JURNAL SYNTAX TRANSFORMATION
Printed ISSN: 2721-3854 | Electronic ISSN: 2721-2769

Volume 7, No. 6 June, 2026
p-ISSN 2721-3854 | e-ISSN 2721-2769

Disparity in Law Enforcement in The Crime of Electronic Information Theft

Iqbal Maulana Ghozi, Endang Sutrisno
Universitas Swadaya Gunung Jati, Indonesia
Email: ghojicirebon@gmail.com, Endang.Sutrisno@ugj.ac.id

Keywords:
Criminal Disparity; Electronic Information; Legal Certainty

Abstract

The rapid digital transformation of society has increased cybercrime incidents significantly, particularly electronic information theft, raising concerns over legal certainty and equal law enforcement in Indonesia. This study aims to analyze disparities in the enforcement of electronic information theft cases within the Indonesian criminal justice system. A normative juridical method with a qualitative descriptive approach was employed, using literature study, statutory analysis, and comparative case review. The findings show that enforcement disparities are influenced by ambiguous legal norms, uneven digital forensic infrastructure, differences in judges' digital literacy, and centralized case handling in major cities. Case comparisons between Banjarmasin, South Jakarta, and Yogyakarta reveal significant sentencing variations for similar cybercrime acts. These inconsistencies indicate the absence of standardized sentencing guidelines and unequal evidentiary capacities across jurisdictions. Consequently, such disparities undermine legal certainty and public trust in cyber law enforcement. The study concludes that structural reforms, including the harmonization of legal interpretation, the standardization of sentencing guidelines, and the equitable distribution of forensic technology, are urgently needed to ensure fair and consistent justice in electronic information crime cases. These reforms are essential to strengthen legal certainty, deterrence, and public confidence in Indonesia's digital justice system and to support equitable access to justice across regions nationwide.

INTRODUCTION

Our lives today have almost completely shifted to the digital space, which unfortunately also opens up wide gaps for the emergence of new crimes. Ideally, the state should provide legal protection that is fair and indiscriminate for every citizen, in accordance with the mandate of Article 28G paragraph (1) of the 1945 Constitution regarding the right to a sense of security and personal self-protection (Priyanjani et al., 2024). The presence of Law No. 1 of 2024 on the ITE Law and the Personal Data Protection Law (PDP Law) should be a strong legal umbrella to ensure that every case of electronic information theft is handled with the same standards of justice (Priyanjani et al., 2024). As emphasized by Endang Sutrisno, the presence of a legal instrument actually carries out a sacred mission to achieve justice, certainty, and social benefits in a balanced manner, where the legal system must not only stop at the text of regulations but must be proven through the performance of its enforcement in the field (Sutrisno, 2010). This certainty is important so that people feel calm when interacting in the digital world, without worrying about their digital rights being ignored by the legal system.

However, the reality on the ground is different: cyberattacks in Indonesia have actually jumped sharply in a short time. Based on records from the State Cyber and Cryptography Agency (BSSN), there were around 3.64 billion cyberattack incidents from January to July 2025 alone, a fantastic number that almost equals the total accumulated attacks over the last five years (Defara, 2025). Most of these attacks are malware that targets people's financial data and personal identities (Verihubs.com, 2026). The rise in these cases indicates that digital threats are no longer just a potential but a real daily risk, while the readiness of our law enforcement system continues to be tested by the massive volume of incoming cases (Unesa.ac.id, 2025).

Ironically, the speed and rigor of the law in handling these cases are often determined by where the cases are reported. Data from the Indonesian National Police shows a striking inequality, where the Metro Jaya Police handled up to 3,709 cyber cases in 2022, while the Regional Police in other regions handled fewer cases or even encountered a dead end (Directorate of Cyber Crime of the Criminal Investigation Branch of the National Police, 2023). This phenomenon creates the impression that there is a center and a periphery in access to digital justice. Local communities often have to wait longer or even lose hope because the investigation process is very slow compared to the handling in the capital city (Directorate of Cyber Crime of the Criminal Investigation Branch of the National Police, 2023).

