Jkt.Pst]," 2020.

[22]Bawaslu RI, *Laporan Pengawasan SIPOL* (Jakarta: Bawaslu, 2024).

of 2022 on Personal Data Protection, its enforcement cannot be directly applied within the electoral context.[23] Consequently, such violations can only be prosecuted under general criminal law provisions, such as those contained in the Indonesian Criminal Code (KUHP), which are not entirely compatible with the specific characteristics of electoral violations. This condition highlights the urgency of reformulating electoral criminal law so that it becomes more adaptive to digital developments and capable of providing effective protection for citizens' privacy rights.

In addition to causing harm to individuals whose identities are used without consent, the misuse of personal data also has the potential to generate broader consequences for the quality of democracy. Invalid data used in the verification of political party membership or support for independent candidates may affect the accuracy of electoral administration and undermine the credibility of the verification process conducted by electoral management bodies.[24] In the long term, such conditions may reduce public trust in digital electoral systems and in the institutions responsible for administering elections.

The unauthorized use of another person's identity in electoral processes constitutes a serious violation of the principles of electoral honesty and fairness. However, it is not yet explicitly regulated under Law Number 7 of 2017 on General Elections. Such practices are frequently found during the verification of political party membership and support for independent candidates, particularly through SIPOL and SILON.[25] This regulatory gap demonstrates the continued weakness of electoral criminal law in protecting citizens' privacy rights.

From the perspective of constitutional law, personal data protection is an integral part of the protection of citizens' constitutional rights, as guaranteed under Article 28G, paragraph (1), of the 1945 Constitution of the Republic of Indonesia. Therefore, any use of personal data without the consent of the data subject not only gives rise to criminal legal consequences but may also be regarded as a violation of human rights.[26] Accordingly, personal data protection in electoral administration must be positioned as an inseparable component of efforts to maintain democratic quality and uphold the rule of law.

Normatively, such conduct may be prosecuted under Articles 520 and 540 of the Election Law concerning false statements and data falsification, as well as Article 263 of the Criminal Code concerning forgery. However, these provisions have not been able to optimally accommodate violations that are based on digital technology. Weak

[23]Indonesia, "Undang-Undang Nomor 27 Tahun 2022 Tentang Pelindungan Data Pribadi [Law No. 27 of 2022 on Personal Data Protection], State Gazette of the Republic of Indonesia Year 2022 No. 196, Supplement to the State Gazette of the Republic of Indonesia No. 6820."

[24]KPU RI, *Verifikasi Partai Politik*, KPU (Jakarta, 2023).

[25]Republic of Indonesia, "Undang-Undang Nomor 7 Tahun 2017 Tentang Pemilihan Umum [Law Number 7 of 2017 Concerning General Elections], State Gazette of the Republic of Indonesia of 2017 Number 182, Supplement to the State Gazette of the Republic of Indonesia Number 6109" (Jakarta: State Secretariat, 2017).

[26]Republic of Indonesia, "Article 28G Paragraph (1) Undang-Undang Dasar Negara Republik Indonesia Tahun 1945 [The 1945 Constitution of the Republic of Indonesia]" (1945).

verification mechanisms within the General Election Commission (KPU), which have not been equipped with adequate consent verification systems or individual authentication mechanisms, render citizens' personal data vulnerable to manipulation and misuse.[27] Meanwhile, Law Number 27 of 2022 on Personal Data Protection has provided a strong legal foundation, but it has not yet been effectively integrated with the Election Law or with supervisory mechanisms implemented by the Election Supervisory Agency (Bawaslu) and the Integrated Law Enforcement Center (Gakkumdu).

This condition indicates that the primary issue lies not only in the substance of the law but also in its structural and cultural dimensions. From a structural perspective, coordination between electoral management bodies and institutions responsible for personal data protection remains insufficient. From a legal culture perspective, public awareness regarding the importance of safeguarding personal data and reporting incidents of identity misuse remains relatively low.[28] Therefore, efforts to address these violations must be undertaken comprehensively through regulatory reform, institutional strengthening, and the enhancement of public digital literacy.

