Journal of Law Science
Volume 7, No. 1, 2025
e-ISSN 2684-9658 pp. 141-149
www.iocscience.org/ejournal/index.php/JLS

Realizing synergy between the ministry of communication and informatics and the national cyber and crypto agency in the era of government digitalization

Reynaldi Usman
Faculty of Law, Universitas Negeri Gorontalo, Gorontalo, Indonesia. E-mail: aldiusman366@gmail.com

ARTICLE INFO

Keywords:

Cyber Security;
Personal Data Protection;
Synchronization of Authority.

Article history:

Received Dec 11, 2024;
Revised Dec 30, 2024;
Accepted Jan 9, 2025;
Online Jan 30, 2025.

ABSTRACT

In particular, overseeing cybersecurity and the protection of personal data in Indonesia has become more difficult in the modern digital age. Inconsistencies in policy often lead to disputes of authority between the National Cyber and Crypto Agency (BSSN) and the Ministry of Communication and Informatics (Kominfo), despite their strategic responsibilities in fostering digital transformation. The absence of effective governance is caused by the overlapping jurisdiction in managing personal data and cybersecurity, which is the fundamental concern. The purpose of this normative descriptive research is to examine legislative measures that might resolve the authority issue between the National Cyber and Crypto Agency and the Ministry of Communication and Informatics. This approach of study delves into both primary and secondary sources of law, including statutes, regulations, and case law from throughout the world. In order to construct a thorough analytical framework, the research also investigates public administration and state administration theories. Findings suggest that formal technical laws, improved coordination mechanisms, and alternative conflict resolution processes like mediation or arbitration may bring about authority synchronization. Furthermore, the efficacy of inter-agency cooperation may be enhanced by enhancing institutional capacity and incorporating best practices from other nations, including Singapore and the European Union. State sovereignty in the cyber world is intended to be strengthened by the proposals that follow, which should help establish a government that is more inclusive, responsive, and flexible in the face of digitalization's problems.

Corresponding Author:

Reynaldi Usman,
Faculty of Law,
Universitas Negeri Gorontalo,
Jl. jendral Sudirman, No. Gorontalo, Gorontalo, 96128, Indonesia
Email: aldiusman366@gmail.com

1. Introduction

A subfield of constitutional law, constitutional law examines the fundamentals of governing the state, state institutions, and interrelationships among these entities in light of constitutional principles (Widodo et al., 2023). An efficient, functional, and rule-based system of governance is the overarching goal of constitutional law (Abqa et al., 2023). In Indonesia, constitutional law serves as a framework for resolving any disputes of power that may emerge between

government entities and also serves as a guide for the distribution of authority among state agencies (Muhtar et al., 2023). In order to maintain constitutionally-guaranteed administration in Indonesia, the system of checks and balances is firmly entrenched in the country's political framework (Indra et al., 2023).

The National Cyber and Crypto Agency (BSSN) and the Ministry of Communication and Informatics (Kominfo) are essential for cybersecurity and digital transformation in Indonesia. However, policy duality caused by overlapping mandates between these organizations hinders governance and efficiency. Kominfo manages ICT legislation and digitization, whereas BSSN protects essential infrastructure and digital sovereignty. These positions must be harmonised to improve administrative procedures, cooperation, and Indonesia's cybersecurity preparedness. Institutional synergy is important, as shown by other countries. The US Department of Homeland Security works with the Cybersecurity and Infrastructure Security Agency (CISA) to avoid redundancy, while the EU uses ENISA to coordinate policies across member states. Based on such experiences, this essay examines ways to connect BSSN with Kominfo to improve Indonesia's digital governance.

The importance of constitutional law in today's world of fast-paced technological advancement is growing as a result of the issues that contemporary government faces (Razak et al., 2023). The regulation of inter-institutional interactions is only one area where digital change has affected government management. As technology develops, it will be necessary to reorganize governmental agencies' responsibilities to avoid duplication of effort. This is consistent with the goals of constitutional law, which are to provide clear laws that help governments function effectively.

Supporting digitalization and ensuring national cyber security are two of the National Cyber and Crypto Agency's key roles. Nevertheless, given the interdependence of the two, the possibility of a power struggle between them cannot be disregarded (Puluhulawa et al., 2023).

