Jurnal RechtsVinding Media Pembinaan Hukum Nasional ISSN 2089-9009
Volume 14 Nomor 2, Agustus 2025

REFORMASI HUKUM KEAMANAN SIBER DI INDONESIA: KEDAULATAN NASIONAL DAN TANGGUNG JAWAB GLOBAL

(Cybersecurity Law Reform in Indonesia: National Sovereignty and Global Responsibility)

Johanes De Brito Siga Nono
Fakultas Hukum Universitas Nusa Cendana
Jl. Adisucipto Penfui, Kupang, NTT, Indonesia
Email : Johanes_nono@staf.undana.ac.id

Abstrak

Keamanan siber global saat ini menghadapi tantangan yang semakin kompleks, dengan ancaman siber yang bersifat lintas batas dan berkembang pesat. Dalam konteks ini, Indonesia, sebagai negara dengan ekonomi digital yang semakin berkembang, harus menghadapi dilema antara mempertahankan kedaulatan nasional atas data dan infrastruktur kritisnya, serta berperan aktif dalam kolaborasi internasional untuk mengatasi ancaman siber global. Artikel ini membahas tantangan yang dihadapi Indonesia dalam merancang dan mengimplementasikan kebijakan hukum keamanan siber yang seimbang antara kedaulatan nasional dan tanggung jawab internasional. Penelitian ini menggunakan pendekatan normatif yuridis dengan metode analisis kualitatif untuk mengeksplorasi dinamika reformasi hukum keamanan siber di Indonesia. Melalui pendekatan normatif yuridis dengan metode analisis kualitatif serta dukungan bahan hukum sekunder dalam melakukan pendekatan deskriptif-analitis artikel ini mengidentifikasi kelemahan dalam kerangka hukum yang ada serta memberikan rekomendasi untuk reformasi hukum yang lebih adaptif dan berbasis kolaborasi internasional. Dengan mengintegrasikan aspek kedaulatan nasional dan tanggung jawab global, artikel ini menawarkan solusi yang dapat menjembatani kesenjangan antara kebijakan domestik dan global dalam keamanan siber. Reformasi hukum yang diajukan diharapkan dapat memperkuat ketahanan siber Indonesia sambil mendukung upaya global dalam menciptakan ruang siber yang lebih aman dan berkelanjutan.

Kata Kunci: Keamanan Siber, Kedaulatan Nasional, Kolaborasi Internasional, Reformasi Hukum

Abstract

Global cybersecurity is currently facing increasingly complex challenges, with threats that are transnational in nature and rapidly evolving. In this context, Indonesia as a country with a rapidly growing digital economy must navigate the dilemma between maintaining national sovereignty actively participating in international cooperation. This article explores the challenges faced by Indonesia. By employing a normative juridical approach combined with qualitative analysis, this study examines the dynamics of cybersecurity law reform in Indonesia. Through descriptive analytical methods and the use of secondary legal materials, this article identifies existing gaps in the current legal framework and offers recommendations for more adaptive legal reforms. By integrating the principles of national sovereignty with global responsibility, the article proposes legal solutions that bridge the gap between domestic and international cybersecurity policies. The proposed legal reforms are expected to enhance Indonesia's cyber resilience

Keywords: *Cybersecurity, National Sovereignty, International Cooperation, Legal Reform*

A. Pendahuluan

Dalam beberapa tahun terakhir ini, Indonesia telah mengalami perkembangan pesat di sektor digital. Hal ini dapat dilihat dari peningkatan jumlah pengguna internet yang signifikan, perluasan adopsi teknologi finansial[1], serta digitalisasi layanan publik yang semakin masif baik pada berbagai sektor. Pergeseran ini turut berpengaruh terhadap struktur sosial, ekonomi dan politik di Indonesia, dimana makin merujuk pada masyarakat digital yang lebih terhubung. Namun, perkembangan ini turut membawa ancaman nyata di dunia digital. Seiring dengan perkembangan internet yang pesat, terbuka pula kesempatan bagi penggunanya untuk memanfaatkan internet, untuk tujuan baik maupun untuk tujuan jahat.[2] Hal ini tergambar dari banyaknya serangan peretasan, penyebaran *malware*, pencurian terhadap data pribadi, dan serangan terhadap infrastruktur kritis negara[3]. Fenomena ini cukup untuk menunjukan bahwa penanganan terkait hal ini menjadi suatu hal yang sangat mendesak.

Namun, respons hukum yang ada saat ini cenderung berfokus pada penguatan kedaulatan negara di dunia digital. Hal ini tercermin dalam peraturan-peraturan nasional seperti Undang-Undang Informasi dan Transaksi Elektronik (UU ITE), Undang-Undang Perlindungan Data Pribadi (UU PDP), serta berbagai regulasi sektoral lainnya. Dalam hal ini negara menempatkan diri menjadi pihak utama dalam pengelolaan data dan pengawasan konten di dunia maya. Meskipun logika kedaulatan merupakan hal yang sangat fundamental demi menjaga kepentingan nasional, namun negara juga menghadapi tantangan besar ketika dihadapkan pada ancaman siber yang bersifat lintas negara, yang berada di luar yurisdiksi hukum nasional.

Kerentanan hukum nasional dalam mengantisipasi serangan yang bersifat global dalam ekosistem digital inilah yang membuat Indonesia kesulitan merespons serangan siber dari luar negeri, mengakses bukti digital lintas batas, serta mengkoordinasikan respons insiden secara efisien. Ketiadaan kerja sama internasional yang efektif, seperti ketidakterlibatan Indonesia dalam kerangka hukum internasional, seperti Konvensi Budapest mengenai Kejahatan Siber, juga semakin memperburuk keterbatasan dalam menghadapi kejahatan siber lintas negara.

Melalui artikel ini, penulis mengevaluasi kondisi hukum keamanan siber di Indonesia, dengan menyoroti ketegangan antara kedaulatan nasional dan kerentanan global. Diharapkan dengan sumbangan pemikiran melalui artikel ini dapat memberikan kontribusi yang signifikan dalam reformasi hukum keamanan siber Indonesia yang lebih relevan dan siap menghadapi tantangan di masa depan.

B. Metode Penulisan

Penelitian ini menggunakan pendekatan normatif yuridis dengan metode analisis kualitatif untuk mengeksplorasi dinamika hukum keamanan siber di Indonesia, khususnya

---

1 Lee Kuan Yew School of Public Policy, "The Rise of Indonesia's Digital Economy" National University of Singapore (2025). https://lkyspp.nus.edu.sg/docs/default-source/case-studies/the-rise-of-indonesia-s-digital-economy.pdf?sfvrsn=c607020a_0 (diakses 31 Mei 2025). .