This problem is even more complicated because of the difference in technological capacity and digital forensic capabilities in each police unit. Cyber case investigations require sophisticated tools and special expertise to maintain the integrity of digital evidence so that it is not damaged (Cahyono, Tri, Erni, and Hidayat, 2025). Unfortunately, many cyber units at the regional level do not have adequate forensic tools, so they have to fully rely on the support of the Criminal Investigation Agency in Jakarta. In addition to infrastructure, the digital literacy of the apparatus is also a big obstacle. There are still many prosecutors and judges in the regions who feel doubtful or confused in assessing the validity of electronic evidence, so they prefer to rely on conventional evidence that is less relevant in cybercrime (Aini and Lubis, 2024).

Legal loopholes also arise from the interpretation of criminal articles, which are often considered to be gray. In the PDP Law and the 2024 ITE Law, terms such as without rights or against the law are not explained in detail, thus leaving room for law enforcement to interpret them subjectively (Fikriansyah & Harris, 2026). This ambiguity often leads to confusion in determining who is most criminally responsible, especially in cases of big data leaks such as the one that has befallen BPJS. Without strict limits on the elements of crime, law enforcement becomes inconsistent and vulnerable to off-target criminalization (Amuedo-Dorantes et al., 2019; Bethune, 2015; Hurst et al., 2018; Ulmer, 2019).

Although regulations have been updated many times, the issue of law enforcement disparity is still a huge hole that is rarely discussed in depth. This study found a research gap in which the update of the rules in the 2024 ITE Law has not been able to touch the root of the technical and coordination problems in the field that cause inequality in case handling (Andhitya and Umam, 2025). If this disparity is allowed to continue, public trust in the national cyber legal system will collapse, which in turn can disrupt the stability of Indonesia's digital economy (Anggono et al.,

2025; Hafel, 2023; Handayani et al., 2025). Investors and business actors will certainly feel hesitant to operate in an environment where data protection is considered unpredictable and inconsistent. In this regard, a fundamental problem arises, namely: How does the disparity occur in relation to law enforcement for the theft of electronic information?

Based on these legal problems, this study aims to further dissect the legal issues that cause the disparity in law enforcement in the crime of electronic information theft. By understanding the root of the problem, it is hoped that this study can formulate concrete recommendations in the form of the standardization of operational capacity and more uniform prosecution guidelines. The ultimate goal is to create a fair justice system, where every individual gets equal protection, without being hindered by infrastructure limitations or differences in legal interpretation.

METHOD

In tracing the root of the problem of inequality in law enforcement in cybercrime, the research relies on a normative juridical approach. This approach was chosen because its main focus is to examine the synchronization between applicable legal instruments, especially Law Number 1 of 2024 concerning the second amendment to the ITE Law and the PDP Law, and its application in judicial practice. Through this approach, the research dissects the legal norms, principles, and doctrines in the literature to see how the text of the law that seems to be multi-interpreted interacts with the reality of criminal disparities in the courtroom. In line with that, the type of research used is qualitative with descriptive-analytical specifications. The description presented does not only explain a series of numbers related to the surge in cybercrime incidents, but also seeks to comprehensively describe how the condition of law enforcement infrastructure and the disparity in verdicts between regions really occurs. The facts raised, such as the striking differences between the verdict at the Banjarmasin District Court and the South Jakarta District Court for similar data manipulation cases, were then analyzed in depth to reveal the meaning behind the inconsistency of the judge's interpretation and the limited forensic capacity of the apparatus. Thus, this study not only answers the problems that are happening, but also unravels the reasons why these inconsistencies can persist.

The data collection process relies on a literature study involving two pillars of legal material sources, namely primary legal materials and secondary legal materials. The primary legal material consists of regulations that have binding authority, which in this context includes the 1945 Constitution of the Republic of Indonesia as well as sectoral legal instruments related to electronic information such as the ITE Law and the PDP Law. Meanwhile, secondary legal materials are used to provide explanations or critical perspectives on primary materials, which include academic literature, cybercrime reference books, relevant previous journal articles, as well as the doctrinal views of experts closely related to the theory of legal certainty and criminal disparity.

