Journal of Applied Computing and Digital Information (JACODI)
Vol. 01, Issue 02, pp. XX–XX, 2025
Available online at: https://jurnal.algoria.biz.id/index.php/jacodi

Virtual Private Networks, Site Blocking, and Digital Security Governance in Indonesia

Irham Hanapi[1]*, Indra Maulana[1], Nisfu Ruwaihan Maulana[1], Nandana Firjatullah[1], Angga Febrian Nugroho[1]

[1]Department of Constitutional Law, Faculty of Sharia, Universitas Islam Negeri Sultan Maulana Hasanuddin Banten, Serang, Indonesia

Article Info

Article history:
Received: 16 June 2024
Revised: 05 January 2025
Accepted: 30 November 2025

Keywords:
virtual private network (VPN)
site blocking
network security
data protection
regulatory compliance

ABSTRACT

VPNs are used to protect communications over untrusted networks and to reach services inaccessible through a particular connection, but they also raise concerns about traffic visibility, privacy, and access to blocked content. This article analyzes VPN use in Indonesia through a technical-governance framework connecting network risks with applicable regulation. The study combines document analysis of Indonesian legal instruments and official regulatory materials with technical literature on VPN security, IPsec, and DNS privacy. It maps electronic-system and personal-data responsibilities to five risk areas: tunnel configuration, DNS/IPv6 leakage, provider-side logging, mobile-app supply-chain behavior, and fail-open connectivity. The analysis indicates that VPN technology must be assessed separately from conduct performed through it; legal consequences depend on the relevant act, content, provider role, and applicable legal elements. Prior empirical research has found serious weaknesses in some mobile VPN applications, but those findings cannot be generalized to every current service. The article provides a regulatory-control matrix and a repeatable technical checklist; it does not claim to test commercial VPN products. It concludes that risk-based verification and precise legal classification are preferable to unsupported claims of a blanket VPN-specific licensing requirement.

This is an open access article under the CC-BY 4.0. license.

Corresponding Author:
Irham Hanapi
Program Studi Hukum Tata Negara, Fakultas Syariah, Universitas Islam Negeri Sultan Maulana Hasanuddin Banten, Serang, Indonesia
Email: irahmhnf7893@gmail.com

1. INTRODUCTION

Virtual private network (VPN) is a networking mechanism that creates a protected logical path between an endpoint and a remote gateway. Depending on its configuration, a VPN can reduce exposure of traffic to local network observers and support remote access to organizational resources. It does not, however, guarantee anonymity, prevent all tracking, or make every destination safe. A VPN operator may observe connection metadata, and application-level protections such as HTTPS remain important. Technical guidance on IPsec emphasizes that security depends on sound protocol selection, configuration, and key management rather than on the label "VPN" alone [10], [11].

©2025. JACODI. This work is openly licensed via CC BY 4.0.

VPN services are also used to reach websites that are inaccessible from a particular network or jurisdiction. This creates a distinction between the network mechanism and the purpose or result of its use. The ability to tunnel traffic does not itself establish whether the accessed content is lawful; conversely, the mere presence of a VPN connection is not sufficient evidence that a user has committed an offense. Assessment must identify the relevant conduct, content, system role, and legal elements. This distinction is especially important in regulatory discussion because a technical control that changes the apparent network route is not the same thing as a legal authorization to access, distribute, or process content.

In Indonesia, the relevant framework is distributed across regulations concerning electronic information and transactions, electronic-system operation, private electronic-system operators, personal-data protection, and content-specific prohibitions. The Information and Electronic Transactions Law (ITE Law) has been amended, including by Law No. 19 of 2016 and Law No. 1 of 2024 [1]–[3]. Government Regulation No. 71 of 2019 addresses the operation of electronic systems [4], while Ministerial Regulation No. 5 of 2020 provides requirements for private electronic-system operators and procedures related to prohibited information and access termination [5]. Law No. 27 of 2022 separately establishes personal-data protection obligations [6]. These instruments should be applied according to their scope and the facts of a particular service; they should not be treated as proof that every VPN application requires a dedicated VPN-specific permit.

The technical relevance is not hypothetical. A measurement study of 283 Android applications using the VPN permission found that some applications used insecure tunneling protocols, exposed IPv6 or DNS traffic, intercepted TLS, or modified traffic for tracking and advertising [9]. The study is an important warning, but its sample and age limit any inference about the entire current VPN market. DNS-over-HTTPS can protect DNS exchanges from some on-path observation, yet it does not by itself demonstrate that all traffic is routed through a VPN tunnel [12]. Therefore, users and organizations need verification controls rather than relying solely on app-store availability or marketing claims.