The constitutional framework, statutes, and implementing rules of Indonesia govern the country's legal system, including the allocation of power among various ministries and governmental organizations. The primary responsibility of the Ministry of Communication and Information, established by Law No. 39 of 2008 on the subject of State Ministries, is the administration of the country's telecommunications networks, the creation and enforcement of digital rules, and the advancement of IT (Muhtar et al., 2019). The regulation of telecommunications networks, internet services, and personal data protection is specifically entrusted to the Ministry of Communication and Information by Law Number 27 of 2022, which pertains to Personal Data Protection (Vania et al., 2023).

However, it was via Presidential Regulations 133 of 2017 and 53 of 2017 that the National Cyber and Crypto Agency was founded. Coordination of cyber defenses, prevention of digital attacks, and protection of critical government and commercial electronic systems are the primary functions of the National Cyber and Crypto Agency. The National Cyber and Crypto Agency was established in response to the growing complexity of cyber threats, such as hacking, data theft, and virus assaults (Rahman et al., 2024).

These two agencies have different but complementary missions, yet their duties frequently overlap, especially in digital data management and national network protection. Authority disputes are more likely, which raises the risk of overlapping policies or initiatives. The main disagreement between the National Cyber and Crypto Agency and the Ministry of Communication and Information is misaligned technology and digital security regulations. Due to conflicting views on the authority of various institutions, regulation becomes dualism. One example is protecting sensitive data and computer networks.

The Personal Data Protection Law asserts the power to control personal data security measures, including the imposition of penalties on those who breach them, as claimed by the Ministry of Communication and Information. On the other hand, managing data security is something that

the National Cyber and Crypto Agency sees as part of their responsibility to safeguard the nation's electronic system. Consequently, data protection measures may not be fully implemented due to a lack of alignment in policy (Gobel et al., 2023).

The absence of cooperation in responding to cyber events is another common issue. In the event of a large-scale cyberattack, the National Cyber and Crypto Agency and the Ministry of Communication and Information often respond separately, without proper cooperation. This leads to muddled thinking among all parties involved, especially the business sector, and weakens the reaction to the danger.

The National Cyber and Crypto Agency and Ministry of Communication and Informatics share authority, as shown by the 2022 data breach that impacted several government offices. This tragedy occurred because a third party's weak security exposed millions of Indonesians' personal data online. According to the Ministry of Communication and Informatics, the National Cyber and Crypto Agency protects critical electronic systems and is responsible for this incident. The National Cyber and Crypto Agency deemed the Ministry of Communication and Informatics responsible since the hacked data was related to app management within their jurisdiction (Wantu et al., 2023).

This dispute between the two institutions shows a lack of collaboration and dissatisfies the public since it is unclear who is responsible for protecting personal data. This incident also reveals that the National Cyber and Crypto Agency and Ministry of Communication and Information need to improve their authority coordination mechanism to avoid future incidents. (1) In this era of government digitalization, how can the National Cyber and Crypto Agency and the Ministry of Communication and Information coordinate to avoid regulatory overlap? (2) How can we develop clear legal rules to oversee Indonesia's transfer of cybersecurity and personal data protection authority from the Ministry of Communication and Information to the National Cyber and Crypto Agency?

2. Method

This paper addresses two primary issues with Indonesia's Criminal proceedings Code-regulated criminal proceedings system. The first concept discusses how the Criminal procedural Code improves victim healing by reconstructing criminal procedural systems. This paper analyzes criminal procedural legislation linked to victim protection, including the right to restitution, compensation, and access to justice, using a normative descriptive method (Amirudin & Zainal Asikin, 2004). This study examines whether the Criminal Procedure Code has allowed victims to obtain fair restitution using primary legal materials like Law Number 8 of 1981 and court decisions and secondary legal materials like literature and comparative studies. The research shows that although the Criminal Procedure Code provides certain normative underpinnings, its execution is frequently suboptimal owing to a lack of technical standards and law enforcement convergence. To provide full substantive justice, this paper advocates reforming criminal procedural law standards, including establishing a victim compensation system.