Research findings by Faradillah Aulia Rahma and Rahajeng Suci Damayanti et al. indicate that electoral criminal law policy in Indonesia remains reactive in nature, acting only after violations occur rather than prioritizing preventive measures through stronger regulations and supervisory systems.[29] As a result, many cases of identity misuse are resolved merely through administrative mechanisms without the imposition of firm criminal sanctions. This situation not only violates citizens' privacy rights but also threatens democratic integrity and diminishes public trust in electoral institutions.

These findings suggest that the current model of electoral law enforcement remains primarily focused on conventional violations, such as vote-buying, unlawful campaigning, and other administrative violations. Meanwhile, developments in information technology have given rise to new forms of misconduct that require different regulatory and enforcement approaches. Therefore, the reform of electoral criminal law should not only aim to impose sanctions on perpetrators but also to establish preventive mechanisms capable of minimizing the risk of personal data misuse from the earliest stages of the electoral process.[30]

Accordingly, this study emphasizes the urgency of reformulating electoral criminal law by explicitly recognizing the unauthorized use of personal data as a specific form of electoral cybercrime. Furthermore, integration between the Election Law, the Personal Data Protection Law, and the Electronic Information and

[27]"Artcle 263 Kitab Undang-Undang Hukum Pidana (KUHP) [Article 263 of the Indonesian Criminal Code]" (n.d.).

[28]Alwi Al Hadad, "Keamanan Data Dalam Proses Pemilu 2024: Identifikasi Dan Mitigasi Ancaman Kebocoran Data Elektoral," *Jurnal Keadilan Pemilu* 2, no. 1 (2023).

[29]M Harun, "Reformulasi Kebijakan Hukum Terhadap Penegakan Hukum Pidana Pemilu Dalam Menjaga Kedaulatan Negara," *Jurnal Rechts Vinding: Media Pembinaan Hukum Nasional* 5, no. 1 (2016).

[30]Harun.

Transactions Law (ITE Law) is necessary to provide more comprehensive protection for citizens' constitutional rights. Through such regulatory harmonization, Indonesia's electoral legal system is expected to be better equipped to address the challenges of digitalization, strengthen the legitimacy of digital democracy, and ensure elections that are more honest, fair, transparent, and accountable.[31]

Such reformulation should also be accompanied by the development of more secure digital verification systems, the implementation of valid consent principles, and the strengthening of technology-based supervisory mechanisms. In this way, personal data protection will not merely exist as a formal legal norm but will become an integral part of electoral administration practices that effectively safeguard citizens' rights and preserve democratic integrity in the digital era.

Ineffectiveness of Regulation and Law Enforcement

The regulation and law enforcement concerning the unauthorized use of personal data in the administration of elections still demonstrate a low level of effectiveness, both in terms of legal substance and institutional capacity. The misuse of citizens' identities in the process of political party registration and candidate support, particularly through the Political Party Information System (SIPOL) and the Candidate Information System (SILON), reflects the weakness of legal mechanisms in addressing the challenges of electoral digitalization. This condition indicates that Law No. 7 of 2017 on General Elections has not fully adapted to the realities of digital democracy, which require the protection of privacy and personal data as constitutional rights of citizens.

The absence of provisions that explicitly prohibit and impose sanctions on the unauthorized use of personal data in the Election Law has created a legal vacuum. Articles 520 and 521 of the Election Law essentially regulate the provision of false information and disruptions to the electoral process but do not accommodate the misuse of digital data. Consequently, serious violations of citizens' privacy rights are often categorized merely as administrative offenses. This situation contradicts the principles of *lex certa* and *nullum crimen sine lege*, which require clear legal certainty and protection against all forms of legal violations, particularly those affecting democratic legitimacy.

From the perspective of criminal law policy, this weakness demonstrates that Indonesia's electoral legal system remains reactive and procedural rather than preventive and substantive. Law enforcement tends to be carried out only after violations have occurred, rather than through the development of systems capable of preventing misuse from the design stage (*data protection by design*). As argued by Arief (2008), criminal law must possess anticipatory, corrective, and protective functions in

[31]Republic of Indonesia, "Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik [Law No. 11 of 2008 on Electronic Information and Transactions], State Gazette of the Republic of Indonesia Year 2008 No. 58, Supplement to the State Gazette of the Republic of I" (Jakarta: State Secretariat, 2008).

responding to social changes, including the emergence of digital crimes that exploit technology in electoral processes.