This article addresses three questions: (1) how should technical VPN risks be mapped to Indonesia's applicable electronic-system and data-protection framework; (2) what unsupported regulatory claims should be avoided when discussing access to blocked websites; and (3) what technical checks can be used to assess VPN privacy and security without conflating a document review with empirical product testing? The contribution is a regulatory-control matrix and a threat-oriented verification checklist. Unlike a purely normative legal analysis, the paper organizes the issue around system components, failure modes, and testable controls. Its findings are analytical and literature-based, not the outcome of testing any commercial VPN application.

2. METHOD

2.1. Research design and sources

The study uses a document-based technical-governance assessment. It combines (i) structured mapping of Indonesian regulatory instruments, (ii) synthesis of established technical guidance and prior VPN-security research, and (iii) scenario analysis of technical failure modes relevant to blocked-site access. The approach is not presented as a systematic literature review: sources were selected purposively for direct relevance to VPN architecture, network security, electronic-system responsibilities, privacy, and content-access controls.

Primary regulatory materials were retrieved from official Indonesian legal-information portals. The legal set included Law No. 11 of 2008 on Electronic Information and Transactions, its amendments, Government Regulation No. 71 of 2019, Ministerial Regulation No. 5 of 2020 on Private Electronic-System Operators (read alongside its amendment), Law No. 27 of 2022 on Personal Data Protection, Law No. 44 of 2008 on Pornography, and Law No. 1 of 2023 on the Criminal Code [1]–[8]. The technical set included an ACM measurement study on Android VPN applications, NIST guidance on IPsec VPNs, the Internet Protocol Security architecture, the DNS-over-HTTPS standard, and the NIST Cybersecurity Framework 2.0 [9]–[13]. Regulatory status and source availability were checked for this revision on 25 October 2026.

2.2. Analytical procedure

The analysis proceeded in four steps. First, each legal instrument was coded by subject, regulatory object, and type of obligation. Second, relevant network functions were decomposed into tunnel establishment, DNS

©2025. JACODI. This work is openly licensed via CC BY 4.0.

resolution, IPv4/IPv6 routing, provider-side processing, mobile-app behavior, and connection-failure handling. Third, technical risks described in the literature were matched with plausible control objectives and the regulatory provisions that may be relevant, while distinguishing binding legal obligations from technical recommendations. Fourth, the results were consolidated into two matrices: a regulatory matrix and a technical risk-control matrix. A control was classified as "recommended" when it was a technical safeguard derived from security guidance or the literature, rather than an express requirement stated in Indonesian legislation.

No VPN applications were installed, scanned, intercepted, or benchmarked for this study. No claims are therefore made about current leak rates, encryption performance, latency, provider logging practices, or the security of a named commercial product. The technical checklist is a proposed reproducible assessment protocol for subsequent empirical work, not a report of completed measurements.

3. RESULTS AND DISCUSSION

3.1. Technical boundary of VPN protection

A VPN protects a communication path between an endpoint and a VPN gateway according to the implemented tunnel protocol and configuration. It should not be treated as an end-to-end guarantee for every application or a substitute for endpoint security. For example, encryption between a device and the VPN gateway may reduce visibility for an access-network observer, but the gateway becomes a trusted intermediary and may process connection metadata. Traffic that leaves the tunnel through an incorrect route, DNS requests that bypass the tunnel, or IPv6 traffic that is not covered by the tunnel can reveal information that users expected to conceal. The IPsec architecture and NIST's implementation guide make configuration, key management, and security-service selection central to effective protection [10], [11].

Application behavior is a separate layer. A mobile VPN application may request broad network permissions, embed third-party software-development kits, collect identifiers, or alter traffic. Ikram et al. reported examples of these behaviors among applications in their historical sample [9]. Their results justify inspection of app behavior and transparency, but they do not justify a claim that all free VPN services are malicious or that all current products retain the same weaknesses. A defensible conclusion must be tied to the product version, operating system, test conditions, and captured evidence.

3.2. Regulatory mapping and claim boundaries

Table 1 maps the primary legal instruments to system-governance questions. It intentionally avoids treating a general electronic-system obligation as a VPN-specific licensing rule. In particular, registration or other duties under rules for electronic-system operators depend on whether the relevant entity and service fall within the regulatory definition and scope. A marketplace listing, the use of a VPN protocol, and the operation of an electronic system are not interchangeable facts. The analysis should identify the responsible legal entity and the service function before applying a particular obligation [4], [5].