RESULTS AND DISCUSSION

The Reality of Cyber Law Enforcement Disparities and Its Implications for Legal Certainty

The fundamental transformation of society toward the digital era has brought a significant paradigm shift in the Indonesian criminal law spectrum. A life that has almost completely migrated to cyberspace not only offers efficiency but also opens a Pandora's box for the emergence of new variants of highly technical and cross-border crime. Ideally, the state has a constitutional obligation to provide definite and indiscriminate legal protection for every citizen, as mandated in Article 28G paragraph (1) of the 1945 Constitution, which guarantees the right to a sense of security and personal protection. However, in practice, law enforcement against cybercrimes, especially electronic information theft, is still often trapped in a vortex of disparity that hurts people's sense of justice.

Based on data from the State Cyber and Cryptography Agency (BSSN), there has been a very dramatic surge in cyberattacks in Indonesia, with a figure of 3.64 billion incidents in the period from January to July 2025 alone. This is a fantastic number that almost matches the total accumulated attacks over the past five years, with the majority of attacks being malware targeting financial data and personal identities. This criminological reality demands the readiness of a judicial system that is not only technologically sophisticated but also dogmatically consistent. The presence of Law Number 1 of 2024 concerning the Second Amendment to the ITE Law and Law Number 27 of 2022 concerning Personal Data Protection (PDP Law) should be an anchor for the standardization of digital justice. Unfortunately, in the field, the speed and rigor of the law are often determined by non-juridical variables such as the geographic location of reporting and the digital forensic capacity of the area.

The phenomenon of "centralization of digital justice" is clearly seen when comparing the burden of cases at the Metro Jaya Police, which handled up to 3,709 cyber cases in 2022, with the Regional Police in other regions that often encounter an impasse in the investigation process. This inequality creates a distortion of the principle of equality before the law. People in the regions often have to wait longer or even lose hope because the investigation process is very slow due to the limitations in adequate digital forensic tools, so they have to rely entirely on the support of the Criminal Investigation Agency in Jakarta. This condition is exacerbated by the low digital literacy of some law enforcement officials who are still hesitant to assess the validity of electronic evidence, so they tend to rely on conventional evidence that is less relevant in cybercrime.

The crime of theft of electronic information is juridically accommodated in Article 32 in conjunction with Article 48 of the ITE Law. This article is designed to protect the integrity, confidentiality, and availability of electronic data from any form of illegal intervention. Article 32 paragraph (1) of the ITE Law explicitly prohibits any person from deliberately and without rights or against the law, in any way, altering, adding, reducing, transmitting, damaging, removing, moving, or concealing electronic information and/or an electronic document belonging to another person or to the public. The element of "without rights or against the law" is at the heart of this offense, which requires proof that the perpetrator does not have legal authority or violates the applicable legal norms when accessing or intervening in the data.

The criminal threat regulated in Article 48 paragraph (1) for the violation of Article 32 paragraph (1) is imprisonment for a maximum of eight (8) years and/or a maximum fine of Rp2,000,000,000 (two billion rupiah). This sanction structure reflects how seriously the state views the integrity of electronic data. However, in its development, there are legal loopholes that arise from the interpretation of these articles, which are often considered "gray." Terms such as "in any way" in Article 32 provide room for law enforcement to interpret a wide variety of technical actions as a criminal offense, which, if not limited by a clear element of the offense, is vulnerable to untargeted criminalization.

In addition, the latest ITE Law (Law No. 1 of 2024) also emphasizes the protection of data so that it is not manipulated as if it were authentic. This often intersects with Article 35 of the ITE Law, which regulates the creation of electronic information so that it is regarded as if it were authentic data (falsification).[1] In the context of information theft, the act of taking data is often followed by manipulation of the data for personal gain or to harm others. Synchronization between the ITE Law and the PDP Law is crucial, where the PDP Law focuses more on the privacy rights of data subjects, while the ITE Law focuses on system security and information integrity (Muaya, Bawole, and Taroreh, 2024).

Sentencing disparity is defined as the application of unequal penalties to the same criminal acts, or to criminal acts whose dangerous nature can be compared, without a clear justification (Idrus, 2023). In the Indonesian legal system, this disparity is often triggered by the freedom of judges to determine the severity of punishment within the range of minimum and maximum sanctions provided by law. However, the disparity becomes a serious problem when the difference in verdicts is so striking that it hurts the community's sense of justice (Akbari, Saputro, and Marbun, 2017).