Weak coordination among institutions further exacerbates the situation. The Integrated Law Enforcement Center (*Gakkumdu*) and the Election Supervisory Agency (*Bawaslu*) continue to face limitations in applying digital evidence standards and encounter difficulties in classifying personal data misuse as an electoral crime. On the other hand, the General Election Commission (KPU) has not yet developed adequate authentication systems or consent verification mechanisms to ensure that political party membership data or candidate support data are obtained lawfully and with the consent of the data subjects. This gap creates opportunities for certain actors to manipulate population data without authorization, ultimately reducing public trust in the integrity of election administration.

From both social and legal perspectives, the impact of weak law enforcement is highly significant. Citizens lose control over their personal data and may suffer identity-related harm, moral damages, and reputational losses. This condition reflects the state's failure to uphold the principles of the rule of law and due process of law as mandated by Article 1, paragraph (3) of the 1945 Constitution of the Republic of Indonesia. Furthermore, the right to personal protection and privacy, as guaranteed by Article 28G, paragraph (1), of the Constitution, becomes practically meaningless if it is not adequately accommodated within electoral legal norms.

Moreover, weak regulation and law enforcement regarding the misuse of personal data in elections have the potential to create a negative precedent for the development of digital democracy in Indonesia. If identity theft and unauthorized use of personal data are allowed to continue without firm sanctions, a perception may emerge that violations of personal data rights carry minimal legal consequences. Therefore, legal reform is required not only to strengthen the normative framework by establishing specific criminal provisions but also to enhance institutional capacity, digital oversight systems, and personal data protection mechanisms at every stage of the electoral process. In this way, the goal of realizing elections that are democratic, credible, and respectful of citizens' constitutional rights can be achieved more effectively in the digital era.

Overall, the findings of this study indicate that personal data protection must be positioned as a fundamental element in developing an electoral legal system that is modern, adaptive, and responsive to advances in information technology. The existence of clear regulations, effective supervisory mechanisms, and strong inter-institutional coordination constitutes an essential prerequisite for preventing identity misuse within electoral processes. In addition, improving public digital literacy is equally important, so that citizens have greater awareness of their personal data rights and are able to take independent measures to protect their information from potential misuse.[32]

[32]Denny Suwondo, "The Legal Protection of Personal Data in the Perspective of Human Rights," *Law Development Journal* 5, no. 4 (2024).

Furthermore, the strengthening of personal data protection within electoral administration should not be viewed solely as a legal obligation but also as a strategic effort to preserve democratic values in the digital era. The protection of personal data contributes to ensuring fair political participation, safeguarding citizens from abuse of power, and maintaining transparency and accountability in electoral governance. Therefore, legal protection of personal data should become an integral component of broader electoral reform efforts in Indonesia.

To address these challenges, future electoral law reform should focus on establishing an integrated, sustainable personal data protection system. Such efforts are intended not only to provide legal certainty and safeguard citizens' constitutional rights but also to strengthen democratic legitimacy, enhance public confidence in electoral management bodies, and ensure that democratic processes in Indonesia operate in accordance with the principles of justice, transparency, accountability, and respect for human rights in the digital age.

Integrating electoral law with personal data protection regulations and other relevant legal frameworks should be accompanied by the development of secure digital infrastructure, periodic security audits, and enhanced monitoring of election-related information systems. Through these measures, electoral institutions will be better equipped to anticipate emerging digital threats and prevent the misuse of personal data before violations occur.

Ultimately, the success of electoral law reform in responding to digitalization challenges will depend not only on the quality of legal norms but also on the commitment of state institutions, political actors, and society as a whole to uphold democratic ethics and respect citizens' privacy rights. A comprehensive and collaborative approach is therefore necessary to ensure that Indonesia's electoral system remains capable of adapting to technological developments while preserving democratic integrity and protecting the constitutional rights of all citizens.

The Interrelationship Between Electoral Law and Personal Data Protection

Unauthorized use of personal data in elections is a serious violation of privacy and constitutional rights, yet it is still treated as an administrative offense by the KPU and Bawaslu. Substantively, however, such acts involve fraud and data misuse that meet the criteria for criminal liability, causing harm to data subjects and undermining democratic integrity.