Table 1. Regulatory-control mapping and limits of interpretation

Instrument / issue	Relevant governance dimension	Interpretation boundary
ITE Law and amendments [1]–[3]	Rules for electronic information/transactions and specific prohibited conduct; relevant where the user's or operator's acts satisfy the legal elements.	Do not infer an offense solely from the existence of a VPN tunnel or from the fact that a destination is blocked. Identify the act, content, intent where relevant, and applicable provision.
Government Regulation No. 71/2019 [4]	Framework for reliable, secure, and accountable electronic-system operation within the scope of the regulation.	First determine whether the VPN provider or another entity qualifies as an electronic-system operator and which duties attach to that role.
Ministerial Regulation No.	Private electronic-system operator framework, including registration and procedures concerning	The instrument is not evidence of a universal, dedicated "VPN permit"

©2025. JACODI. This work is openly licensed via CC BY 4.0.

5/2020 and amendment [5]	prohibited information/access termination where applicable.	unless a specific provision and scope are shown to establish it.
Personal Data Protection Law No. 27/2022 [6]	Applies to personal-data processing according to the roles and activities of controllers/processors and applicable territorial rules.	Assess what data is collected, purposes, retention, disclosure, security, and potential cross-border transfers; do not assume every provider has the same role.
Pornography Law and Criminal Code [7], [8]	Content-related restrictions and criminal provisions must be assessed under the applicable, current text and relevant elements.	The Pornography Law is recorded as partially affected by Law No. 1/2023. Verify the current consolidated legal basis before relying on a specific article or penalty.

The legal framework is therefore activity- and role-sensitive. The ITE Law cannot be summarized as a general prohibition of VPN use; its provisions apply to specified conduct and elements. Likewise, the duty to operate an electronic system securely is addressed to entities and systems within the regulation's scope, rather than being a blanket statement that all software using tunneling must obtain a special permit [1]–[5]. The same caution applies to data protection: the existence of a VPN connection does not by itself reveal whether a service is a controller or processor, what personal data is processed, or whether a particular transfer is unlawful. Those questions require evidence about actual processing and the applicable legal roles [6].

Content-related laws must also be cited precisely. The use of VPN technology does not remove the application of laws governing prohibited content or transactions, but access, possession, creation, distribution, and facilitation may be legally distinct acts. Further, Law No. 44 of 2008 is listed in the official legal database as partially affected by Law No. 1 of 2023 [7], [8]. For any legal opinion or future resubmission, the current text and commencement provisions should be checked before citing a specific criminal article or penalty. The paper therefore does not repeat the original manuscript's categorical claim that every visit to a blocked site automatically constitutes a criminal offense.

3.3. Technical risks and recommended verification controls

The technical control matrix in Table 2 connects documented VPN risk categories with checks that can be performed in a future empirical study. Severity labels describe potential consequences, not measured frequencies. "High" refers to a failure that can directly expose sensitive traffic or identity-related metadata; "medium" refers to risks whose severity depends more heavily on configuration, endpoint context, and the data processed. The classifications should be validated against the use case and threat model rather than treated as universal scores.

Table 2. Technical VPN risk scenarios and verification checklist

Risk area	Potential failure mode	Potential severity	Recommended verification
Tunnel protocol and cryptographic configuration	Weak/obsolete protocols, inadequate cipher configuration, poor key management, or unpatched clients may reduce confidentiality and integrity.	High	Record protocol/version and negotiated algorithms; review configuration against current organizational guidance; verify certificate/key validation and update status. [10], [11]
DNS and IPv6 routing	DNS queries or IPv6 packets may bypass the intended tunnel and reveal queried domains or endpoint traffic to an on-path observer.	High	Capture traffic at the client and an external interface; compare DNS resolver destinations; test IPv4 and IPv6 routes; repeat during reconnect and network changes. [9], [12]

©2025. JACODI. This work is openly licensed via CC BY 4.0.

Provider logging and data handling	The VPN gateway may observe connection metadata; unclear retention or sharing practices can create privacy risk.	High	Review privacy notice and data-processing terms; record stated retention, sharing, jurisdiction, and contact; treat statements as claims until technically or contractually validated. [6], [13]
Mobile-app supply chain	Third-party SDKs, excessive permissions, tracking components, or traffic manipulation can undermine user expectations.	High	Record app version, publisher, permissions, SDK inventory, network destinations, and observable traffic changes; document reproducible evidence. [9], [13]
Tunnel failure behavior	When the tunnel disconnects, fail-open behavior may route traffic through the ordinary interface without user awareness.	Medium–High	Force controlled disconnects and network changes; verify kill-switch behavior and whether traffic exits outside the tunnel before reconnection.
Blocked-site access and legal compliance	Changing the route may alter network reachability but does not determine whether the content or transaction is lawful.	Context-dependent	Record the network condition and technical mechanism separately from the content, purpose, user conduct, and applicable legal rule. [1]–[8]