2 Book Chapter 6 in Colarik, Andrew, Julian Jang-Jaccard, and Anuradha Mathrani, eds. Cyber Security and Policy : A Substantive Dialogue. Auckland, New Zealand: Massey University Press, 2017. Hal. 66.

3 Intan Rakhmayanti Dewi, "Serangan Ransomware pada Pusat Data Nasional," https://www.cnbcindonesia.com/tech/20240627081538-37-549695/pusat-data-nasional-kena-ransomware-guru-besar-it-angkat-bicara, CNBC Indonesia (diakses 27 Mei 2025)

dalam konteks ketegangan antara prinsip kedaulatan nasional dan tuntutan kolaborasi global. Pendekatan ini dipilih karena fokus utama kajian terletak pada analisis norma-norma hukum, baik yang bersumber dari sistem hukum nasional maupun dari instrumen hukum internasional yang relevan. Sumber data dalam penelitian ini terdiri dari bahan hukum primer, termasuk peraturan perundang-undangan yang relevan seperti Undang-Undang Informasi dan Transaksi Elektronik (UU ITE), Undang-Undang Perlindungan Data Pribadi (UU PDP), serta regulasi teknis yang diterbitkan oleh Badan Siber dan Sandi Negara (BSSN).

Selain itu, penelitian ini juga mengkaji instrumen hukum internasional seperti Konvensi Budapest tentang Kejahatan Siber. Bahan hukum sekunder turut digunakan untuk memperkaya analisis, berupa literatur akademik. Pengumpulan data dilakukan melalui studi pustaka secara sistematis. Data yang diperoleh dianalisis dengan pendekatan deskriptif-analitis untuk mengidentifikasi kesesuaian, kelemahan, dan kesenjangan antara kerangka hukum nasional Indonesia dan standar hukum internasional. Berdasarkan hasil analisis tersebut, penelitian ini merumuskan rekomendasi hukum yang menyeimbangkan perlindungan atas kedaulatan digital Indonesia dengan kebutuhan kolaborasi internasional dalam merespons ancaman siber yang semakin transnasional dan kompleks.

C. Pembahasan

Kemajuan teknologi digital telah mendefinisikan ulang cara negara menjalankan kedaulatannya, termasuk dalam ranah keamanan siber. Di Indonesia, pendekatan hukum dalam menghadapi tantangan dunia digital masih sangat berakar pada prinsip kedaulatan nasional[4]. Hal ini tercermin dalam penguatan regulasi domestik seperti UU ITE dan UU PDP, serta peran sentral Badan Siber dan Sandi Negara (BSSN) dalam menjaga ruang siber nasional. Namun, realitas di lapangan menunjukkan bahwa ancaman siber kian bersifat lintas batas dan kompleks[5], membuat pendekatan hukum yang berfokus pada batas teritorial menjadi kurang memadai. Fragmentasi kebijakan, lemahnya kerja sama lintas negara, dan keterlibatan terbatas Indonesia dalam forum global membuat respons terhadap insiden siber sering kali berjalan lambat dan tidak efektif. Situasi ini menuntut adanya reformasi hukum yang lebih terbuka dan adaptif.

Perlindungan terhadap kedaulatan digital tetap penting, namun perlu disandingkan dengan keterlibatan aktif dalam norma dan mekanisme internasional. Mengadopsi prinsip-prinsip dari Konvensi Budapest secara selektif serta menyelaraskan hukum nasional dengan standar global menjadi langkah strategis yang tidak hanya melindungi kepentingan domestik, tetapi juga memperkuat posisi Indonesia dalam tata kelola siber global. Dengan pendekatan yang seimbang ini, Indonesia berpeluang membangun kerangka hukum keamanan siber yang lebih tangguh, kolaboratif, dan siap

[4] Adonis, Abid A. "Critical Engagement on Digital Sovereignty in International Relations: Actor Transformation and Global Hierarchy." Global: *Jurnal Politik Internasional* 21, no. 2 (2019):262-. doi:10.7454/globalv21i2.412.

[5] Kuzior, A., I. Tiutiunyk, A. Zielińska, and R. Kelemen. "Cybersecurity and Cybercrime: Current Trends and Threats." *Journal of International Studies* 17, no. 2 (2024). doi:https://doi.org/10.14254/2071-8330.2024/17-2/12.

menghadapi tantangan dunia digital yang terus berkembang.

1. Kedaulatan Nasional dan Batasan Hukum Keamanan Siber Indonesia

Kedaulatan adalah prinsip dasar dalam sistem hukum internasional yang memberi negara hak eksklusif untuk mengatur urusan di wilayahnya. Dalam era digital, konsep ini berkembang menjadi kedaulatan siber, yang mengacu pada kewenangan negara untuk mengatur dan mengontrol ruang siber di dalam yurisdiksinya, termasuk data, infrastruktur digital, dan aktivitas siber masyarakat. Di Indonesia, pendekatan terhadap hukum keamanan siber sebagian besar didorong oleh prinsip kedaulatan ini. Negara berusaha memastikan otoritasnya dalam dunia digital melalui berbagai perangkat hukum dan lembaga untuk menjaga keamanan nasional, melindungi integritas informasi, dan melindungi kepentingan publik.

Kerangka hukum yang mendasari pendekatan ini tersebar dalam beberapa regulasi penting. Salah satunya adalah Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE), yang telah diperbaharui menjadi UU Nomor 19 Tahun 2016 . UU ini menjadi dasar pengaturan aktivitas elektronik dan penegakan hukum di dunia maya. Selain memfasilitasi transaksi elektronik dan komunikasi digital, UU ITE juga mencakup ketentuan pidana terkait konten yang mengandung kebencian, hoaks, dan pencemaran nama baik, yang memperkuat kontrol negara terhadap arus informasi di internet.