The second issue formulation addresses ways to improve functional difference and suspect/defendant rights in Indonesia's criminal justice system. This research uses a juridical-analytical method to identify barriers to functional difference between police, prosecutors, and courts. This report examines the implementation of suspects/defendants' procedural rights, such as the right to legal counsel, the right to stay quiet, and the presumption of innocence, exposing ongoing inequity. Comparing judicial systems in various nations helped uncover better integration and coordination approaches. The research found that lack of coordination and overlapping power amongst agencies are the biggest barriers to criminal procedural legislation. This report advises enhancing the regulatory framework, including inter-institutional coordination mechanisms and procedural rights, to build a fairer and more community-responsive judicial system.

Legal-analytical methods can identify normative and regulatory issues in inter-agency coordination, but they may not address practical obstacles like organisational culture, communication gaps, and resource allocation, which are essential for effective collaboration between agencies like BSSN and Kominfo. These techniques should be supplemented by empirical methods like interviews, case studies, and implementation assessments to identify practical hurdles and areas for development. To guarantee relevance and application, nations must be compared based on governance systems, digitization levels, agency missions, and socioeconomic situations. While the US and EU offer insights from their advanced digital governance systems, ASEAN comparisons may yield more contextually relevant recommendations for Indonesia's unique challenges and opportunities.

3. Analysis and Results

3.1. Synchronization of Authority Between the Ministry of Communication and Information and the National Cyber and Crypto Agency in the Era of Government Digitalization

Digitalization has changed how the government handles policy, delivers public services, and secures the country. These constitutional amendments need detailed measures to ensure government activities work smoothly, notably via synchronization of power across ministries and institutions (Amanuha et al., 2021). Understanding government coordination is based on the separation of powers and checks and balances. Montesquieu's division of powers doctrine ensures that each government agency has distinct jurisdiction yet works together to accomplish national objectives (Yudhanegara et al., 2024). The 1945 Constitution of Indonesia establishes this concept, which governs governmental agencies including the Ministry of Communication and Information and the National Cyber and Crypto Agency.

The Ministry of Communication and Informatics (Kominfo) and the National Cyber and Crypto Agency (BSSN) have had varied results in their collaboration. Both organizations have made progress in digitization and cybersecurity, but overlapping missions and unclear duties have often hampered collaboration. Kominfo's emphasis on digital infrastructure development and regulations conflicts with BSSN's cybersecurity, which may cause redundancy or delays in adopting integrated rules. However, collaborative efforts to resist cyber attacks and secure vital information infrastructure during significant events have shown the potential for synergy when coordination mechanisms work. These gaps need a more formal framework for inter-agency communication and job distribution, as well as frequent reviews to improve cooperation practices. Empirical investigations and stakeholder input from field activities would reveal this cooperation's breadth and places for development.

Synchronizing authority is both a technical measure to reduce duplication and a sign of effective governance (Suryani et al., 2023). Good governance stresses openness, accountability, and efficiency in public administration, including digitization. The Ministry of Communication and Information regulates and develops IT infrastructure, while the National Cyber and Crypto Agency handles cybersecurity. Although they have separate objectives, these two entities work together to perform digital government services. Thus, the governance system theory that stresses cooperation between components might explain the necessity for synergy between the Ministry of Communication and Information and the National Cyber and Crypto Agency (Addahlawi et al., 2019).

Data security and information protection are crucial to national sovereignty in the digital age. Cybersecurity theory considers hacking, data theft, and malware assaults non-traditional dangers that necessitate cross-institutional solutions (Kesuma et al., 2021). This idea highlights that cybersecurity needs government agencies to work together. Network theory applies here, as a system's success relies on its nodes' strength and coordination. As two important nodes in the national cybersecurity network, the Ministry of Communication and Information and the National Cyber and Crypto Agency must cooperate together to succeed in government digitalization in Indonesia.

In actuality, synchronizing power between the Ministry of Communication and Informatics and the National Cyber and Crypto Agency is difficult. The lack of defined authority boundaries sometimes leads to conflicts of tasks and functions. The Ministry of Communication and Informatics may regulate data protection measures under Law Number 27 of 2022 on Personal Data Protection. The National Cyber and Crypto Agency secures electronic systems and protects data on a larger scale (NA Putri, 2023). These institutions act autonomously without cooperation, resulting in policy implementation gaps.