3.4. Proposed reproducible evaluation protocol

To move from document-based synthesis to an empirical system-information study, future work should test a controlled sample of VPN clients rather than infer their properties from promotional descriptions. A minimum protocol should specify (1) a dated inventory of application name, publisher, version, platform, and installation source; (2) a test environment with controlled IPv4/IPv6 connectivity and known DNS resolvers; (3) packet capture before, during, and after tunnel activation; (4) controlled tunnel failures, DNS requests, and IPv6 requests; (5) inspection of permissions and third-party network destinations; and (6) evidence retention that avoids collecting unnecessary personal data. The test should use only test accounts and benign destinations and should not attempt to access illegal content.

For each test case, the report should record preconditions, expected behavior, observed behavior, evidence artifact, and pass/fail criteria. Examples include: all test DNS queries remain on the configured path while the tunnel is active; IPv4 and IPv6 behavior matches the documented policy; the kill switch prevents ordinary egress during tunnel failure; the app does not transmit undisclosed identifiers to unexpected endpoints; and privacy statements accurately disclose relevant collection and retention. A negative result must be reproducible and tied to a particular software version. The protocol aligns with risk governance principles such as identifying assets and threats, selecting protection measures, monitoring behavior, and communicating residual risk [13]. No pass/fail outcomes are reported in this article because the protocol has not yet been executed.

3.5. Discussion implications, prior work, and limitations

The proposed framework extends the conversation beyond a binary question of whether VPN use is "legal" or "illegal." It separates three analytical layers: the network service, the provider's processing and security practices, and the user's conduct through the service. This separation makes the resulting assessment more actionable. A technical reviewer can test tunnel behavior and privacy controls; a compliance reviewer can determine the role of the provider and applicable legal duties; and a content-enforcement analysis can examine the relevant material and the specific conduct alleged. Conflating these layers risks both technical overclaiming and legal overgeneralization.

©2025. JACODI. This work is openly licensed via CC BY 4.0.

The technical findings are consistent with the direction of prior empirical work. Ikram et al. examined 283 Android applications and documented, among other issues, insecure tunneling, DNS/IPv6 leakage, TLS interception, and traffic manipulation in some applications [9]. The present article does not reproduce those measurements or claim that the same problems persist in all modern apps. Its contribution is instead to translate those failure categories into an Indonesian governance context and a repeatable set of proposed checks. NIST's IPsec guide similarly supports the principle that VPN security depends on implementation and operational configuration [10], while the NIST Cybersecurity Framework 2.0 offers a broader risk-management vocabulary for identifying, protecting, detecting, responding, and recovering from cyber risks [13].

The practical implication for users is to treat VPN selection as a trust decision. A VPN can move some trust from the local access network to the VPN operator; it cannot eliminate trust requirements. Organizations should define an approved-service profile and verify routing, DNS, IPv6, failure handling, patching, and provider transparency. Application publishers should document data collection, retention, sharing, and security limitations in plain language. Regulators and reviewers should state the specific legal basis and the regulated entity rather than describe a broad even using AI [14], unverified VPN permit requirement. Any proposed restriction or blocking process should also be distinguished from the technical fact that a tunnel can alter network reachability.

The study has three principal limitations. First, it is based on public legal materials and selected technical literature rather than field interviews or empirical measurement. Second, it does not test individual VPN products, so it cannot rank products, quantify leak rates, or verify the accuracy of provider privacy statements. Third, it does not provide a comparative analysis of VPN law across jurisdictions. These limitations constrain the conclusions to a document-based risk and regulatory mapping. An empirical follow-up should preregister a sample, use a transparent test harness, archive reproducible evidence, and re-check the regulatory status and consolidated text of relevant laws at the date of publication.

4. CONCLUSION

This article has mapped VPN-related technical risks to Indonesia's electronic-system, personal-data, and content-related regulatory framework. The central finding is that the VPN mechanism, the provider's system and data-processing role, and the user's conduct must be examined separately. The sources reviewed do not support an unqualified claim that every VPN application needs a dedicated VPN-specific permit, nor do they establish that every connection to a blocked website automatically constitutes a criminal offense. Relevant duties and legal consequences depend on the applicable provisions, the role of the entity, the specific act and content, and the facts of the case.