Selain UU ITE, Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi (UU PDP) menandai langkah penting dalam memperkuat peran negara dalam pengelolaan data pribadi oleh sektor publik dan swasta[6]. UU ini mewajibkan data pribadi warga negara Indonesia yang diproses oleh entitas digital, baik dalam negeri maupun luar negeri, untuk mematuhi prinsip dan ketentuan hukum nasional. Regulasi mengenai perlindungan data pribadi telah disusun dan implementasikan oleh banyak negara.[7] Salah satu kebijakan penting dalam UU PDP adalah pelokalan data (*data localization*), yang mengharuskan beberapa entitas digital untuk menyimpan dan memproses data di wilayah Hukum Negara Republik Indonesia, guna menjaga kedaulatan data dan memastikan keamanan informasi strategis. Selain itu, regulasi ini juga dapat digunakan untuk tujuan yang lebih luas berkaitan dengan melindungi kepentingan dari pengguna itu sendiri seperti yang telah diimplemetasikan oleh negara-negara di Eropa[8].

Peran Badan Siber dan Sandi Negara (BSSN) sebagai lembaga yang bertanggung jawab atas kebijakan dan pengendalian keamanan siber nasional semakin penting dalam implementasi

---

6 Prasetyoningsih, N., Ismail Nawang, N., Putri, W.V., Amirullah, M.N.R. (2024). Legal Protection for the Personal Data in Indonesia and Malaysia. In: Moallem, A. (eds) HCI for Cybersecurity, Privacy and Trust. HCII 2024. Lecture Notes in Computer Science, vol 14728. Springer, Cham. https://doi-org.ezproxy2.library.drexel.edu/10.1007/978-3-031-61379-1_11. Hal. 164

7 Ghosh, J., Sinha, V.K. (2024). Big Data Analytics in Industry 4.0 in Legal Perspective: Past, Present and Future. In: Kumar, A., Sagar, S., Thangamuthu, P., Balamurugan, B. (eds) Digital Transformation. Disruptive Technologies and Digital Transformations for Society 5.0. Springer, Singapore. https://doiorg.ezproxy2.library.drexel.edu/10.1007/978-981-99-8118-2_7.

8 Book Chapter Two of Barker, Jessica. Confident Cyber Security : The Essential Insights and How to Protect from Threats. Second edition. London, England: Kogan Page Limited, 2023. Hal. 4.

kebijakan ini. BSSN mengatur pelaksanaan Standar Teknis Keamanan Informasi (STKI), pemantauan trafik siber yang anomali, serta audit keamanan informasi pada lembaga pemerintah dan sektor vital nasional. Melalui BSSN, negara memperkuat kapasitasnya dalam membangun ketahanan siber dan merespons insiden siber secara terpusat.

Namun, meskipun pendekatan ini mengutamakan kedaulatan, ada beberapa tantangan yang perlu dihadapi. Pertama, fragmentasi regulasi dan ketidaksinkronan antar lembaga negara menciptakan tumpang tindih kewenangan, ketidakpastian hukum, dan lambannya koordinasi dalam menghadapi serangan siber yang semakin kompleks[9].

Kedua, pendekatan yang terlalu represif ini cenderung mengabaikan pembangunan ketahanan jangka panjang[10], seperti peningkatan kapasitas teknis, budaya keamanan siber, dan keterlibatan masyarakat sipil dalam tata kelola digital. Fokus yang besar pada penindakan hukum dan kontrol konten malah mengesampingkan pentingnya pendidikan keamanan digital. Padahal, kurangnya literasi digital dikalangan masyarakat juga masih menjadi problem[11] yang masih menjadi persoalan tersendiri dan perlu perhatian khusus dari pemerintah. Selain itu, peraturan yang telah diterapkan juga cenderung menghambat pembangunan ekosistem yang inklusif dan partisipatif. Hal ini ditandai dengan aturan yang tergambar dalam UU ITE serta Peraturan Menteri Komunikasi dan Informatika Nomor 5 Tahun 2020 yang lebih mengedepankan kekuasaan absolut pemerintah terhadap penggunaan platform digital yang beroperasi di Indonesia[12]. Kemajuan teknologi yang pesat ini juga perlu dimanfaatkan bukan hanya untuk memperbaiki sistem yang cacat, tetapi juga untuk merancang tatanan masyarakat baru yang menjaga kualitas hidup tinggi tanpa mengambil hak-hak dasar dari masyarakat itu sendiri[13].

Ketiga, pendekatan kedaulatan nasional seringkali tidak sejalan dengan kebutuhan akan kerja sama internasional dalam menghadapi ancaman siber yang bersifat transnasional[14]. Tanpa adanya kerangka kerja sama yang solid di tingkat global, Indonesia menghadapi keterbatasan dalam mengakses bukti digital lintas batas, menindak pelaku serangan siber dari luar negeri, serta berbagi informasi secara real-time dengan negara lain.

Keempat, adanya kerentanan dalam pengelolaan data pribadi karena kurangnya kapasitas pengawas data dan mekanisme

---

9 Gatra Priyandita, "Indonesia's Cybersecurity Woes: Reflections for the Next Government" *CSIS Commentaries CSISCOM00624*(2024).https://s3-csis-web.s3.ap-southeast1.amazonaws.com/doc/CSIS_Commentaries_CSISCOM00624.pdf?download=1

10 Sangeeta Mahapatra. Repression by Legal Means: Governments' Anti-Fake News Lawfare. German Institute of Global and Area Studies GIGA, n.d.

11 Norman Harsono. "Despite improvements, Indonesia's digital literacy remains low" The Jakarta Post (2022). https://www.thejakartapost.com/business/2022/01/20/despite-improvements-indonesias-digital-literacy-remains-low.html (Diakses 29 Mei 2025)

12 Abdurrohim, Muhammad, Indah Kumalasari, and Fathur Rosy. "The Paradox of Indonesia Cyberspace Policy and Cooperation: Neoclassical Realism Perspective." Jurnal Hubungan Internasional. (Yogyakarta) 11, no. 2 (2022): 13–23. doi:10.18196/jhi.v11i2.14361.

13 Book Chapter Two of Geng, Hwaiyu, ed. The Internet of Things and Data Analytics Handbook. 1st ed. Hoboken, New Jersey: John Wiley & Sons, 2008. doi:10.1002/9781119173601. Hal. 39

14 Lazari C.C. "Cybersecurity and Sovereignty in Cyberspace: Challenges and Prospects of International Law". *Moscow Journal of International Law*. 2025;(1):125-137. (In Russ.) https://doi.org/10.24833/0869-0049-2025-1-125-137.

keamanan hukum yang berpotensi meng-akibatkan penyalahgunaan data oleh pihak yang tidak bertanggungjawab[15]. Oleh karena itu dibutuhkan tenaga professional yang dapat bertanggung jawab dalam menangkal ancaman dan mengembangkan cara yang lebih efektif untuk melindungi data pribadi[16]. Selain itu, kesalahan dalam mengawasi data personal juga dapat menimbulkan dampak negatif, seperti kerugian finansial, korban jiwa, dan ancaman terhadap keamanan nasional[17]. Tidak dapat dipungkiri pula bahwa perkembangan internet yang masif ini pula dapat dijadikan bagian dalam memperluas aksi teroris lintas negara[18], sehingga perlindungan data pribadi menjadi suatu hal yang sangat krusial.

