■ Submitted: 15 January 2024 ■ Revised: 24 April 2024 ■ Accepted: 15 May 2024

Legal Construction of Fake Diploma Allegations: An Analysis of Electronic Data Integrity under the Personal Data Protection and Electronic Information Laws

Rijal Ibnu Sani[1], Suartini[2], Tri Cahya Indra Permana[3], Ahmad[4], Misno[5]
[1345]Universitas Muhammadiyah Tangerang
[2]Universitas Al Azhar Indonesia
Jalan Perintis Kemerdekaan I/33 Cikokol Kota Tangerang 15118
*Correspondence email: rijalibnu-sani@umt.ac.id

ABSTRACT: The discourse surrounding the validity of public officials' diplomas in cyberspace is frequently entangled in the criminalization of defamation offenses. There exists a profound ambiguity in law enforcement practices that fail to distinguish between criticizing the validity of an electronic document and intending to attack an individual's personal honor. This blurred boundary generates concern among citizens who seek to exercise social control over the integrity of educational data, yet are instead confronted with the excessive penal threats of the Electronic Information and Transactions (ITE) Law. This study aims to deconstruct the juridical status of diplomas as electronic data within the framework of the ITE Law and the Personal Data Protection (PDP) Law, and to examine the implications of Constitutional Court Decision No. 104/2024 for the legal protection of individuals who verify public data within the digital ecosystem. Method: This research employs a normative juridical method using statutory and case approaches to analyze the ratio decidendi of the Constitutional Court. Results: The findings demonstrate that, from a telematics law perspective, a diploma constitutes a set of electronic information characterized as an object of information or a digital asset. Based on the latest Constitutional Court ruling, a clear distinction is established whereby the object of defamation is limited to human beings as legal subjects possessing dignity and honor, rather than objects or documents. Conclusion**:** Juridically, questioning the integrity of diploma data cannot automatically be classified as defamation. As long as the statement focuses on the authentication and verification of the document, such conduct forms part of freedom of expression and the exercise of social control protected by law.

KEYWORDS : Fake Diploma; Defamation; Constitutional Court Decision; Data Integrity.

INTRODUCTION

Digital transformation has fundamentally reshaped the nature of legal documents within modern legal systems (Susskind, 2023). Diplomas, once understood as physical documents authenticated through holograms and handwritten signatures, have evolved into electronic information whose validity depends on the integrity of digital systems (Rehman Khan & Ahmad, 2022). Within the telematics legal framework, a diploma is no longer merely a material artifact but a structured set of electronic data whose authenticity relies on authentication mechanisms, encryption protocols, and validation processes embedded in nationally integrated educational information systems.

This shift in medium carries significant juridical consequences, particularly in matters of evidentiary standards and legal certainty. While digitalization enables more efficient and transparent verification, it simultaneously opens space for disputes over data

authenticity in cyberspace (Herawati, 2025). Legal tension arises when members of the public who question or verify the integrity of diploma data are confronted with potential criminal liability under Article 27A of the Electronic Information and Transactions Law (Octora, 2022).

This situation generates a normative dilemma: does questioning the validity of electronic data relating to a public official constitute an attack on personal honor, or is it merely an attempt to test the reliability of an information system? The absence of a clear demarcation risks producing a chilling effect on freedom of expression and weakening the function of social oversight in a digital society.Therefore, diplomas must be conceptually positioned as objects of electronic information subject to verification. Criticism directed at document validity cannot automatically be equated with an attack on the dignity of the individual concerned. Without a clear distinction between object and subject, law enforcement risks blurring constitutional protections for freedom of expression.

Legal conflict, recent legal practice demonstrates a sharp tension between the public's right to exercise social control and the protection of individual dignity within defamation law. When efforts to verify the authenticity of a public official's educational credentials are met with criminal complaints under cyber defamation provisions, law shifts from a protective instrument into a restrictive one. Such criminalization is not merely a technical issue of overlapping norms but raises concerns about the foundations of digital democracy. When individuals refrain from questioning the authenticity of public data due to fear of prosecution, public discourse is effectively suppressed. From a telematics law perspective, a diploma constitutes electronic information whose integrity must be open to verification (Syafwar, 2025a). If every inquiry into data validity is interpreted as defamation, the legal system risks creating zones of impunity for public office holders (Umaña Hernández, 2022).