Lack of technical rules governing the Ministry of Communication and Information and National Cyber and Crypto Agency's working relationship is another issue. Avoiding inter-institutional conflict in constitutional law requires clear legal rules. Unfortunately, there are no rules that outline the power split between the two entities. Thus, tasks are typically interpreted differently by each organization, which may lead to overlapping regulations or internal rivalry. This circumstance undermines government efficacy and public confidence in its digitization management.

Formal and continuous coordination methods may synchronize authority, according to public management theory. Administrative coordination theory stresses that government performance relies on agency-wide objective, resource, and action alignment (Yassine et al., 2024). To resolve the authority disagreement, the Ministry of Communication and Information and the National Cyber and Crypto Agency might organize a task group. Policy discussions, priority alignment, and coordinated cyber threat response may occur in this task force.

Conflict management theory may also resolve the Ministry of Communication and Information-National Cyber and Crypto Agency dispute. This paradigm emphasises mediation, negotiation, and open communication to resolve inter-agency disputes (De Dreu et al., 2001). The government might undertake a more extensive interaction between the two institutions to guarantee that government digitalization policies and initiatives are founded on a common understanding of each other's tasks and functions.

Due to a weak security system, millions of Indonesians' personal data was leaked in 2022, highlighting the need for authority synchronization between the Ministry of Communication and Informatics and the National Cyber and Crypto Agency. The Ministry of Communication and Informatics and the National Cyber and Crypto Agency passed the buck, confusing the public and eroding faith in the government's data protection services. This episode highlights the necessity for stricter laws and collaboration to avoid such catastrophes.

This difficulty requires the government to learn from overseas practices. In the EU, the General Data Protection Regulation (GDPR) and the Network and Information Security Directive control data management and cybersecurity authority synchronization. Both legislation outline how data supervisory agencies and cybersecurity authorities should divide duties, which Indonesia might utilize to design comparable regulations.

Understanding the importance of theory and concepts in managing inter-agency authority makes synchronization efforts between the Ministry of Communication and Information and the National Cyber and Crypto Agency technical needs and good governance principles. Successfully harmonizing these two entities' jurisdiction will improve governance, data protection, and cybersecurity. This combination should help create a digitalization-era government that is adaptable, inclusive, and responsive.

3.2. Effective Legal Steps to Regulate the Division of Authority Between the Ministry of Communication and Information and the National Cyber and Crypto Agency in Managing Cyber Security and Personal Data Protection in Indonesia

Effective legislative actions to regulate the Ministry of Communication and Information and National Cyber and Crypto Agency's authority division are needed to address government digitization. Cybersecurity management and personal data protection are interconnected and need robust institutional cooperation. According to constitutional law, state institutions must be

divided by checks and balances to guarantee that each has distinct roles and powers and does not overlap. The basic foundation for legislative efforts to improve institution cooperation and integration is this idea.

Reviewing the normative foundation helps explain the legal stages. As the ministry responsible for administering information and communication technology, the Ministry of Communication and Informatics regulates digitalization, including technical infrastructure and data security. Law Number 11 of 2008 on Information and Electronic Transactions empowers the Ministry of Communication and Informatics to regulate electronic systems. Law Number 27 of 2022 on the Protection of Personal Data also makes the Ministry of Communication and Informatics the principal data protection authority. However, the National Cyber and Crypto Agency, established by Presidential Regulation Number 53 of 2017 and Presidential Regulation Number 133 of 2017, protects critical information infrastructure and prevents digital threats to state interests (VS Putri et al., 2023).

They have diverse roles, although they frequently overlap, notably in personal data protection and electronic system security. This missynchronization has caused overlapping rules, cyber incident coordination issues, and legal ambiguity for business and the public. The Ministry of Communication and Information and the National Cyber and Crypto Agency disputed responsibility for a government digital platform data breach. This conflict illustrates the necessity for stricter legislative measures to restrict the two institutions' power.