Meskipun pendekatan kedaulatan nasional memiliki nilai strategis untuk melindungi kepentingan negara dan warganya, hukum keamanan siber Indonesia saat ini belum sepenuhnya mampu mengatasi kompleksitas ancaman global. Oleh karena itu, reformasi kerangka hukum dan tata kelola diperlukan agar prinsip kedaulatan digital dapat diintegrasikan dengan kebutuhan akan interoperabilitas global dan respons multilateral terhadap ancaman siber yang terus berkembang.

2. Ketimpangan Regulasi Nasional dan Realitas Ancaman Global

Ruang siber saat ini menjadi arena yang melampaui batas-batas geografis konvensional. Serangan siber bisa dilakukan dari satu negara ke negara lain tanpa harus melintasi perbatasan fisik. Aktor-aktor siber, baik yang berasal dari negara maupun non-negara, dapat menyamarkan identitas dan lokasi mereka menggunakan teknik digital yang canggih[19].

Fenomena ini menciptakan apa yang disebut dengan kerentanan global, sebuah kenyataan di mana negara-negara, termasuk Indonesia, terpapar pada ancaman lintas batas yang saling terkait dan sering kali tidak bisa diatasi secara sepihak. Salah satu kasus yang menjadi sorotan publik yakni bocornya data pribadi warga Indonesia yang dikelola oleh Badan Penyelenggara Jaminan Sosial (BPJS) di internet[20]. Dalam konteks ini, pendekatan hukum nasional menghadapi banyak keterbatasan, baik dalam hal yurisdiksi, penegakan hukum, maupun kerja sama internasional.

Salah satu bentuk nyata dari kerentanan global ini adalah meningkatnya serangan

---

15 Kurniawan, Kukuh Dwi, Deassy J. A. Hehanussa, Rahmat Setiawan, Indah Susilowati, Sopian, and Desmarani Helfisar. 2024. "Criminal Sanctions and Personal Data Protection in Indonesia". *Lex Publica* 11 (2):221-47. https://doi.org/10.58829/lp.11.2.2024.1-27.

16 Book Chapter Three of Anunciacao, Pedro Fernandes, Claudio Roberto Magalhaes Pessoa, and George Leal Jamil, eds. Digital Transformation and Challenges to Data Security and Privacy. Hershey, Pennsylvania: IGI Global, 2021. doi:10.4018/978-1-7998-4201-9. Hal 40 .

17 Book Chapter One of Guidetti, Oliver, Mohiuddin Ahmed, and Craig Speelman. Psybersecurity : Human Factors of Cyber Defence. 1st ed. Boca Raton: Taylor & Francis Group, 2024.

18 Book Chapter Thirteen of Reich, Pauline C, and Eduardo Gelbstein. Law, Policy, and Technology: Cyberterrorism, Information Warfare, and Internet Immobilization. Hershey, PA: Information Science Reference, 2012. doi:10.4018/978-1-61520-831-9. Hal. 356

19 Farber, Shai. "The Evolving Nexus of Cybercrime and Terrorism: A Systematic Review of Convergence and Policy Implications." Security Journal 38, no. 1 (2025). doi:10.1057/s41284-025-00471-7.

20 Yakub Pryatama Wijayaatmaja. "Soal Kebocoran Data BPJS Kesehatan, Polri Dalami Peran IT" Media Indonesia (2021). https://mediaindonesia.com/politik-dan-hukum/409284/soal-kebocoran-data-bpjs-kesehatan-polri-dalami-peran-it (Diakses 28 Mei 2025)

terhadap infrastruktur kritis nasional[21]. Sebagai contoh, menurut BSSN, Indonesia mencatat terjadi serangan siber yang sangat masif pada tahun 2019. Jumlah ini melonjak secara drastis yang hampir menyentuh dua kali lipat dari jumlah insiden hanya dalam lima bulan pertama tahun 2021[22]. Sebagian besar serangan ini memerlukan respons teknis dan hukum yang melibatkan kolaborasi lintas negara. Namun, terbatasnya mekanisme kerja sama internasional menyebabkan proses investigasi, pertukaran data digital, dan penegakan hukum menjadi sangat lambat, bahkan sering kali tidak memungkinkan untuk dilakukan. Sebagai tambahan, UU Nomor 19 Tahun 2016 yang dipercaya dapat menanggulangi krisis ini juga tak mampu menjadi ujung tombak dalam menghadapi persoalan mengenai serangan siber[23].

Di tingkat internasional, masih terdapat kesenjangan normatif terkait standar pengaturan dan penegakan hukum di ruang siber. Tidak adanya konvensi global yang mengikat secara universal mengenai keamanan siber membuat negara-negara mengembangkan kerangka hukum masing-masing, yang sering kali memiliki orientasi yang berbeda-beda. Indonesia, misalnya, belum meratifikasi Konvensi Budapest tentang Kejahatan Siber[24], satu-satunya instrumen internasional yang saat ini menjadi referensi dalam penanggulangan kejahatan siber lintas negara. Ketidakterlibatan Indonesia dalam konvensi ini memperlemah posisi negara dalam membangun kerja sama ekstradisi, bantuan hukum timbal balik (*mutual legal assistance*), serta investigasi bersama yang sangat penting untuk menangani serangan siber yang berasal dari luar negeri.