This complexity is exacerbated by overlapping interpretations between the Electronic Information and Transactions Law and the Personal Data Protection Law (Ghufron Rosadi Hidayah et al., 2025). In the absence of clear normative parameters, law enforcement authorities frequently fail to distinguish between criticism directed at a digital object and an attack on personal character (Muhammad Jarnawansyah, 2025). Logically and systematically, verification of document authenticity should precede any assessment of reputational harm (Dharmawan et al., 2024).

In this regard, Constitutional Court Decision No. 104/2024 constitutes a pivotal development. The Court clarified that defamation offenses are inherently personal and may only attach to human beings as legal subjects possessing dignity and honor (Herlina, 2025). The validity of a document cannot be equated with the honor of its holder. Conceptually, within the telematics framework, a diploma is an electronic information object whose integrity is binary either valid or invalid based on digital verification mechanisms (Shuban et al., 2024). When its authenticity is questioned, the focus lies on the quality of the data and the reliability of the authentication system, not on human dignity. The Constitutional Court's ruling provides a crucial normative demarcation: testing the integrity of data does not constitute an attack on personal honor. If this boundary is consistently upheld, social oversight can function without criminalization, while the protection of individual dignity remains safeguarded within constitutional limits.

This interpretation is highly consequential for our legal ecosystem. Without a clear distinction between objects and persons, law enforcement authorities risk becoming entangled in the subjective perceptions of complainants who claim to feel insulted merely

because the validity of their data has been questioned (Clifford, 2024). The Constitutional Court's ruling compels investigators to prioritize substance: is the matter under dispute the factual accuracy of a document, or merely an unfounded verbal attack? Accordingly, Decision No. 104/2024 provides a normative foundation for requiring administrative verification through governmental telematics systems (such as SIVIL) to be conducted first, in order to ensure data integrity before entering the domain of criminal defamation.

Previous scholarship demonstrates that allegations of fake diplomas have predominantly been framed within the context of criminal forgery rather than constitutional debates concerning the limits of criticism toward public documents. Gunawan and Bayu Aji (2025) argue that accusations regarding President Joko Widodo's diploma lacked legal basis because the elements of Article 263 of the Indonesian Criminal Code were not fulfilled and the document's authenticity had been verified by the issuing institution (Gunawan & Aji, 2025b). Safitri, Firganefi, and Tamza (2024), as well as Simbolon and Nababan (2025), similarly focus on criminal liability for the use of fake diplomas through analysis of judicial decisions (Safitri et al., 2024; Simbolon & Nababan, 2025). These studies concentrate on the construction of criminal offenses and judicial reasoning in sentencing, rather than addressing whether questioning the authenticity of a diploma can be legally characterized as an attack on the individual's honor.

On the other hand, Sugitanata (2025) approaches the alleged fake diploma controversy of a former president as a matter of constitutional legitimacy and public trust in state institutions (Sugitanata, 2025), while Rahman (2025) examines academic degree manipulation from a legal policy perspective, emphasizing regulatory reform (Rahman, 2025). Although these studies broaden the discourse into constitutional and legislative policy dimensions, they do not explicitly distinguish between the object under scrutiny the diploma as document or data and the legal subject who may claim reputational harm. Consequently, the existing literature leaves a conceptual gap regarding whether verification or testing of a public official's educational credentials may be equated with defamation, particularly after Decision No. 104/2024 clarified the separation between the object of defamation and the legal subject.

In contrast to the prevailing literature, which remains confined to the dichotomy of document forgery (criminal fraud) or political legitimacy debates, this study advances a more fundamental and telematics-specific inquiry. Its principal novelty lies in synchronizing the concept of Electronic Data Integrity under the Electronic Information and Transactions Law and the Personal Data Protection Law with the ratio decidendi of Constitutional Court Decision No. 104/2024.

This research explores a largely overlooked legal dimension: the paradigm shift from physical document examination to the audit of digital data bits. Whereas prior studies emphasize criminal responsibility of diploma holders, this study centers on legal protection for those conducting verification by drawing a firm distinction between diplomas as objects of digital information and human dignity as a legal subject. In doing so, the article fills a conceptual void by asserting that, within a telematics ecosystem, verification of data authentication constitutes a technical-legal act that cannot be criminalized as an attack on personal honor.