First, technical laws that specifically define the Ministry of Communication and Information and National Cyber and Crypto Agency's authority division may enhance the legal foundation. The government may issue a Presidential Regulation (Perpres) or Government Regulation (PP) that details each institution's roles and powers, particularly in areas prone to authority disputes. Creating a common task force to align policy and react to cyber events is necessary to coordinate this legislation. The Ministry of Communication and Information and the National Cyber and Crypto Agency may use this task force to improve communication so they can make decisions based on each other's priorities and duties.

The Personal Data Protection Law and the Electronic Information and Transactions Law can be amended to include more specific provisions about the Ministry of Communication and Information and the National Cyber and Crypto Agency's working relationship (Abdussamad & Muhtar, 2022). State administrative law emphasizes precise legal rules to avoid institution disputes, therefore this change should take it into consideration. The Personal Data Protection Law may include an article dividing duties between the Ministry of Communication and Information as data protection regulator and the National Cyber and Crypto Agency as vital information infrastructure protector. Thus, each organization has clear jurisdiction, decreasing overlap and improving policy execution (Anisah & Nurisman, 2022).

Strengthening institutional conflict resolution is another legal step. Mediation or arbitration by independent organizations like the Constitutional Court (MK) or special institutions may address authority problems between government entities under the constitutional law system (Agustina et al., 2024). This method may settle policy or task conflicts between the Ministry of Communication and Information and the National Cyber and Crypto Agency. The administrative court may also examine policies that contravene division of power. An efficient dispute settlement procedure may reduce inter-agency disagreements, making government more harmonious.

The Ministry of Communication and Informatics and the National Cyber and Crypto Agency require training, human resource development, and proper financial allocation to support these legal actions. Institutional capability is a fundamental determinant in policy effectiveness in public administration theory. Therefore, the Ministry of Communication and Informatics and the National Cyber and Crypto Agency require appropriate resources to do their jobs. To develop a secure and sustainable digital environment, these two organizations must work more

with the commercial sector and civil society. Public consultation forums, educational initiatives, and stakeholder-led strategic alliances may achieve this collaboration.

Indonesia may learn from other nations that have effectively divided cybersecurity and data protection authorities from a comparative legal viewpoint. The EU General Data Protection Regulation (GDPR) establishes data protection agencies in each member state and regulates personal data management. The Network and Information Security Directive (NIS Directive) promotes national and international cybersecurity collaboration. This model indicates that digital policy execution requires solid laws and systematic collaboration.

Singapore is an Asian example of successful agency power division. Singapore's Cybersecurity Act creates a national cybersecurity body to safeguard vital infrastructure and coordinate government entities. The Personal Data Protection Act (PDPA) establishes independent but complementary regulatory authorities with the cybersecurity authority to offer a clear framework for personal data management. This proves that clear regulation and strong cooperation can establish a trustworthy digital environment (Muhtar et al., 2024).

Given the obstacles and possibilities, effective legislative procedures to control the Ministry of Communication and Informatics and the National Cyber and Crypto Agency's authority division must be comprehensive and constitutional. For the two institutions to work together, strong laws, clear coordination procedures, and institutional capacity must be strengthened. Long-term, these actions should help create a government that is adaptable, inclusive, and responsive to digital requirements. Thus, Indonesia can confidently address digitalization problems while preserving people's rights and state sovereignty in cyberspace.

4. Conclusion

The Ministry of Communication and Informatics and the National Cyber and Crypto Agency must work together to handle cybersecurity and personal data in the complicated digitalization era. These two institutions have separate roles, yet their overlap in power may cause disputes that hamper government. Thus, explicit technical laws, strengthened coordination procedures, and mediation or arbitration of inter-agency disagreements are essential. Creating a secure and credible digital environment also requires developing institutional capacity, enhancing private sector collaboration, and implementing worldwide best practices. With a holistic approach based on constitutional law, the Ministry of Communication and Informatics and the National Cyber and Crypto Agency can support adaptive, inclusive, and responsive governance to the digital era's challenges so Indonesia can maintain sovereignty and protect community interests in the cyber world.