Di sisi lain, hukum nasional Indonesia cenderung berfokus pada urusan domestik dan belum sepenuhnya disesuaikan untuk mengatasi kompleksitas ancaman siber global. Undang-Undang Informasi dan Transaksi Elektronik (UU ITE) serta Undang-Undang Perlindungan Data Pribadi (UU PDP), misalnya, tidak menyediakan mekanisme yang memadai untuk koordinasi lintas yurisdiksi, baik dalam hal perolehan bukti digital maupun penindakan terhadap pelaku yang berasal dari negara lain. *Deepfakes* menjadi salah satu contoh nyata dalam hal ini, pesatnya perkembangan teknologi *deepfakes* ini telah melampaui kerangka hukum yang ada dimana dapat menjadi tantangan tersendiri bagi analis forensik digital dan lembaga hukum dalam menjalankan perannya.[25] Selain itu, kebijakan mengenai kewajiban data localization dapat

---

21 Nikita Dewi Kurnia Salwa. "Tantangan & Hambatan Besar yang Dihadapi CSIRT-BSSN Indonesia" CSIRT (2024). https://csirt.or.id/pengetahuan-dasar/tantangan-csirt-bssn#:~:text=CSIRT%20(Computer%20Security%20Incident%20Response,tantangan%20yang%20memerlukan%20perhatian%20serius. (Diakses 28 Mei 2025)

22 Ananda Putra. "Serangan Siber di RI Terus Meningkat, Capai 448 Juta Kasus". Media Indonesia (2021). https://mediaindonesia.com/politik-dan-hukum/414225/serangan-siber-di-ri-terus-meningkat-capai-448-juta-kasus (Diakses 29 Mei 2025)

23 MKRI. "Sejumlah Pencipta Konten Persoalkan Unsur Pencemaran Nama Baik Dalam UU ITE" Mahkamah Tinggi Republik Indonesia (2022). https://www.mkri.id/index.php?page=web.Berita&id=18118&menu=2 (Diakses 29 Mei 20225).

24 Cartin-Pecson, R., Karsono, B., L. Sulastri, Z. Rony., and C. Chavez. "Defending the Digital Domain: A Critical Look at Cybercrime Legislation in Indonesia and the Philippines." *Academic Journal of Interdisciplinary Studies 14(2):198.* doi:10.36941/ajis-2025-0040

25 Montasari, R. (2024). Responding to Deepfake Challenges in the United Kingdom: Legal and Technical Insights with Recommendations. In: Cyberspace, Cyberterrorism and the International Security in the Fourth Industrial Revolution. Advanced Sciences and Technologies for Security Applications. Springer, Cham. https://doi-org.ezproxy2.library.drexel.edu/10.1007/978-3-031-50454-9_12.

memicu ketegangan diplomatik dengan negara-negara mitra serta membatasi interoperabilitas sistem keamanan digital yang beroperasi lintas negara.

Krisis ini semakin diperburuk oleh rendahnya keterlibatan Indonesia dalam forum-forum global yang membahas tata kelola siber secara inklusif[26], maupun kemitraan antara sektor publik dan swasta dalam memperkuat infrastruktur keamanan digital. Minimnya partisipasi Indonesia dalam perumusan norma global menjadikannya lebih sebagai objek kebijakan internasional daripada sebagai subjek yang dapat mempengaruhi arah tata kelola siber global. Indonesia pun dapat dikatakan tertinggal dari negara-negara tetangga di ASEAN.[27] Ini dapat dilihat dari pesatnya perkembangan teknologi keamanan siber serta regulasi yang mumpuni dari negara-negara ASEAN dalam upaya mengeliminasi ataupun meminimalisir serangan siber di wilayahnya.

Dengan menyadari runtuhnya garis pembatas antara nasional dan internasional dalam hal ini, pemerintah perlu untuk membentuk regulasi yang dapat meredakan lingkungan digital yang sangat dinamis dan rentan[28], sekaligus mendorong kolaborasi lintas negara untuk menghadapi ancaman siber yang bersifat transnasional. Kerentanan global ini menuntut negara-negara, termasuk Indonesia, untuk tidak hanya mengandalkan pendekatan hukum nasional yang bersifat teritorial dan berorientasi pada kedaulatan mutlak. Sebaliknya, diperlukan paradigma hukum keamanan siber yang dapat menyeimbangkan antara perlindungan kepentingan nasional dan pengembangan solidaritas internasional dalam menghadapi ancaman bersama. Tanpa penyesuaian terhadap realitas global ini, hukum keamanan siber Indonesia akan terus berada dalam posisi krisis: tidak cukup kuat untuk melindungi, dan tidak cukup fleksibel untuk berkolaborasi.

3. Reformasi Hukum Keamanan Siber Indonesia

Di tengah meningkatnya kompleksitas dan sifat lintas batas dari ancaman siber, Indonesia menghadapi kebutuhan mendesak untuk merumuskan ulang pendekatan hukum yang mampu menjembatani antara perlindungan kedaulatan nasional dan partisipasi aktif dalam tanggung jawab global. Keamanan siber kini tidak lagi dapat dipandang semata-mata sebagai isu domestik saja, namun telah menjadi bagian integral dari tantangan global yang menuntut koordinasi antarnegara dan penguatan mekanisme hukum internasional. Oleh karena itu, reformasi hukum keamanan siber di Indonesia perlu diarahkan pada penciptaan keseimbangan antara perlindungan atas data dan infrastruktur kritis nasional dengan keterlibatan konstruktif dalam sistem kerja sama keamanan siber internasional.

Di tingkat nasional, Indonesia telah mengembangkan sejumlah instrumen hukum

---

26 Albert Triwibowo. "The Characteristics of Indonesian Digital Diplomacy." JAS : *Journal of Asean Studies* 11, no. 1 (2023): 167–96. doi:10.21512/jas.v11i1.8525.

27 Putri, Kristiani Virgi Kusuma. 2021. "Kerja Sama Indonesia Dengan ASEAN Mengenai Cyber Security Dan Cyber Resilience Dalam Mengatasi Cyber Crime". *Jurnal Hukum Lex Generalis* 2 (7):542-54. https://doi.org/10.56370/jhlg.v2i7.90.

28 Chapter Twelve of Subramanian, Ramesh, ed. *Computer Security, Privacy and Politics: Current Issues, Challenges and Solutions.* Hershey, PA: IGI Global Scientific Publishing, 2008. https://doi-org.ezproxy2.library.drexel.edu/10.4018/978-1-59904-804-8. Hal. 378

penting, seperti Undang-Undang Informasi dan Transaksi Elektronik (UU ITE) serta Undang-Undang Perlindungan Data Pribadi (UU PDP). Pendekatan kepatuhan yang tepat memungkinkan Indonesia dapat mengelola akses pengguna secara berkelanjutan, bukan sekadar melalui audit satu kali yang minim kontribusi terhadap terciptanya lingkungan komputasi yang aman dan berkelanjutan[29]. Regulasi-regulasi ini menyediakan kerangka awal dalam merespons risiko digital dan melindungi data individu serta transaksi elektronik. Namun, dalam konteks keamanan siber yang bersifat transnasional, kerangka hukum tersebut masih menghadapi sejumlah keterbatasan[30]. Salah satu kelemahan utama terletak pada belum adanya mekanisme hukum yang jelas dan efisien untuk menangani kejahatan siber lintas yurisdiksi serta ketiadaan prosedur standar untuk kerja sama internasional dalam penegakan hukum digital.