Research Problem**, a**gainst the backdrop of growing criminalization of efforts to verify public data, this study focuses on two critical determinants for the future enforcement of telematics law. First, there is an urgent need to redefine the juridical qualification of questioning diploma authenticity in cyberspace. The central issue is whether statements concerning a "fake diploma" constitute a form of testing electronic data integrity as envisioned by the Electronic Information and Transactions Law and the

Personal Data Protection Law, or whether they amount purely to an attack on personal honor. This distinction is essential to differentiate between discourse on digital facts and the inherently subjective offense of defamation.

Second, this study further examines the juridical implications of Constitutional Court Decision No. 104/2024 in delineating the boundary between criticism directed at the validity of a document as an object and attacks on human dignity as a legal subject. The core issue lies in how to reconcile the right to public information concerning the educational credentials of public officials with the privacy protections enshrined in the Personal Data Protection Law, without undermining legal certainty for citizens performing their social control function. Through these two analytical pillars, this article seeks to formulate precise parameters for law enforcement authorities in handling information disputes within the telematics era.

By dissecting these two central problems, the article endeavors to construct a more proportionate understanding of the limits of criminal offenses in digital spaces. The expected outcome is a legal framework capable of safeguarding individual dignity in a balanced manner while simultaneously ensuring protection for data integrity and transparency of public information. Ultimately, the harmonization of the Electronic Information and Transactions Law, the Personal Data Protection Law, and the constitutional guidance articulated by the Constitutional Court constitutes the principal foundation for resolving the dilemma of criminalization surrounding diploma verification in the telematics age.

RESEARCH METHOD

This study employs a normative juridical legal research method focused on the examination of positive law and the identification of underlying legal principles within telematics regulation. Through a statute approach, the analysis explores the synchronization between the Electronic Information and Transactions Law and the Personal Data Protection Law in order to determine the legal status of diplomas as electronic information possessing data integrity.

In addition, a case approach is applied through an in-depth analysis of the ratio decidendi of Constitutional Court Decision No. 104/2024. This approach is essential to establish a clear demarcation between the object of an offense, understood as amaterial or digital object, and the legal subject endowed with personal dignity. Secondary data consisting of primary legal materials (statutes and judicial decisions) and secondary materials (academic literature) are analyzed qualitatively using deductive reasoning. This method is selected to reconstruct a more proportionate legal understanding in addressing the dilemma of criminalization related to the verification of public data in cyberspace.

ANALYSIS AND DISCUSSION

Normative Analysis of Constitutional Court Decision No. 104/2024: Separating Documentary Objects from Legal Subjects

At the core of the normative analysis lies the need to examine how Constitutional Court Decision No. 104/PUU-XXI/2024 functions as a catalyst for a paradigm shift in the law of defamation within digital spaces. For years, a persistent conceptual confusion has blurred the distinction between the legal subject and the informational object. This article seeks to clarify that demarcation: defamation is inherently personal and inseparably attached to human dignity, not to the validity of an object or document.

Within a broader telematics law perspective, a diploma must be clearly positioned as

an electronic document an object of information rather than a bearer of personality (Boiko, 2024). Technically, a diploma represents the digital manifestation of an academic fact (Babu et al., 2025). When an individual questions or alleges that a diploma is falsified, the juridical target of such a statement is the authentication of data or the validity of the document itself (Gunawan & Aji, 2025a). The critical misunderstanding often made by law enforcement authorities is equating scrutiny of a document's authenticity with an attack on the moral character or personal integrity of its holder (Syafwar, 2025a). These are analytically distinct acts.

Referring to the revised Article 27A of the Electronic Information and Transactions Law, the element of "attacking honor or reputation" requires the presence of malicious intent (mens rea) directed at degrading a person's dignity (Viko Musadad & Chepi Ali Firman Zakaria, 2024). However, when the dispute concerns the validity of an object or the integrity of a set of digital bits, the element of personal attack is legally inapplicable (Sandro, 2018; Yoshino, 2007). Conceptually and ontologically, a document does not possess emotional agency or intentional states; it cannot experience humiliation or reputational harm (Deigh, 2010; Svašek, 2024). A diploma functions as evidentiary material. Consequently, any inconsistency between a claimant's assertion and official database records—such as those maintained in national information systems constitutes an administrative or data-integrity issue rather than a criminal defamation offense (Gunawan & Aji, 2025b).