The right to personal data is part of the constitutional and human rights guaranteed under Article 28G, paragraph (1), of the 1945 Constitution. This is reinforced in Law No. 27 of 2022 on Personal Data Protection, particularly Article 65 paragraph (1), which prohibits the use of personal data without valid consent. In practice, however, the principles of personal data protection are not fully integrated into electoral administration. Unauthorized use of personal data in systems such as SIPOL is often categorized as administrative rather than criminal. This legal gap shows that Indonesia's electoral law is not adaptive to digitalization and personal data

protection, leaving citizens' political rights unprotected. Integration between the Election Law and the PDP Law is needed to ensure digital identity protection as part of citizens' political rights.

Criminal law plays a vital role in safeguarding democracy by protecting citizens' privacy from data misuse. Yet, Law No. 7 of 2017 does not explicitly classify unauthorized use of personal data as an electoral crime. This normative gap creates ambiguity in enforcement, leading to violations being handled administratively rather than with firm criminal sanctions.[33] Sudarto emphasizes that criminal law must have preventive and repressive functions to maintain social order and public justice. In line with this, reformulating the Election Law is necessary to categorize misuse of personal data as an electoral crime, thereby directly affecting electoral legitimacy. The principle of *lex specialis derogat legi generali* is crucial so that the Election Law functions as a special law overriding general provisions in the Criminal Code, while integrating PDP Law principles to ensure justice, transparency, and protection of constitutional rights.[34]

Political parties and electoral institutions, such as the KPU, have a constitutional responsibility to safeguard the integrity of membership and voter data. Data misuse in party verification is not merely administrative but reflects the legitimacy of citizens' political participation. Thus, unauthorized use of data constitutes a serious violation of constitutional rights under Article 28G, paragraph (1), and the PDP Law.

Unfortunately, the Election Law does not explicitly require the KPU to verify data directly with its owners; instead, it relies on data submitted by parties via SIPOL. This legal gap enables misuse without firm sanctions. As public law entities, political parties are obliged to uphold good governance and accountability in the management of membership data. From a criminal law perspective, the intentional misuse of personal data for political purposes constitutes a criminal offense under Article 65, paragraphs (1) and (3), of the PDP Law. Reformulating the legal responsibilities of political parties and the KPU is therefore essential to strengthen electoral law systems that are adaptive to political digitalization, by imposing criminal sanctions for violations of personal data to safeguard democratic integrity.

In the context of the rapid development of information technology, the electoral legal system must adapt to the emerging new forms of violations in the digital sphere. The shift in the pattern of violations from conventional forms to technology-based offenses demonstrates that electoral law cannot focus solely on administrative and procedural aspects. Instead, a more progressive legal approach is needed by integrating personal data protection principles into every electoral policy, supervisory mechanism, and law enforcement process.[35]

---

[33]Meyke M Camaru et al., "The Nature of Law Enforcement of General Election Crimes in Indonesia," *IOSR Journal Of Humanities And Social Science (IOSR-JHSS* 28, no. 2 (2023).

[34]Sudarto, *Hukum Pidana Dan Perkembangan Masyarakat*.

[35]Any Ismayawati, Aristoni Aristoni, and Amrina Rosyada, "Challenges in Criminal Law Enforcement against Political Patronage in Regional Head Elections," *De Jure: Jurnal Hukum Dan Syar'iah* 17, no. 2 (2025), https://doi.org/10.18860/j-fsh.v17i2.33001.

Strengthening personal data protection in elections requires the involvement of various stakeholders, including the government, election management bodies, political parties, law enforcement agencies, and society as a whole. Such stakeholder synergy is essential for fostering a legal culture that respects privacy and ensures the responsible use of personal data. Without collective awareness regarding the importance of personal data protection, various regulatory reform efforts may fail to operate effectively in practice.

Accordingly, the reformulation of electoral criminal law that recognizes the misuse of personal data as an electoral crime is intended not only to provide legal certainty and deterrent effects for perpetrators but also to serve as a strategic measure for strengthening human rights protection, improving the quality of digital democracy, and safeguarding the legitimacy of electoral outcomes. The existence of comprehensive regulations and effective law enforcement mechanisms is expected to create a more reliable and integrity-based electoral system capable of responding to future technological developments.