Dalam upaya menjembatani kesenjangan ini, Konvensi Budapest tentang Kejahatan Siber seringkali dijadikan acuan internasional. Konvensi ini dapat memberikan kerangka hukum yang komprehensif mengenai yurisdiksi ekstrateritorial, pengumpulan bukti digital lintas batas, serta koordinasi dalam penegakan hukum siber. Meskipun Indonesia belum meratifikasi Konvensi Budapest, prinsip-prinsip yang dikandungnya tetap relevan sebagai acuan dalam harmonisasi hukum nasional. Ketidakhadiran Indonesia dalam kerangka hukum ini berisiko menghambat partisipasi negara dalam forum-forum global yang menangani serangan siber multinasional secara cepat dan terkoordinasi.

Lebih jauh, aktor-aktor internasional seperti International Telecommunication Union (ITU) dan United Nations Open-Ended Working Group (UN OEWG) telah menjadi platform penting dalam membangun norma global keamanan siber, termasuk prinsip transparansi, non-agresi digital, dan pembangunan kapasitas negara berkembang. Indonesia secara aktif berpartisipasi dalam diskusi yang difasilitasi oleh UN OEWG, namun partisipasi ini belum sepenuhnya tercermin dalam struktur hukum nasional. Sementara itu, ASEAN sebagai organisasi kawasan juga mendorong pendekatan regional terhadap keamanan siber, termasuk melalui ASEAN Cybersecurity Cooperation Strategy dan ASEAN Regional Computer Emergency Response Team (ASEAN CERT). Indonesia perlu mengadopsi pendekatan strategis seperti yang diterapkan oleh Singapura, yang mengembangkan keamanan sibernya melalui empat pilar utama dan pengakuan terhadap hukum internasional[31]. Langkah ini penting sebagai upaya memperkuat kerangka keamanan siber nasional yang responsif terhadap dinamika ancaman global dan selaras dengan norma internasional. Kerja sama ini membuka peluang bagi Indonesia untuk menyelaraskan kebijakan nasionalnya dengan standar regional, tanpa harus tunduk sepenuhnya pada sistem hukum negara-negara maju.

---

29 Book Chapter Twenty, Morey J. Haber, Darran Rolls. Identity Attack Vectors: Strategically Designing and Implementing Identity Security, Second Edition. Apress, 2024.

30 Sarjito, Aris. 2024. "Technological Pride and National Resilience: How Innovation Shapes Stability and Security". *Jurnal Lemhannas RI* 12 (3), 277-98. https://doi.org/10.55960/jlri.v12i3.940.

31 Ang, Benjamin, Scott N Romaniuk, and Mary Manjikian. "Singapore: A Leading Actor in ASEAN Cybersecurity." In Routledge Companion to Global Cyber-Security Strategy, 1st ed., 381–91. Routledge, 2021. doi:10.4324/9780429399718-35.

Namun demikian, resistensi terhadap ratifikasi penuh Konvensi Budapest masih terjadi[32], terutama karena kekhawatiran akan potensi pelanggaran terhadap kedaulatan digital nasional. Selain Australia yang meratifikasi konvensi Budapest dalam rangka pemenuhan strategi terkait keamanan siber dalam Cyber Security Strategy[33] serta Australia's International Cyber Engagement Strategy[34], sebagian pihak menilai bahwa keterbukaan terhadap kerja sama internasional dapat mengurangi kendali negara atas data strategis, terutama apabila melibatkan akses oleh lembaga penegak hukum asing. Oleh karena itu, reformasi hukum yang ideal bukanlah adopsi secara keseluruhan, melainkan pendekatan harmonisasi selektif. Dengan strategi ini, Indonesia dapat mengintegrasikan prinsip-prinsip substantif dari Konvensi Budapest ke dalam hukum nasional, dengan memastikan bahwa kedaulatan negara tetap menjadi prinsip utama.

Langkah reformasi ini memerlukan pemetaan menyeluruh terhadap norma-norma internasional yang kompatibel dengan sistem hukum Indonesia, serta penerapan prinsip kehati-hatian dalam mengadaptasi prosedur-prosedur hukum asing. Harmonisasi yang kontekstual ini akan memungkinkan Indonesia untuk mempertahankan kontrol atas ruang digital nasional, sambil memainkan peran aktif dalam pembangunan tatanan hukum global yang inklusif dan responsif terhadap ancaman siber. Selain itu, reformasi ini perlu mempertimbangkan munculnya teknologi baru seperti kecerdasan buatan (AI), *Internet of Things* (IoT), dan *blockchain*, yang masing-masing menimbulkan tantangan tersendiri dalam aspek regulasi, privasi, dan keamanan. Hal ini dikarenakan kemungkinan menurunnya peran manusia dalam pembangunan di masa yang akan datang[35].

Dengan demikian, reformasi hukum keamanan siber Indonesia seharusnya tidak hanya berorientasi pada penguatan kapasitas domestik, tetapi juga diarahkan untuk menciptakan sistem hukum yang kompatibel dengan norma dan praktik global. Pendekatan ini akan meningkatkan kemampuan Indonesia dalam menangani insiden siber yang bersifat transnasional serta memperkuat posisi negara dalam forum internasional, baik di tingkat ASEAN, ITU, maupun PBB. Kerangka hukum yang terintegrasi antara kedaulatan nasional dan tanggung jawab global inilah yang pada akhirnya akan mampu memberikan perlindungan maksimal terhadap data, infrastruktur digital, dan kepentingan strategis Indonesia dalam era siber yang saling terhubung.

D. Penutup

Pembangunan sistem keamanan siber yang tangguh dan berdaya saing global di

---

32 Auliaurrahman, Auliaurrahman, Nur Anshari, and Sunny Ummul Firdaus. "The Existence and Regulation of Cyber Law: The Government's Role in Combating Digital Crime in Indonesia." *Jurisprudensi: Jurnal Ilmu Syariah, Perundang-Undangan Dan Ekonomi Islam* 17, no. 1 (2025): 206-223.

33 Anu Stuparu. "Australia's Cybersecurity." In Routledge Companion to Global Cyber-Security Strategy, 1st ed., 381–91. Routledge, 2021. doi:10.4324/9780429399718-35.