The effectiveness of Kominfo-BSSN collaboration has varied results, with important social and economic ramifications. While digitization and cybersecurity issues have been addressed, overlapping mandates and unclear duties have often hampered collaboration, resulting in inefficiencies. Delays in adopting integrated policies may leave crucial sectors exposed to cyberattacks, eroding public faith in digital services and e-governance uptake. Gaps may raise cyber incident management costs, damage digital infrastructure, and prevent investments in Indonesia's burgeoning digital economy. However, good coordination to secure essential infrastructure during major events may improve public safety and economic stability. Inter-agency communication and job allocation must be designed to improve operational efficiency, public confidence, and economic resilience in the digital age.

References

Abdussamad, Z., & Muhtar, MH (2022). Ethics of Using Social Media in Promoting Tourism Destinations in Patoameme Village. Accounting and Humanities: Journal of Community Service, 1(2), Article 2. https://doi.org/10.38142/ahjpm.v1i2.339

Abqa, MAR, SH, M., Dedi Mulyadi, SH, Rohman, MMM, Mia Amalia, SH, Tanesab, MJ, Sos, S., Junaidi, SH, & MH, C. (2023). ELECTION LEGAL POLITICS. PT. Sonpedia Publishing Indonesia.

https://www.researchgate.net/profile/Mohamad-Hidayat-Muhtar/publication/371735353_Penerbit/links/6492eb86b9ed6874a5c549fc/Penerbit.pdf

Addahlawi, HA, Mustaghfiroh, U., Ni'mah, LK, Sundusiyah, A., & Hidayatullah, AF (2019). IMPLEMENTATION OF GOOD ENVIRONMENTAL GOVERNANCE PRINCIPLES IN WASTE MANAGEMENT IN INDONESIA. Journal of Green Growth and Environmental Management, 8(2), 106–118. https://doi.org/10.21009/JGG.082.04

Agustina, E., Irvita, M., Saharuddin, S., Rahim, EI, & Muhtar, MH (2024). Finding a new direction for Indonesian democracy: Analysis of limitations of the president's powers in the amendments to the constitution. LEGAL BRIEF, 13(1), Article 1. https://doi.org/10.35335/legal.v13i1.929

Amanuha, G., Hasanah, B., Sururi, A., & Sukendar, S. (2021). Digitalization of Government Through the Implementation of SIMRAL in Supporting Sustainable Regional Development. MINANGKABAU GOVERNMENT APPLIED JOURNAL, 1(2), Article 2. https://doi.org/10.33701/jtpm.v1i2.2086

Amirudin & Zainal Asikin. (2004). Introduction to Legal Research Methods. Radja Grafindo.

Anisah, AP, & Nurisman, E. (2022). Cyberstalking: Crimes Against Personal Data Protection as a Trigger for Criminal Acts. KRTHA BHAYANGKARA, 16(1), 163–176. https://doi.org/10.31599/krtha.v16i1.1047

De Dreu, C.K.W., Evers, A., Beersma, B., Kluwer, E.S., & Nauta, A. (2001). A theory-based measure of conflict management strategies in the workplace. Journal of Organizational Behavior, 22(6), 645–668. https://doi.org/10.1002/job.107

Gobel, RTS, Muhtar, MH, & Putri, VS (2023). Regulation And Institutional Arrangement Of Village-Owned Enterprises After The Work Creation Era Is Applied. Pamator Journal*: Scientific Journal of Trunojoyo University*, 16(1), 15–33. https://doi.org/10.21107/pamator.v16i1.19135

Indra, M., Saragih, GM, & Muhtar, MH (2023). Strength of Constitutional Court Decisions in Judicial Review of the 1945 Constitution in Indonesia: Strength of Constitutional Court Decisions in Judicial Review of the 1945 Constitution in Indonesia. Constitutional Journal, 20(2), Article 2. https://doi.org/10.31078/jk2026

Kesuma, AANDH, Budiartha, INP, & Wesna, PAS (2021). Legal Protection of Personal Data Security of Financial Technology Consumers in Electronic Transactions. Journal of Legal Preferences, 2(2), Article 2. https://doi.org/10.22225/jph.2.2.3350.411-416