The separation between object and subject also serves as a safeguard for responsible freedom of expression (Mamarasulov, 2022). Citizens are entitled to ensure that public data presented by state officials are authentic and verifiable (OECD, 2024). If every act of verifying a digital document is construed as an insult to its holder, the legal system risks elevating administrative claims to untouchable status, thereby undermining democratic accountability (Gstrein & Kochenov, 2020). Constitutional Court Decision No. 104/2024 reorients criminal law toward proportionality, reaffirming that penal sanctions operate as ultimum remedium and may only be invoked where genuine human dignity is attacked, not where documentary validity is examined (Ginting, 2024).

Accordingly, this analysis affirms that within the telematics ecosystem, a diploma must be treated as an informational entity distinct from the legal personality of its holder. Challenging the authenticity of a diploma constitutes a legitimate act of information audit under the law. Without a firm demarcation between attacks on "objects" and attacks on "persons," telematics law risks devolving into an instrument that suppresses factual scrutiny rather than facilitating truth verification in the public sphere

Diploma Data Integrity under the PDP and EIT Regimes: Between Privacy and Public Accountability

A deeper examination is required to unpack the tension between individual privacy protection and the demand for public accountability through the lens of telematics law. In the digital era, a diploma has transformed from a physical document into a set of electronic information bits of data whose legal value depends on systemic integrity. Under the Electronic Information and Transactions Law (EIT Law), the integrity of electronic information constitutes a foundational principle: data must be authentic, complete, and verifiable within a reliable information system from creation to storage and retrieval (Smith, 2023). Integrity, therefore, is not merely technical compliance but a juridical condition for legal certainty.

The issue becomes more complex when viewed alongside the Personal Data Protection Law (PDP Law). Educational data, including graduation information reflected in

a diploma, qualifies as personal data. This classification is frequently invoked as a protective shield to restrict public access to verification processes under the banner of privacy. Yet, privacy rights are not absolute; they operate within a framework of proportionality and legitimate public interest (Chaandra, 2025). The PDP Law itself permits the processing of personal data for public interest purposes or to fulfill legal obligations prescribed by legislation (Siti Yuniarti, 2022). Thus, privacy must be interpreted within a structured balancing test rather than as an impenetrable barrier.

For public officials or candidates for public office, a diploma transcends the sphere of purely private information and becomes an instrument of public accountability (Syafwar, 2025b). The legal dialectic lies in determining the appropriate threshold at which personal privacy yields to the public's right to accurate and verifiable information. From a telematics perspective, questioning the integrity of diploma data constitutes an act of informational audit. If the diploma is valid and duly recorded within a national education database, verification should operate as an objective and binary administrative procedure valid or invalid, registered or unregistered (Saryoko et al., 2024).

Nevertheless, societal attempts to exercise oversight are often met with the threat of criminalization. A persistent misconception equates any scrutiny of personal data even for the purpose of verifying a document relevant to public office with an attack on personal honor (Gohi & Bujad, 2022). Such reasoning neglects the accountability principle embedded in both the PDP and EIT frameworks. Individuals occupying public office bear not only moral but also juridical responsibility to ensure the authenticity and integrity of their official credentials (Mahpudin & Ahmad Tazzul Aripin, 2025). Invoking privacy to obstruct legitimate verification risks undermining the credibility of the information system itself (Surendrababu, 2022).

An ideal legal construction should therefore recognize diploma data integrity as a publicly examinable object when it relates to public office qualifications (Muhammad Jarnawansyah, 2025). A clear distinction must be drawn between privacy safeguarding an individual's domestic sphere and accountability attached to formal qualifications presented before the state. Without transparent telematics mechanisms enabling verification, the PDP and EIT regimes may inadvertently function as instruments shielding administrative dishonesty rather than protecting personal data (Carmo & Prastyanti, 2025). Harmonization between these statutes must thus aim at equilibrium: privacy remains protected, yet it cannot operate as an impediment to public truth, informational transparency, and the integrity of national data systems

Adjudicative Dilemma: Evidentiary Parameters for Alleged Fake Diplomas Without Criminalization

As this analysis approaches its concluding section, attention must turn to the courtroom reality: the adjudicative dilemma. The most pressing challenge confronting judges and law enforcement officials is the formulation of fair evidentiary parameters without sacrificing citizens' constitutional right to freedom of expression. In practice, a recurrent logical shortcut is observable courts often move directly from questioning a document to concluding defamation, without first undertaking a proper data audit (Herman & Anatasya, 2024). This procedural leap distorts both evidentiary reasoning and proportionality in criminal law.