34 Feakin, Tobias, Johanna Weaver, Eneken Tikk, and Mika Kerttunen. "Cyber Diplomacy: An Australian Perspective." In Routledge Handbook of International Cybersecurity, 1st ed., 277–85. Routledge, 2020. doi:10.4324/9781351038904-29.

35 Book Chapter One of Sergi, Bruno S, Elena G Popkova, Aleksei V Bogoviz, and Tatiana N Litvinova. Understanding Industry 4.0: AI, the Internet of Things, and the Future of Work. First edition. Bingley, UK: Emerald Publishing Limited, 2019. doi:10.1108/9781789733112. Hal. 5

Indonesia membutuhkan reformasi hukum yang mengintegrasikan prinsip kedaulatan nasional dengan tanggung jawab global. Pendekatan kedaulatan siber yang mengedepankan kontrol negara atas ruang digital nasional, meskipun penting untuk melindungi infrastruktur kritis dan data strategis, menghadapi tantangan besar akibat kerentanan global yang bersifat lintas batas. Ketidaksesuaian antara kerangka hukum domestik dan kebutuhan akan kerja sama internasional dalam menghadapi ancaman siber yang semakin kompleks menuntut adanya penyesuaian yang lebih mendalam terhadap standar global.

Reformasi hukum yang efektif harus mencakup harmonisasi regulasi domestik dengan prinsip-prinsip internasional, seperti yang diatur dalam Konvensi Budapest, tanpa mengorbankan kedaulatan negara. Adopsi prinsip-prinsip tersebut secara selektif dapat memperkuat kapasitas Indonesia dalam mengelola ancaman siber, baik di tingkat domestik maupun internasional, serta memfasilitasi kerja sama lintas batas yang lebih efisien. Selain itu, penting untuk mempertimbangkan perkembangan teknologi baru, seperti kecerdasan buatan, *Internet of Things*, dan *blockchain*, dalam merancang kerangka hukum yang adaptif dan responsif.

Secara keseluruhan, Indonesia perlu mengembangkan pendekatan hukum yang menyeimbangkan antara perlindungan kepentingan nasional dan partisipasi aktif dalam tatanan keamanan siber global. Reformasi hukum yang inklusif dan kolaboratif ini diharapkan dapat memperkuat ketahanan siber domestik sekaligus meningkatkan kontribusi Indonesia dalam menghadapi tantangan siber global.

Daftar Pustaka

Buku

Ang, Benjamin, Scott N Romaniuk, and Mary Manjikian. “Singapore: A Leading Actor in ASEAN Cybersecurity.” In Routledge Companion to Global Cyber-Security Strategy, 1st ed., 381–91. Routledge, 2021. doi:10.4324/9780429399718-35.

Anunciacao, Pedro Fernandes, Claudio Roberto Magalhaes Pessoa, and George Leal Jamil, eds. Digital Transformation and Challenges to Data Security and Privacy. Hershey, Pennsylvania: IGI Global, 2021. doi:10.4018/978-1-7998-4201-9.

Anu Stuparu. “Australia’s Cybersecurity.” In Routledge Companion to Global Cyber-Security Strategy, 1st ed., 381–91. Routledge, 2021. doi:10.4324/9780429399718-35.

Barker, Jessica. Confident Cyber Security : The Essential Insights and How to Protect from Threats. Second edition. London, England: Kogan Page Limited, 2023

Colarik, Andrew, Julian Jang-Jaccard, and Anuradha Mathrani, eds. Cyber Security and Policy : A Substantive Dialogue. Auckland, New Zealand: Massey University Press, 2017.

Geng, Hwaiyu, ed. The Internet of Things and Data Analytics Handbook. 1st ed. Hoboken, New Jersey: John Wiley & Sons, 2008. doi:10.1002/9781119173601.

Ghosh, J., Sinha, V.K. (2024). Big Data Analytics in Industry 4.0 in Legal Perspective: Past, Present and Future. In: Kumar, A., Sagar, S., Thangamuthu, P., Balamurugan, B. (eds) Digital Transformation. Disruptive Technologies and Digital Transformations for Society 5.0. Springer, Singapore. https://doi-org.ezproxy2.library.drexel.edu/10.1007/978-981-99-8118-2_7.

Guidetti, Oliver, Mohiuddin Ahmed, and Craig Speelman. Psybersecurity : Human Factors of Cyber Defence. 1st ed. Boca Raton: Taylor & Francis Group, 2024.

Montasari, R. (2024). Responding to Deepfake Challenges in the United Kingdom: Legal and Technical Insights with Recommendations. In: Cyberspace, Cyberterrorism and the International Security in the Fourth Industrial Revolution. Advanced Sciences and Technologies for Security Applications.

Springer, Cham. https://doi-org.ezproxy2.library.drexel.edu/10.1007/978-3-031-50454-9_12

Morey J. Haber, Darran Rolls. Identity Attack Vectors: Strategically Designing and Implementing Identity Security, Second Edition. Apress, 2024

Prasetyoningsih, N., Ismail Nawang, N., Putri, W.V., Amirullah, M.N.R. (2024). Legal Protection for the Personal Data in Indonesia and Malaysia. In: Moallem, A. (eds) HCI for Cybersecurity, Privacy and Trust. HCII 2024. Lecture Notes in Computer Science, vol 14728. Springer, Cham. https://doi-org.ezproxy2.library.drexel.edu/10.1007/978-3-031-61379-1_11

Reich, Pauline C, and Eduardo Gelbstein. Law, Policy, and Technology : Cyberterrorism, Information Warfare, and Internet Immobilization. Hershey, PA: Information Science Reference, 2012. doi:10.4018/978-1-61520-831-9.

Sangeeta Mahapatra. Repression by Legal Means: Governments' Anti-Fake News Lawfare. German Institute of Global and Area Studies GIGA, n.d. 2024

Sergi, Bruno S, Elena G Popkova, Aleksei V Bogoviz, and Tatiana N Litvinova. Understanding Industry 4.0: AI, the Internet of Things, and the Future of Work. First edition. Bingley, UK: Emerald Publishing Limited, 2019. doi:10.1108/9781789733112.

Subramanian, Ramesh, ed. *Computer Security, Privacy and Politics: Current Issues, Challenges and Solutions.* Hershey, PA: IGI Global Scientific Publishing, 2008. https://doi-org.ezproxy2.library.drexel.edu/10.4018/978-1-59904-804-8.