Some legal experts, such as Harkristuti Harkrisnowo and Muladi, argue that disparity occurs due to the human element of the judge who decides cases (Akbari, Saputro, and Marbun, 2017). This factor includes the social background, education, religion, experience, and digital literacy level of each judge. Judges with a deep understanding of digital forensics may impose harsher sentences because they understand the destructive impact of information theft on the system, while judges with little digital literacy may view it as ordinary theft with low evidentiary value.

In addition to the internal factors of judges, the regulatory system that does not provide standard sentencing guidelines is also a main cause. The ITE Law tends to provide a very wide range of sanctions without clear minimum limits on certain articles, thus providing flexibility for judges to decide on verdicts based on subjective intuition rather than objective standards (Potale, Wantu, and Apripari, 2025). The impact of this inconsistency is very real; it makes digital law feel like a "lottery" for both victims and perpetrators, where legal certainty varies depending on the jurisdiction in which the case is processed.

To concretely illustrate how this disparity in law enforcement occurs, this study compares two court decisions involving electronic information crimes with comparable characteristics.

1. Banjarmasin District Court Decision Number 68/Pid.Sus/2024/PN Bjm (Banjarmasin District Court 2024). In this case, the defendant Muhammad Sohaymi bin Yusuf was charged with jointly committing online fraud (buying and selling fictitious cars) and manipulating electronic information to make it appear authentic. The panel of judges at the Banjarmasin District Court sentenced him to 4 (four) years and 6 (six) months in prison and a fine of Rp1,000,000,000 (one billion rupiah).

   The ratio decidendi that affects the severity of this verdict is placed on sociological parameters and track record. The judge explicitly considered the aggravating circumstances in the form of the status of the defendant who had been convicted of narcotics crimes, his actions that disturbed the community, and the amount of damage caused to the victims. Meanwhile, the mitigating thing is only the defendant's remorse and promise not to repeat his actions. The judge also bases his decision on the principle of punishment as a corrective, preventive, educational, and repressive tool to provide a real deterrent effect.
2. South Jakarta District Court Decision Number 764/Pid.B/2016/PN. Jkt.Sel (South Jakarta District Court 2016). This case involves the defendant Panji Henindya Nugraha, an employee of PT Telkomsel's subcontractor, who hacked servers and transferred credit illegally for personal gain. The panel of judges of the South Jakarta District Court sentenced him to imprisonment for 1 (one) year and 6 (six) months and a fine of Rp50,000,000 (fifty million rupiah).

   In contrast to the decision in Banjarmasin, the ratio decidendi of the judge in South Jakarta limits the consideration of purely aggravating circumstances to the aspect of the scope of the act and material loss, namely the act was committed in the work environment and caused a loss of exactly IDR 80,427,600 for PT Telkomsel. The judge gave great weight to the mitigating circumstances, namely the defendant behaved politely, confessed frankly, and had never been convicted. The judge uses the philosophy that punishment is not solely retributive, but aims to foster and educate the defendant.
3. Additional Analysis: Yogyakarta District Court Decision Number 345/Pid.Sus/2021/PN Yyk (Yogyakarta District Court 2021). As supporting data, this verdict involves a case of carding, where the defendant Faisal Umar Firmansyah illegally used credit card data and payment applications belonging to Foreign Citizens to buy Apple products (iPhone 12 Pro)

   In this case, the panel of judges imposed a very light sentence, namely imprisonment for 6 (six) months and a fine of Rp3,000,000 (three million rupiah). The judge's ratio decidendi focused the aggravating circumstances only on the normative argument that the defendant's actions did not support the government's program in eradicating ITE crimes. On the contrary, the gap for leniency is wide opened through the consideration of a very subjective human equation, namely the judge considers that the defendant is still young so that it is expected to be good in the future, in addition to his remorse and status that has never been punished.