The root of the dilemma lies in the formal legal system's failure to distinguish between factual inaccuracy and malicious intent. In cases involving allegations of a fake diploma, adjudication should begin by examining the material truth of the disputed object the diploma itself as electronic data (Király, 2017). Evidentiary standards must not hinge on

the subjective feeling of offense by the complainant but rather on objective verification within a telematics system (University of Kragujevac, Faculty of Law, Serbia & Turanjanin, 2024). When a citizen questions the authenticity of a public official's diploma based on the absence or inconsistency of data in official databases (such as SIVIL), that conduct should be interpreted as an attempt to ascertain factual accuracy, not as an attack on personal honor.

To prevent overcriminalization, adjudication must incorporate the principle of *exceptio veritatis* the defense of truth (Charney, 2016). Where a statement is grounded in rational argumentation or supported by indicia of irregularities within an electronic system, the defamatory element under Article 27A of the EIT Law cannot be deemed fulfilled (Suhandry Aristo Sitanggang et al., 2025). Constitutional Court Decision No. 104/2024 serves as a normative anchor: the judiciary must distinguish between an attack on an object (the integrity of a document) and an attack on a person (personal dignity). Criminally prosecuting an individual for questioning a public document's validity without first establishing the document's factual authenticity constitutes a procedural misstep incompatible with modern evidentiary logic (Siswandi et al., 2025).

Moreover, evidentiary parameters must account for the public interest dimension. Within telematics law, the diploma of a public official is not merely private data; it carries a social function (Syafwar, 2025c). Consequently, the burden of proof should not rest exclusively upon the questioning citizen. The diploma holder particularly when occupying public office bears a corresponding responsibility to demonstrate data transparency through legitimate authentication systems (Kazan, 2022). A balanced adjudicative framework requires differentiating between criticism of defective "bits of data" and indiscriminate character attacks. Such differentiation significantly reduces the risk of criminalizing legitimate social oversight (Alqudah et al., 2024).

Ultimately, resolving this adjudicative dilemma demands judicial courage and doctrinal clarity. Judges must resist rigid textualism and instead approach these disputes through an objective telematics lens. In the digital era, data validity underpins public trust. Evidentiary standards must shift from the subjective metric of wounded honor to the objective verification of informational truth. Only through this recalibration can the legal system simultaneously safeguard human dignity and preserve the critical scrutiny necessary to uphold the integrity of public documents

CONCLUSION AND RECOMMENDATIONS

Conclusion

Based on the comprehensive analysis presented, this study arrives at two principal conclusions. First, within the telematics legal framework, a diploma has evolved into a digital asset, essentially a configuration of electronic data whose validity depends on the integrity of the information system that records and authenticates it. Although a diploma constitutes personal data under the Personal Data Protection Law (PDP Law), its function as a formal qualification for public office necessitates a higher threshold of transparency and accountability than that ordinarily attached to private data. Verifying the integrity of such data must therefore be understood as a legitimate and rational administrative procedure within the rule of law.Second, Constitutional Court Decision No. 104/2024 provides a decisive juridical clarification by establishing a firm demarcation between the object of a document and the subject of law. Defamation, by its nature, attaches exclusively to human dignity. Accordingly, a statement questioning the authentication of a diploma as an object or digital entity cannot automatically be construed as an attack on personal

honor. Where allegations of a fake diploma are grounded in inconsistencies within official information systems and are not directed at degrading personal character, the element of "attacking honor" under Article 27A of the EIT Law cannot be deemed fulfilled as a matter of law.