Makalah/Artikel/Prosiding/Hasil Penelitian

Abdurrohim, Muhammad, Indah Kumalasari, and Fathur Rosy. "The Paradox of Indonesia Cyberspace Policy and Cooperation: Neoclassical Realism Perspective." *Jurnal Hubungan Internasional*. (Yogyakarta) 11, no. 2 (2022): 13–23. doi:10.18196/jhi.v11i2.14361.

Adonis, Abid A. "Critical Engagement on Digital Sovereignty in International Relations: Actor Transformation and Global Hierarchy." Global : *Jurnal Politik Internasional* 21, no. 2 (2019): 262-. doi:10.7454/global.v21i2.412.

Albert Triwibowo. "The Characteristics of Indonesian Digital Diplomacy." JAS : *Journal of Asean Studies* 11, no. 1 (2023): 167–96. doi:10.21512/jas.v11i1.8525.

Auliaurrahman, Nur Anshari, and Sunny Ummul Firdaus. "The Existence and Regulation of Cyber Law: The Government's Role in Combating Digital Crime in Indonesia." *Jurisprudensi: Jurnal Ilmu Syariah, Perundang-Undangan Dan Ekonomi Islam* 17, no. 1 (2025): 206-223.

Cartin-Pecson, R., Karsono, B., L. Sulastri, Z. Rony., and C. Chavez. "Defending the Digital Domain: A Critical Look at Cybercrime Legislation in Indonesia and the Philippines." *Academic Journal of Interdisciplinary Studies 14(2):198.* doi:10.36941/ajis-2025-0040

Kurniawan, Kukuh Dwi, Deassy J. A. Hehanussa, Rahmat Setiawan, Indah Susilowati, Sopian, and Desmarani Helfisar. 2024. "Criminal Sanctions and Personal Data Protection in Indonesia". *Lex Publica* 11 (2):221-47. https://doi.org/10.58829/lp.11.2.2024.1-27.

Kuzior, A., I. Tiutiunyk, A. Zielińska, and R. Kelemen. "Cybersecurity and Cybercrime: Current Trends and Threats." *Journal of International Studies* 17, no. 2 (2024). doi:https://doi.org/10.14254/2071-8330.2024/17-2/12.

Lazari C.C. Cybersecurity and Sovereignty in Cyberspace: Challenges and Prospects of International Law. *Moscow Journal of International Law*. 2025;(1):125-137. (In Russ.) https://doi.org/10.24833/0869-0049-2025-1-125-137

Lee Kuan Yew School of Public Policy, "The Rise of Indonesia's Digital Economy" National *University of Singapore* (2025). https://lkyspp.nus.edu.sg/docs/default-source/case-studies/the-rise-of-indonesia-s-digital-economy.pdf?sfvrsn=c607020a_0 (Diakses 31 Mei 2025).

Mahapatra, Sangeeta, Janjira Sombatpoonsiri, and Andreas Ufen. "Repression by Legal Means: Governments' Anti-Fake News Lawfare." German Institute of Global and Area Studies (GIGA), 2024. http://www.jstor.org/stable/resrep58466.

Priyandita, G., "Indonesia's Cybersecurity Woes: Reflections for the Next Government" *CSIS Commentaries CSISCOM00624* (2024)

Putri, Kristiani Virgi Kusuma. 2021. "Kerja Sama Indonesia Dengan ASEAN Mengenai Cyber Security Dan Cyber Resilience Dalam Mengatasi

Cyber Crime". *Jurnal Hukum Lex Generalis* 2 (7):542-54. https://doi.org/10.56370/jhlg.v2i7.90.

Sarjito, Aris. 2024. "Technological Pride and National Resilience: How Innovation Shapes Stability and Security ". *Jurnal Lemhannas RI* 12 (3), 277-98. https://doi.org/10.55960/jlri.v12i3.940.

Shai Farber. "The Evolving Nexus of Cybercrime and Terrorism: A Systematic Review of Convergence and Policy Implications." *Security Journal 38*, no. 1 (2025). doi:10.1057/s41284-025-00471-7.

Internet

Ananda Putra. "Serangan Siber di RI Terus Meningkat, Capai 448 Juta Kasus". Media Indonesia (2021). https://mediaindonesia.com/politik-dan-hukum/414225/serangan-siber-di-ri-terus-meningkat-capai-448-juta-kasus (Diakses 29 Mei 2025)

Intan Rakhmayanti Dewi, "Serangan Ransomware pada Pusat Data Nasional," https://www.cnbcindonesia.com/tech/20240627081538-37-549695/pusat-data-nasional-kena-ransomware-guru-besar-it-angkat-bicara, CNBC Indonesia (diakses 29 Mei 2025)

Nikita Dewi Kurnia Salwa. "Tantangan & Hambatan Besar yang Dihadapi CSIRT-BSSN Indonesia" CSIRT (2024). https://csirt.or.id/pengetahuan-dasar/tantangan-csirt-bssn#:~:text=CSIRT%20(Computer%20Security%20Incident%20Response,tantangan%20yang%20memerlukan%20perhatian%20serius. (diakses 29 Mei 2025)

Norman Harsono. "Despite improvements, Indonesia's digital literacy remains low" The Jakarta Post (2022). https://www.thejakartapost.com/business/2022/01/20/despite-improvements-indonesias-digital-literacy-remains-low.html (Diakses 29 Mei 2025)

MKRI. "Sejumlah Pencipta Konten Persoalkan Unsur Pencemaran Nama Baik Dalam UU ITE" Mahkamah Tinggi Republik Indonesia (2022). https://www.mkri.id/index.php?page=web.Berita&id=18118&menu=2 (Diakses 29 Mei 2025)

Yakub Pryatama Wijayaatmaja. "Soal Kebocoran Data BPJS Kesehatan, Polri Dalami Peran IT" Media Indonesia (2021). https://mediaindonesia.com/politik-dan-hukum/409284/soal-kebocoran-data-bpjs-kesehatan-polri-dalami-peran-it (Diakses 29 Mei 2025)

Peraturan Perundang-Undangan

Undang-Undang Nomor 27 Tahun 2022 Tentang Pelindungan Data Pribadi (UU PDP)

Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik (UU ITE)

Undang-Undang Nomor 19 Tahun 2016 Tentang Informasi dan Transaksi Elektronik (UU ITE)

Konvensi Internasional

Konvensi Budapest tentang Kejahatan Dunia Maya