The presentation of the three ratio decidendi above shows the real root of the disparity. The difference in sentences (4.5 years, 1.5 years, and 6 months) for the anatomy of cybercrimes that both violate the integrity of electronic data proves to be highly dependent on the freedom of the

parameters chosen by the judge. In one area, judges impose heavy sentences by focusing on past criminal records (although different types of crimes). In other areas, judges tend to be pragmatic by measuring corporate losses, or even very lenient on the grounds of the defendant's young age and future. This disparity in the standard of objective consideration confirms that the disparity in criminality is not just an anomaly, but a consistent pathology in the cyberjustice courtroom.

Seeing this pattern, cyber law enforcement in Indonesia should not be continuously trapped in a rigid positivistic approach, a purely textual and mechanical legal approach will negate the value of human values and distance the judicial order from the real sense of substantive justice in society (Sutrisno 2015).

Implications of Criminal Disparity from the Crime of Electronic Information Theft

The huge difference in sentences between 4.5 years in Banjarmasin, 1.5 years in South Jakarta, and 8 months in Yogyakarta invites a fundamental question: why is this happening? In-depth analysis shows the interaction between the legal, technical, and psychological factors of judges.

In the South Jakarta District Court's decision, the judge seems to give great weight to the value of the actual financial loss (Rp80.4 million) as the main parameter in determining the severity of the punishment. On the other hand, in the Banjarmasin District Court decision, the judge focused more on the aspect of the defendant's criminal track record (recidivism) and the potential danger of data manipulation itself to cyber public order. This points to a philosophical inconsistency: should cyber law protect the economic value of data (material loss) or the integrity of the system itself (formal harm)? This difference in focus leads to immeasurable variations in verdicts.

The recidivism factor in the Banjarmasin District Court decision is the main differentiating variable that pushes the verdict to the upper limit. Regional judges often take a more repressive stance against perpetrators to provide a maximum deterrent effect. Meanwhile, in big cities like Jakarta and Yogyakarta, sociological factors such as "wanting to continue studying" or "being polite in court" are often taken into account more leniently as a reason for imposing a sentence at the lower boundary. This reflects a disparity in the standard of "judicial morality" between regions.

One of the crucial findings in this study is the influence of digital forensic laboratory capacity on judges' convictions. In Jakarta, the presentation of digital evidence is often carried out comprehensively by forensic experts from the Criminal Investigation Department, which makes it easier for judges to understand the mechanism of the crime clearly. However, in areas with limited tools, evidence is often only superficial, which ironically can have a double impact: judges become too hesitant and give light sentences, or judges become too harsh for fear of repercussions they don't fully understand. This hesitation of law enforcement officials is a manifestation of what Endang Sutrisno calls an apathetic legal culture, in which the ideas, perceptions, values, and behavior of the apparatus that are not constructive ultimately greatly affect the process of the law's functioning, so that they are not fully able to translate the substance of justice from the legal texts (Sutrisno and Fajarini, 2016).

The inequality of cyber law enforcement in Indonesia cannot be separated from the problem of technocratic infrastructure. Handling cyber cases requires sophisticated tools to maintain the integrity of digital evidence and prevent it from being damaged or manipulated during legal proceedings. Unfortunately, many cyber units at the level of the Regional Police and Resort Police do not have adequate forensic tools, so they have to wait in long queues to get support from the central laboratory in Jakarta. This delay not only disrupts the investigation process but can also affect the quality of the evidence presented before the court, which ultimately triggers the judge's doubts in deciding the case proportionately. This dependence on infrastructure creates the centralization of justice, a condition that often occurs due to the misinterpretation of laws that consistently ignore regional rights and local interests, because their authority and facilities are taken over by the rulers at the center (Sutrisno, 2014).

The problem of coordination between institutions is also an obstacle. There is still an overlap in interpretations between police investigators, public prosecutors, and judges regarding the application of Article 32 of the ITE Law compared to the articles in the PDP Law. Without an integrated and uniform Standard Operating Procedure (SOP) across all Indonesian jurisdictions, the prosecution process will continue to be marked by uncertainty. This creates the impression of a "center and periphery" in access to justice, where victims in metropolitan areas receive more predictable treatment than victims in remote areas.

This striking disparity in punishment has had a far-reaching impact on public trust in the national legal system. First, it violates the principle of legal certainty, which is a fundamental principle in the rule of law. Legal certainty demands that laws be fixed, clear, and predictable (Gustav Radbruch). If the same crime results in drastically different verdicts simply because of the difference in court location, then the law fails to provide definite protection for its citizens.