Recommendations

To Law Enforcement Authorities: A paradigm shift is required in handling defamation complaints related to diploma authenticity. Investigators and prosecutors should prioritize factual verification (*exceptio veritatis*) through a systematic audit of government telematics databases before proceeding with criminal prosecution. The assessment must begin with the integrity of the electronic data, not with the subjective perception of offense. To the Government: There is an urgent need to strengthen and harmonize the national educational data infrastructure into an integrated, reliable, and publicly verifiable system. Transparent verification mechanisms will reduce legal disputes and prevent the misuse of criminal law as an instrument to suppress legitimate social oversight in the digital era

REFERENCES:

Alqudah, M., Al-Amawi, A., Khashashneh, T., & Balas, H. (2024). The crime of character assassination in the Jordanian cybercrime law. *International Journal of Religion, 5*(10), 3671–3684. https://doi.org/10.61707/gsfk2s22

Ary Syadewa, Azhari, M. S., Aghitsa, M. R., & Yusufa, F. (2025). Keabsahan akta autentik digital (cyber notary) dalam penyelesaian sengketa di pengadilan. *Indonesian Journal of Islamic Jurisprudence, Economic and Legal Theory, 3*(2), 2015–2030. https://doi.org/10.62976/ijijel.v3i2.1203

Babu, S., Anbumozhi, A., S., P., N., V., & Kaliamoorthy, V. (2025). Blockchain for credentialing and academic record-keeping. In J. Moore, S. Gupta, M. Sharma, A. Garg, & H. J. V. L. Josephine (Eds.), *Advances in computational intelligence and robotics* (pp. 407–448). IGI Global Scientific Publishing. https://doi.org/10.4018/979-8-3373-2185-1.ch014

Boiko, O. (2024). Electronic document: Domestic and international experience of information storage. *Visnyk of Kharkiv State Academy of Culture, 65*, 25–36. https://doi.org/10.31516/2410-5333.065.02

Carmo, G. M. D., & Prastyanti, R. A. (2025). Tinjauan yuridis atas penyalahgunaan data pribadi dalam transaksi elektronik berdasarkan Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi. *El-Mujtama: Jurnal Pengabdian Masyarakat, 5*(4). https://doi.org/10.47467/elmujtama.v5i4.7988

Chaandra, R. (2025). Right to privacy vs. right to public health: A debatable question of supremacy. *International Journal for Multidisciplinary Research, 7*(4), 49299. https://doi.org/10.36948/ijfmr.2025.v07i04.49299

Charney, J. (2016). The tensions between free speech and the protection to one's reputation: Importance and limits of the exceptio veritatis. *Revista de Derecho, 29*(2), 175–193. https://doi.org/10.4067/S0718-09502016000200008

Clifford, D. (2024). Conclusion. In *Data protection law and emotion* (pp. 219–228). Oxford University Press. https://doi.org/10.1093/oso/9780192845863.003.0007

Deigh, J. (2010). Concepts of emotions in modern philosophy and psychology. In *The Oxford handbook of philosophy of emotion*. Oxford University Press. https://doi.org/10.1093/oxfordhb/9780199235018.003.0002

Dharmawan, M. A., Faziya, A. D., Salsabillah, S. K., Sadrianoor, S., & Apriyani, R. (2024). Perbedaan perbuatan merendahkan kehormatan dan keluhuran martabat hakim dengan contempt of court dalam sistem peradilan Indonesia. *Nomos: Jurnal Penelitian Ilmu Hukum, 5*(1), 14–19. https://doi.org/10.56393/nomos.v5i1.2512

Ghufron Rosadi Hidayah, Djazim Ma'shum, H., & Awaluddin, M. (2025). Studi komparatif perlindungan data pribadi dalam UU ITE 2024 dan UU PDP 2022. *Jurnal Riset Rumpun Ilmu Sosial, Politik dan Humaniora, 4*(4), 61–70. https://doi.org/10.55606/jurrish.v4i4.6341

Ginting, Y. (2024). Penyelesaian perkara pidana di luar pengadilan berdasarkan asas ultimum remedium. *The Prosecutor Law Review, 2*(1). https://doi.org/10.64843/prolev.v2i1.32

Gohi, M. S. L., & Bujad, C. (2022). Data ownership: A mistaken perspective to protection of data privacy. *Towards Excellence*, 458–464. https://doi.org/10.37867/TE140143

Gstrein, O. J., & Kochenov, D. (2020). Digital identity and distributed ledger technology: Paving the way to a neo-feudal brave new world? *Frontiers in Blockchain, 3*, 10. https://doi.org/10.3389/fbloc.2020.00010

Gunawan, G., & Aji, R. B. (2025). Kontroversi ijazah Joko Widodo: Antara tuduhan palsu dan fakta hukum yang terverifikasi. *Law and Humanity, 3*(2), 139–152. https://doi.org/10.37504/lh.v3i2.739