Muhtar, MH, Hadju, ZAA, Abdussamad, Z., & Gobel, RTS (2019). Expansion of the Indonesian Broadcasting Commission's Authority on Digital Media Supervision Authorities Expansion of Indonesian Broadcasting Commission on Digital. https://www.researchgate.net/profile/Mohamad-Hidayat-Muhtar/publication/359736620_Perluasan_Kewenangan_Komisi_Penyiaran_Indonesia_Terhadap_Pengawasan_Media_Digital/links/62b9a88693242c74cad1b47a/Perluasan-Kewenangan-Komisi-Penyiaran-Indonesia-Terhadap-Pengawasan-Media-Digital.pdf

Muhtar, MH, Maranjaya, AK, Arfiani, N., & Rahim, E. (2023). CONSTITUTIONAL THEORY & LAW: Basic Knowledge and Understanding and Insight into the Implementation of Constitutional Law in Indonesia. PT. Sonpedia Publishing Indonesia.

Muhtar, MH, Yassine, C., Amirulkamar, S., Hammadi, A., Putri, VS, & Achir, N. (2024). Critical Study of Sharia Regional Regulations on Women's Emancipation. International Journal of Religion, 5(2), Article 2. https://doi.org/10.61707/a7s8vg65

Pensiunulawa, J., Muhtar, MH, Towadi, M., & Swarianata, V. (2023). The Concept of Cyber Insurance as a Loss Guarantee on Data Protection Hacking in Indonesia. Law, State and Telecommunications Review, 15(2), 132–145.

Putri, NA (2023). Doxing for Malicious Purposes vs Doxing for Political Purposes: The Urgency of Classifying the Threat of Punishment for Doxing Perpetrators in Law Number 27 of 2022 concerning Personal Data Protection. Padjadjaran Law Review, 11(1), 102–113. https://doi.org/10.56895/plr.v11i1.1286

Putri, VS, Muhtar, MH, Winarsasi, PA, & Manullang, SO (2023). Authority of Space Utilization Permits Post Job Creation Law. Eureka Media Aksara. https://repository.penerbiteureka.com/publications/563020/

Rahman, I., Muhtar, MH, Mongdong, NM, Setiawan, R., Setiawan, B., & Siburian, HK (2024). Harmonization of Digital laws and Adaptation Strategies in Indonesia focusing on E-Commerce and Digital transactions. Innovative: Journal Of Social Science Research, 4(1), Article 1. https://doi.org/10.31004/innovative.v4i1.8240

Razak, A., Muhtar, M.H., Rivera, K.M., & Saragih, G.M. (2023). Balancing Civil and Political Rights: Constitutional Court Powers in Indonesia and Austria. Journal of Indonesian Legal Studies, 8(2), Article 2. https://doi.org/10.15294/jils.v8i2.70717

Suryani, I., Muhtar, MH, Rahman, YM, Jaya, BPM, & Khalaf, AA (2023). Integration of Islamic Law in Regional Development in Indonesia. JURIS (Jurnal Ilmiah Syariah), 22(1), Article 1. https://doi.org/10.31958/juris.v22i1.8770

Vania, C., Markoni, M., Saragih, H., & Widarto, J. (2023). Legal Review of Personal Data Protection from the Aspects of Data Security and Cyber Security. Indonesian Multidisciplinary Journal, 2(3), 654–666. https://doi.org/10.58344/jmi.v2i3.157

Wantu, F., Muhtar, MH, Putri, VS, Thalib, MC, & Junus, N. (2023). THE EXISTENCE OF MEDIATION AS A FORM OF ENVIRONMENTAL DISPUTE RESOLUTION AFTER THE JOB CREATION LAW EFFECTS. Environmental Law Development, 7(2), 267–289. https://bhl-jurnal.or.id/index.php/bhl/article/view/193

English: State Administrative Law.

Yassine, C., Ahmad, A., Muhtar, MH, Rivera, KM, & Putri, VS (2024). Admissibility of Lawsuits Based on Interest under Algerian Civil and Administrative Procedures. Jambura Law Review, 6(2), Article 2. https://doi.org/10.33756/jlr.v6i2.24309

Yudhanegara, F., Arifuddin, Q., Muhtar, MH, Yani, MA, Amalia, M., Judijanto, L., & HR, MA (2024). Introduction to Legal Philosophy: An Ontology, Epistemology, and Axiology of Legal Science. PT. Sonpedia Publishing Indonesia.