Second, for victims of information theft, this disparity causes deep disappointment. Victims who lose money and reputation in the regions may find that the perpetrator is only lightly punished, while in other areas, similar acts are punished very severely. This condition can trigger the perception that justice is a geographical "lottery." Third, in terms of the digital economy, this disparity hinders investment. International business actors and investors will be hesitant to operate in Indonesia if its data protection system is considered inconsistent and unpredictable by law.

Based on a comprehensive analysis of cyber incident data, regulatory construction, and a comparison of court decisions, it can be concluded that the disparity in law enforcement in the crime of electronic information theft in Indonesia is at an alarming level. The difference in verdicts that reaches a span of years for similar cases shows that the principle of equality before the law is still a major challenge in our cyberspace.

This disparity is not only caused by legal factors that still provide too broad a discretion for judges without standard guidelines but also by technical factors in the form of inequality in digital forensic infrastructure and differences in the digital literacy of law enforcement officials between regions. If this condition is allowed to continue, then legal certainty for the digital society will continue to be distorted, which in turn can collapse public trust and hinder the stability of the national digital economy. Therefore, structural legal reforms, ranging from the drafting of

sentencing guidelines to the equitable distribution of forensic technology, are urgent needs that cannot be postponed in order to realize truly equitable digital justice for all Indonesian people.

CONCLUSION

The existence of law enforcement disparities in the crime of electronic information theft in Indonesia is not just a procedural anomaly, but a manifestation of systemic pathology rooted in three problematic fundamentals. First, the failure of normative synchronization between the ITE Law and the PDP Law which gave birth to the dualism of criminal threats and the practice of forum shopping by law enforcement officials. The ambiguity of the phrases "without rights" and "against the law" provides immeasurable discretion, so that the qualification of the crime depends heavily on the subjectivity of the interpretation of the investigator and the public prosecutor rather than the substance of the violation of the data subject's rights.

Second, the portrait of justice in cyberspace is currently trapped in the phenomenon of geographical differences, where the degree of legal protection of a citizen is determined by the location of the report and the capacity of the local forensic infrastructure. The stark contrast in verdicts between the Banjarmasin District Court (4 years and 6 months) and the South Jakarta District Court (1 year and 6 months) for similar crime anatomy proves that the judge's ratio decidendi is still dominated by the human equation factor—namely variations in digital literacy and the judge's personal background—due to the absence of standard criminal guidelines.

Third, the gap in the accessibility of forensic technology between the central and regional regions creates a hierarchy of evidentiary quality. The chronic dependence of regional cyber units on the Criminal Investigation Branch of the National Police results in a slow process and is vulnerable to degradation of the integrity of digital evidence, which in turn encourages regional judges to render minimalist verdicts due to intellectual doubts in assessing electronic evidence.

REFERENCES

Aini, N., & Lubis, F. (2024). Tantangan pembuktian dalam kasus kejahatan siber. *Judge: Jurnal Hukum*.

Akbari, A. R., Saputro, A. A., & Marbun, A. N. (2017). *Memaknai dan mengukur disparitas: Studi terhadap praktik pemidanaan pada tindak pidana korupsi* (R. B. Permana & N. Norita, Eds.). Badan Penerbit Fakultas Hukum Universitas Indonesia-Masyarakat Pemantau Peradilan Indonesia Fakultas Hukum Universitas Indonesia-USAID.

Amuedo-Dorantes, C., Puttitanun, T., & Martinez-Donate, A. P. (2019). Deporting “bad hombres”? The profile of deportees under widespread versus prioritized enforcement. *International Migration Review, 53*(2), 518–547.

Andhitya, R., & Umam, J. (2025). Analisis kritis penegakan hukum kejahatan siber data breach dalam perspektif hukum pidana Indonesia. *Rewang Rencang: Jurnal Hukum Lex Generalis, 6*(7), 1–16.