Herawati, K. M. (2025). Legal challenges and opportunities in the digitalization era. *Formosa Journal of Science and Technology, 4*(7), 2213–2222. https://doi.org/10.55927/fjst.v4i7.189

Herlina, S. (2025). Criminal defamation through social media and its legal implications in Indonesia. *International Journal of Law, Environment, and Natural Resources, 5*(1), 83–98. https://doi.org/10.51749/injurlens.v5i1.142 Herman, H., & Anatasya, A. E. F. (2024). Analisis kasus defamasi melalui Instagram yang menyerang lembaga kepolisian berdasarkan putusan Nomor 58/Pid.Sus/2021/PN.SDR. *Khatulistiwa Law Review, 3*(1), 444–468. https://doi.org/10.24260/klr.v3i1.3563

Kazan, R. (2022). Diploma verification using blockchain technology. *AURUM Journal of Engineering Systems and Architecture*. https://doi.org/10.53600/ajesa.1065827

Király, L. (2017). Access to information and evidence on the basis of the draft bill on the new code of civil procedure. *Hungarian Journal of Legal Studies, 58*(1), 51–78. https://doi.org/10.1556/2052.2017.58.1.4

Law Faculty, Universitas Kristen Maranatha, & Octora, R. (2022). Criminalization of the action of submitting criticism to the government based on the Electronic

Information and Transaction Law in Indonesia, and protection of the right to freedom of speech in a democratic country. *International Journal of Social Science and Human Research, 5*(5). https://doi.org/10.47191/ijsshr/v5-i5-46 Mahpudin, M., & Aripin, A. T. (2025). Akuntabilitas Komisi Pemilihan Umum Kota Serang dalam mengatasi pencatutan data masyarakat secara ilegal melalui

sistem informasi partai politik (SIPOL) pada Pilkada tahun 2024. *Jurnal Silatene Sosial Humaniora, 3*(1), 1–9. https://doi.org/10.53611/d8065b02

Mamarasulov, A. R. (2022). Problems of definition of freedom through the concept of responsibility. *Философская Мысль*, (9), 25–43. https://doi.org/10.25136/2409-8728.2022.9.38847

Muhammad Jarnawansyah. (2025). Tindak pidana pemalsuan ijazah dalam perspektif hukum pidana Indonesia. *Journal of New Trends in Sciences, 3*(3), 41–55. https://doi.org/10.59031/jnts.v3i3.734

OECD. (2024). *Government at a glance: Latin America and the Caribbean 2024*. OECD Publishing. https://doi.org/10.1787/4abdba16-en

Rahman, F. Z. (2025). Kebijakan hukum terhadap fenomena manipulasi gelar akademik di Indonesia. *Mavisha: Law and Society Journal, 2*(1). https://doi.org/10.15408/bycssa97

Rehman Khan, A. U., & Ahmad, R. W. (2022). Blockchain-based academic degrees issuance and attestation. In *2022 International Conference on IT and Industrial Technologies (ICIT)* (pp. 1–6). IEEE. https://doi.org/10.1109/ICIT56493.2022.9989203

Safitri, W. F., Firganefi, F., & Tamza, F. B. (2024). Responsibility of perpetrators of the criminal act of using fake diplomas in the nomination of legislative members (Study of Decision No. 105/PID/2021/PT.TJK jo. Decision No. 43/PID/2021/PN LIW). *Multidisciplinary Journals, 1*(4), 251–258. https://doi.org/10.37676/mj.v1i4.638

Sandro, P. (2018). Unlocking legal validity: Some remarks on the artificial ontology of law. In *Law and Philosophy Library* (Vol. 122, pp. 99–123). Springer. https://doi.org/10.1007/978-3-319-77522-7_5

Saryoko, A., Saputra, I., Sumanto, Budihartanti, C., Masturoh, S., Wahyudi, M., Nainggolan, E. R., Nurlela, S., & Sutedja, I. (2024). A conceptual model for diploma verification in education: Leveraging NFTs and dynamic smart contracts. In *2024 International Conference on Information Technology Research and Innovation (ICITRI)* (pp. 82–87). IEEE. https://doi.org/10.1109/ICITRI62858.2024.10699024