Ultimately, the success of personal data protection in the administration of elections will serve as an important indicator of Indonesia's democracy's maturity. The stronger the protection of citizens' personal data, the greater the public trust in electoral processes and outcomes. Therefore, electoral law reform oriented toward personal data protection constitutes an urgent necessity for realizing a democratic system that is not only procedurally democratic but also just, accountable, integrity-based, and respectful of the constitutional rights of every citizen.

Urgency of Reformulating Electoral Criminal Law Policy

This study highlights the urgency of comprehensively and responsively reformulating electoral criminal law policy for the digital era. Harmonization between the Election Law, the PDP Law, and the ITE Law is essential so that unauthorized use of personal data can be categorized as an electoral crime rather than an administrative violation. Legal reform will strengthen legal certainty, guarantee the protection of constitutional rights, and restore public trust in electoral justice and integrity.

Digital technology has fundamentally transformed Indonesia's electoral system while also creating new challenges, such as unauthorized misuse of personal data. This practice constitutes a serious violation of privacy and constitutional rights, but is not adequately addressed within electoral criminal law. This regulatory gap threatens the integrity of digital democracy and underscores the need to reformulate electoral criminal law to adapt to technological developments.[36]

First, from the theoretical foundation of criminal law policy emphasize that criminal law must function not only repressively but also preventively and adaptively to social changes. In the context of electoral digitalization, criminal law must anticipate

[36]Muhtar Hadi Wibowo, "Corporate Responsibility in Money Laundering Crime (Perspective Criminal Law Policy in Crime of Corruption in Indonesia)," *Journal of Indonesian Legal Studies* 3, no. 2 (2018).

new crimes such as voter data misuse and identity manipulation for political purposes. Yet Law No. 7 of 2017 does not explicitly treat misuse of personal data as an electoral crime, leaving it an administrative matter. Substantively, however, such acts constitute fraud and violations of constitutional rights under Article 28G paragraph (1) and the PDP Law. *Second*, reformulating electoral norms and sanctions must explicitly regulate the unauthorized use of personal data as an electoral crime. This reformulation should integrate the principle of *lex specialis derogat legi generali*, making the Election Law a special law that accommodates personal data protection and aligns with the PDP Law and the new Criminal Code (Law No. 1 of 2023).

Conclusion

Based on the findings of this study, it can be concluded that the unauthorized use of another person's name or identity in electoral administrative processes constitutes a legal violation with criminal characteristics. Although not explicitly regulated under Law Number 7 of 2017 on General Elections, such conduct constitutes criminal offenses under Articles 263 and 378 of the Indonesian Criminal Code (KUHP) on forgery and fraud, as well as under Articles 65 and 67 of Law Number 27 of 2022 on Personal Data Protection. The misuse of personal data in electoral processes violates citizens' constitutional rights to privacy and may undermine electoral integrity, public trust, and the legitimacy of democratic processes. Therefore, personal data protection in election administration should be recognized as an essential element of democratic governance rather than merely an administrative matter. This study highlights the need for regulatory reform and harmonization between electoral law, personal data protection law, and criminal law to establish a clear legal framework for addressing personal data misuse as a specific electoral offense. Strengthening the legal framework should be accompanied by improved digital monitoring systems, enhanced institutional capacity, and greater public awareness to ensure elections that are fair, transparent, and accountable in the digital era.

References

Arief, Barda Nawawi. *Bunga Rampai Kebijakan Hukum Pidana: Perkembangan Penyusunan Konsep KUHP Baru*. Jakarta: Kencana Prenada Media Group, 2011.

———. *Masalah Penegakan Hukum Dan Kebijakan Hukum Pidana Dalam Penanggulangan Kejahatan*. Jakarta: Kencana Prenada Media Group, 2018.

Artcle 263 Kitab Undang-Undang Hukum Pidana (KUHP) [Article 263 of the Indonesian Criminal Code] (n.d.).

Asshiddiqie, Jimly. *Konstitusi Dan Pemilu Dalam Perspektif Demokrasi*. Jakarta: Rajawali Pers, 2011.

Bassiouni, M. Cherif. *Introduction to International Criminal Law*. Leiden: Brill, 2003.

Bawaslu RI. *Laporan Pengawasan SIPOL*. Jakarta: Bawaslu, 2024.

Camaru, Meyke M, Mulyati Pawennei, Syaharuddin Nawi, and Nasrullah Arsyad. "The Nature of Law Enforcement of General Election Crimes in Indonesia." *IOSR Journal Of Humanities And Social Science (IOSR-JHSS* 28, no. 2 (2023).