Anggono, B. D., Wahanisa, R., AP, A. O. V. P. S., & Adiyatma, S. E. (2025). Interrogating the legal foundations of digital transformation: Balancing economic growth and social welfare in the era of disruption. *Volksgeist: Jurnal Ilmu Hukum dan Konstitusi*, 191–211.

Bethune, R. A. (2015). *Profiling white-collar criminals: What is white-collar crime, who perpetrates it and why?*

Cahyono, S. T., Erni, W., & Hidayat, T. (2025). RIKONSTRUKSI hukum pidana terhadap kejahatan siber (cyber crime) dalam sistem peradilan pidana Indonesia. *DJH Dame Jurnal Hukum Yayasan Pesantren Islam Literasi Nusantara, 1*(1), 111–133.

Defara, D. (2025). Indonesia's BSSN records 3.64 billion cyberattacks in first half of 2025. *Tempo*. https://en.tempo.co/read/2037469/indonesias-bssn-records-3-64-billion-cyberattacks-in-first-half-of-2025

Fikriansyah, F., & Harris, F. (2026). Legal analysis of the application of criminal penalties under Law No. 27 of 2022 on the protection of personal data against doxing on social media. *International Journal of New Approaches to Law and Rationality in Nationhood, Governance, and Rights Advocacy, 1*(2), 662–673.

Handayani, E. P., Arifin, Z., & Fernando, Z. J. (2025). Criminal penalties in cyberspace: Between the development of digital democracy and authoritarianism. *Indonesian Journal of Criminal Law Studies, 10*(1), 45–82.

Hafel, M. (2023). Digital transformation in politics and governance in Indonesia: Opportunities and challenges in the era of technological disruption. *Society*.

Hurst, A. N., Bailey, M. L., Krueger, N. T., Garba, R., & Cokley, K. (2018). The psychological impact of policing on African American students. In *Law enforcement in the age of Black Lives Matter: Policing Black and Brown bodies* (pp. 53–74).

Idrus, N. F. A. (2023). Disparitas putusan pemidanaan perkara-perkara penipuan online: Kajian putusan Nomor 118/Pid.Sus/2021/PN.Wkb dan Nomor 210/Pid.Sus/2021/PN.Sdr. *Jurnal Yudisial, 16*(3), 325–341. https://doi.org/10.29123/jy.v16i3.598

Muaya, R. G., Bawole, H., & Taroreh, V. F. (2024). Tindak pidana penistaan agama melalui media sosial berdasarkan Undang-Undang Nomor 1 Tahun 2024 (Studi kasus putusan pengadilan No.122/Pid.Sus/2020/PN.Sorong). *E-Journal Unsrat*, 1–11.

Potale, M., Wantu, F. M., & Apripari. (2025). Disparitas putusan hakim terhadap tindak pidana pencemaran nama baik melalui media sosial. *PCHukumsosial.org, 3*(1), 46–57. https://pchukumsosial.org/index.php/pchs

Priyanjani, A. R., Fadillah, F., Ghalib, A., Sutrisno, E., & Permana, Y. (2024). Legal protection data in the world of work in the era of digitalization of technology and information. *JOSS: Journal of Social Science, 3*(3), 1264–1282. https://joss.al-makkipublisher.com/index.php/js

Sutrisno, E. (2010). Role of law in construction and development of small scale. *Jurnal Dinamika Hukum, 15*, 5–6.

Sutrisno, E. (2014). Implementasi pengelolaan sumber daya pesisir berbasis pengelolaan wilayah pesisir secara terpadu untuk kesejahteraan nelayan (Studi di perdesaan nelayan Cangkol Kelurahan Lemahwungkuk Kecamatan Lemahwungkuk Kota Cirebon). *Jurnal Dinamika Hukum, 14*, 1–12.

Sutrisno, E. (2015). Tracing the performance of law in Indonesia: A perspective of Thomas Kuhn's "normal science." *Journal of Law, Policy and Globalization, 37*, 126–137.

Sutrisno, E., & Fajarini, H. (2016). Legal culture of pharmacist in the perspective of law. *Jurnal Dinamika Hukum, 16*(35), 148–155.

Ulmer, J. T. (2019). Criminal courts as inhabited institutions: Making sense of difference and similarity in sentencing. *Crime and Justice, 48*(1), 483–522.