Shuban, E. Z., Indrawan, K. W., & Edbert, I. S. (2024). Blockchain implementation to ensure the authenticity and integrity of graduation and diploma certificates. In *2024 International Conference on Artificial Intelligence, Blockchain, Cloud Computing, and Data Analytics (ICoABCD)* (pp. 113–118). IEEE. https://doi.org/10.1109/ICoABCD63526.2024.10704330

Simbolon, H. N., & Nababan, R. (2025). Analisis yuridis terhadap tindak pidana penggunaan ijazah palsu: Studi putusan Nomor 1583/Pid.Sus/2021/PT.MDN. *As-Syar'i: Jurnal Bimbingan & Konseling Keluarga, 7*(1), 21–34. https://doi.org/10.47467/as.v7i1.5631

Siswandi, L., Suprayitno, P. H., & Sholahuddin, M. (2025). Analisa terhadap pidana pemalsuan ditinjau dari KUHP dan KUHAP yang berakibat terhadap hukum tata negara yang berlaku di Indonesia. *Jurnal Yustitia, 26*(1). https://doi.org/10.53712/yustitia.v26i1.2672

Siti Yuniarti. (2022). Protection of Indonesia's personal data after ratification of personal data protection act. *Progressive Law Review, 4*(2), 54–68. https://doi.org/10.36448/plr.v4i02.85

Smith, K. (2023). Ensuring data integrity in modern information systems. *Open Science Framework*. https://doi.org/10.31219/osf.io/z5kt7

Sugitanata, A. (2025). Kontroversi dugaan ijazah palsu mantan presiden dalam bingkai hukum tata negara. *Al-Balad: Jurnal Hukum Tata Negara dan Politik Islam, 5*(1), 38–54. https://doi.org/10.59259/ab.v5i1.243

Suhandry Aristo Sitanggang, T. Arifin, & I. Fauzia. (2025). Kebebasan berpendapat dan jerat digital: Analisis nullum crimen sine lege dalam Pasal 27 ayat (3) Undang- Undang ITE dan relevansinya dengan Pasal 19 Deklarasi Universal Hak Asasi Manusia. *As-Syar'i: Jurnal Bimbingan & Konseling Keluarga, 7*(1), 267–277. https://doi.org/10.47467/as.v7i1.6423

Surendrababu, H. K. (2022). System integrity – A cautionary tale. In *2022 IEEE Physical Assurance and Inspection of Electronics (PAINE)* (pp. 1–6). IEEE. https://doi.org/10.1109/PAINE56030.2022.10014826

Susskind, R. (2023). Disruptive legal technologies. In *Tomorrow's lawyers* (3rd ed., pp. 63–78). Oxford University Press. https://doi.org/10.1093/9780192864727.003.0007

Svašek, M. (2024). Moving corpses: Emotions and subject-object ambiguity. In *The emotions: A cultural reader*. Taylor & Francis. https://doi.org/10.4324/9781003579557-21

Syafwar, R. (2025). Personal data protection and disclosure of information on public officials' diplomas: A legal review in Indonesia. *Jurnal Ilmiah Ekotrans & Erudisi, 5*(1), 111–119. https://doi.org/10.69989/0gt8q135

Umaña Hernández, C. E. (2022). Impunity as a sanctuary. *Oñati Socio-Legal Series, 12*(4), 981–1000. https://doi.org/10.35295/osls.iisl/0000-0000-0000-1316 University of Kragujevac, Faculty of Law, & Turanjanin, V. (2024). Interception of communications in criminal proceedings and proving the rape. In *Međunarodna Naučna Konferencija Izazovi i Otvorena Pitanja Uslužnog Prava - Tom2* (pp. 413–440). https://doi.org/10.46793/XXMajsko2.413T

Viko Musadad, & Zakaria, C. A. F. (2024). Pencemaran nama baik sebagai tindak pidana berdasarkan KUHP dan Undang-Undang ITE. *Bandung Conference Series: Law Studies, 4*(1), 722–729. https://doi.org/10.29313/bcsls.v4i1.12446

Yoshino, H. (2007). Logical structure of change of legal relations and its representation in legal knowledge base system. In *Proceedings of the International Conference on Artificial Intelligence and Law* (pp. 91–92). Association for Computing Machinery. https://doi.org/10.1145/1276318.1276334