Deviana, Mia Puteri, Poppy Hermaya, and Yusuf Abdul Rahman. "Kajian Yuridis Perlindungan Data Pribadi Masyarakat Yang Dicatut Calon Peserta Pemilu 2024." *PALAR (Pakuan Law Review)* 9, no. 3 (2023).

Eddy, O. H. *Asas Legalitas Dan Penemuan Hukum Dalam Hukum Pidana*. Jakarta: Erlangga, 2009.

Eklöf, Stefan. "The 1997 General Election in Indonesia." *Asian Survey* 37, no. 12 (1997). https://doi.org/10.2307/2645765.

Hadad, Alwi Al. "Keamanan Data Dalam Proses Pemilu 2024: Identifikasi Dan Mitigasi Ancaman Kebocoran Data Elektoral." *Jurnal Keadilan Pemilu* 2, no. 1 (2023).

Harun, M. "Reformulasi Kebijakan Hukum Terhadap Penegakan Hukum Pidana Pemilu Dalam Menjaga Kedaulatan Negara." *Jurnal Rechts Vinding: Media Pembinaan Hukum Nasional* 5, no. 1 (2016).

Indonesia, Republic of. "Undang-Undang Nomor 1 Tahun 2023 Tentang Kitab Undang-Undang Hukum Pidana [Law No. 1 of 2023 on the Criminal Code], State Gazette of the Republic of Indonesia Year 2023 No. 1, Supplement to the State Gazette of the Republic of Indonesia No. 6842." Jakarta: State Secretariat, 2023.

———. "Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik [Law No. 11 of 2008 on Electronic Information and Transactions], State Gazette of the Republic of Indonesia Year 2008 No. 58, Supplement to the State Gazette of the Republic of I." Jakarta: State Secretariat, 2008.

———. "Undang-Undang Nomor 27 Tahun 2022 Tentang Pelindungan Data Pribadi [Law No. 27 of 2022 on Personal Data Protection], State Gazette of the Republic of Indonesia Year 2022 No. 196, Supplement to the State Gazette of the Republic of Indonesia No. 6820." Jakarta: State Secretariat, 2022.

———. "Undang-Undang Nomor 7 Tahun 2017 Tentang Pemilihan Umum [Law No. 7 of 2017 Concerning General Elections], State Gazette of the Republic of Indonesia Year 2017 No. 182, Supplement to the State Gazette of the Republic of Indonesia No. 6109)." Jakarta: State Secretariat, 2017.

———. "Undang-Undang Nomor 7 Tahun 2017 Tentang Pemilihan Umum [Law Number 7 of 2017 Concerning General Elections], State Gazette of the Republic of Indonesia of 2017 Number 182, Supplement to the State Gazette of the Republic of Indonesia Number 6109." Jakarta: State Secretariat, 2017.

Ismayawati, Any, Aristoni Aristoni, and Amrina Rosyada. "Challenges in Criminal Law Enforcement against Political Patronage in Regional Head Elections." *De Jure: Jurnal Hukum Dan Syar'iah* 17, no. 2 (2025). https://doi.org/10.18860/j-fsh.v17i2.33001.

Karya, Gede, Wikan Danar Sunindyo, Benhard Sitohang, Saiful Akbar, and Adi Mulyanto. "Big Data Integration Design for General Election in Indonesia." In *2020 5th International Conference on Informatics and Computing, ICIC 2020*, 2020. https://doi.org/10.1109/ICIC50835.2020.9288657.

Knapp, Yves Mény and Andrew. *Government and Politics in Western Europe: Britain, France, Italy, Germany*. Oxford: Oxford University Press, 1998.

Kurniawan, Kukuh Dwi, Deassy J. A. Hehanussa, Rahmat Setiawan, Indah Susilowati, Sopian, and Desmarani Helfisar. "Criminal Sanctions and Personal Data Protection in Indonesia." *Lex Publica* 11, no. 2 (2024). https://doi.org/10.58829/lp.11.2.2024.255.

Lessig, Lawrence. *Code and Other Laws of Cyberspace*. New York: Basic Books, 1999.

Meuwissen, D. *Pengantar Ilmu Hukum*. Jakarta: UI Press, 2002.