For technical assessment, the article proposes verification of tunnel configuration, DNS and IPv6 routing, provider data practices, mobile-app behavior, and fail-open conditions. These controls provide a concrete basis for future empirical research and for more precise discussion in a computing and digital-information journal. Because no application was tested in this study, no product-specific performance or security conclusion is claimed. Future work should implement the protocol, publish version-specific measurements, and reassess current legal texts before drawing product-level or enforcement-level conclusions.

ACKNOWLEDGMENTS

The authors acknowledge the academic guidance provided during preparation of the original manuscript. Any funding or institutional support should be added here only if applicable and confirmed by the authors.

REFERENCES

[1] Republic of Indonesia, "Law No. 11 of 2008 concerning Electronic Information and Transactions," State Gazette of the Republic of Indonesia, No. 58, 2008. Available: https://peraturan.bpk.go.id/Details/37589/uu-no-11-tahun-2008

[2] Republic of Indonesia, "Law No. 19 of 2016 concerning Amendment to Law No. 11 of 2008 concerning Electronic Information and Transactions," State Gazette of the Republic of Indonesia, No. 251, 2016.

©2025. JACODI. This work is openly licensed via CC BY 4.0.

[3] Republic of Indonesia, "Law No. 1 of 2024 concerning the Second Amendment to Law No. 11 of 2008 concerning Electronic Information and Transactions," State Gazette of the Republic of Indonesia, No. 1, 2024. Available: https://peraturan.bpk.go.id/Details/274494/uu-no-1-tahun-2024

[4] Republic of Indonesia, "Government Regulation No. 71 of 2019 concerning the Operation of Electronic Systems and Transactions," State Gazette of the Republic of Indonesia, No. 185, 2019. Available: https://peraturan.bpk.go.id/Details/122030/pp-no-71-tahun-2019

[5] Ministry of Communication and Informatics of the Republic of Indonesia, "Ministerial Regulation No. 5 of 2020 concerning Private Electronic-System Operators," State Bulletin of the Republic of Indonesia, No. 1376, 2020, as amended by Ministerial Regulation No. 10 of 2021. Available: https://jdih.komdigi.go.id/produk_hukum/view/id/759

[6] Republic of Indonesia, "Law No. 27 of 2022 concerning Personal Data Protection," State Gazette of the Republic of Indonesia, No. 196, 2022. Available: https://peraturan.bpk.go.id/Details/229798/uu-no-27-tahun-2022

[7] Republic of Indonesia, "Law No. 44 of 2008 concerning Pornography," State Gazette of the Republic of Indonesia, No. 181, 2008. Available: https://peraturan.bpk.go.id/Details/39740/uu-no-44-tahun-2008

[8] Republic of Indonesia, "Law No. 1 of 2023 concerning the Criminal Code," State Gazette of the Republic of Indonesia, No. 1, 2023. Effective 2 January 2026. Available: https://peraturan.bpk.go.id/Details/234935/uu-no-1-tahun-2023

[9] M. Ikram, H. J. Asghar, M. A. Kaafar, A. Mahanti, and B. Singh, "An Analysis of the Privacy and Security Risks of Android VPN Permission-enabled Apps," in Proc. 2016 ACM Internet Measurement Conference, Santa Monica, CA, USA, 2016, pp. 349–364, doi: 10.1145/2987443.2987471.

[10] E. Barker, Q. Dang, S. Frankel, K. Scarfone, and P. Wouters, "Guide to IPsec VPNs," NIST Special Publication 800-77 Rev. 1, National Institute of Standards and Technology, Gaithersburg, MD, 2020, doi: 10.6028/NIST.SP.800-77r1.

[11] S. Kent and K. Seo, "Security Architecture for the Internet Protocol," Internet Engineering Task Force, RFC 4301, Dec. 2005. Available: https://www.rfc-editor.org/rfc/rfc4301

[12] P. Hoffman and P. McManus, "DNS Queries over HTTPS (DoH)," Internet Engineering Task Force, RFC 8484, Oct. 2018. Available: https://www.rfc-editor.org/rfc/rfc8484

[13] C. Pascoe, S. Quinn, and K. Scarfone, "The NIST Cybersecurity Framework (CSF) 2.0," NIST Cybersecurity White Paper 29, National Institute of Standards and Technology, Gaithersburg, MD, 2024, doi: 10.6028/NIST.CSWP.29.

[14] M. I. Wahyudi and S. J. Sa'idu, "Artificial Intelligence Similarity Index Detection App as an Anti-Plagiarism Campaign Against Intellectual Property Crime," Digital Muslim Review, 1(2), (2023): pp. 120-130.

©2025. JACODI. This work is openly licensed via CC BY 4.0.