Milošević, Mladen. "Personal Data Protection In Criminal Law." *Journal of Criminology and Criminal Law* 59, no. 2 (2021). https://doi.org/10.47152/rkkp.59.2.7.

Muladi, and Barda Nawai Arief. *Teori-Teori Dan Kebijakan Pidana*. Bandung: Alumni, 1992.

Negeri, Pengadilan. "Putusan Pengadilan Negeri Jakarta Pusat No. 123/Pid.Sus/2020/PN.Jkt.Pst [Central Jakarta District Court, Decision No. 123/Pid.Sus/2020/PN.Jkt.Pst]," 2020.

Programme, United Nations Development. *Universal Declaration of Human Rights*. New York: United Nations Development Programme (UNDP), 1948.

Rahim, Erman I., Mohamad Afriyansyah Dukalang, Abdul Hamid Tome, Nuvazria Achir, and Souad Ezzerouali. "Personal Data Protection in Political Party Information Systems in the Organization of General Elections: Concept and Law Reform Recommendations." *Journal of Law and Legal Reform* 6, no. 3 (2025). https://doi.org/10.15294/jllr.v6i3.12942.

Republic of Indonesia. Article 28G Paragraph (1) Undang-Undang Dasar Negara Republik Indonesia Tahun 1945 [The 1945 Constitution of the Republic of Indonesia] (1945).

RI, KPU. *Verifikasi Partai Politik*. KPU. Jakarta, 2023.

Risky, Saiful, Sholahuddin Al-Fatih, and Mabarroh Azizah. "Political Configuration of Electoral System Law in Indonesia from State Administration Perspective." *Volksgeist: Jurnal Ilmu Hukum Dan Konstitusi* 6, no. 1 (2023). https://doi.org/10.24090/volksgeist.v6i1.7940.

Safitri, Anisya Ines, Aldo Andrieyan Putra Makaminan, and Mujiono Hafidh Prasetyo. "Kebijakan Hukum Pidana Dalam Upaya Penanggulangan Tindak Cyber Prostitution." *Jurnal Pembangunan Hukum Indonesia* 3, no. 1 (2021). https://doi.org/10.14710/jphi.v3i1.70-79.

Saifulloh, Putra Perdana Ahmad, Beni Kurnia Illahi, and Sonia Ivana Barus. "Legal Standing to the Corruption Eradication Commission as a Applicant for the Dissolution of a Political Party at the Constitutional Court." *Jurnal Konstitusi* 20, no. 2 (2023). https://doi.org/10.31078/jk2028.

Shahrullah, Rina Shahriyani, Jihyun Park, and Irwansyah. "Examining Personal Data Protection Law of Indonesia and South Korea: The Privacy Rights Fulfilment." *Hasanuddin Law Review* 10, no. 1 (2024).

Sudarto. *Hukum Pidana Dan Perkembangan Masyarakat*. Bandung: Sinar Baru, 1983.

Suwondo, Denny. "The Legal Protection of Personal Data in the Perspective of Human Rights." *Law Development Journal* 5, no. 4 (2024).

Syafei, Muhammad, and Muhammad Rafi Darajati. "Design of General Election in Indonesia." *Law Reform: Jurnal Pembaharuan Hukum* 16, no. 1 (2020). https://doi.org/10.14710/lr.v16i1.30308.

Syailendra, Moody Rizqy. "Personal Data Protection Law In Indonesia: Challenges And Opportunities." *Indonesia Law Review* 14, no. 2 (2024). https://doi.org/10.15742/ilrev.v14n2.4.

Tobin, John. "Teaching Human Rights." In *The Struggle for Human Rights*, 2021. https://doi.org/10.1093/oso/9780198868064.003.0013.

Tomakati, Afdhal Ananda. "Konsepsi Teori Hukum Pidana Dalam Perkembangan Ilmu Hukum." *Jurnal Hukum Pidana Dan Kriminologi* 4, no. 1 (2023). https://doi.org/10.51370/jhpk.v4i1.99.

Wibowo, Muhtar Hadi. "Corporate Responsibility in Money Laundering Crime (Perspective Criminal Law Policy in Crime of Corruption in Indonesia)." *Journal of Indonesian Legal Studies* 3, no. 2 (2018).