

**KEKOSONGAN NORMA HUKUM TERHADAP PENYALAHGUNAAN
IDENTITAS DIGITAL DALAM PERSPEKTIF HUKUM SIBER
INDONESIA*****THE VAPOR IN LEGAL NORMS REGARDING DIGITAL IDENTITY
MISUSE FROM THE PERSPECTIVE OF INDONESIAN CYBER LAW*****Lovika Augusta Purwaningtyas¹⁾, Anisa Ramadhani²⁾, Rose Rizki Salsabila³⁾**^{1,2,3}Prodi Ilmu Hukum, Fakultas Hukum,
Universitas Abdurachman Saleh Situbondo²Email: dnia81169@gmail.com*Naskah diterima tanggal 19-05-2026, disetujui tanggal 18-06-2026, dipublikasikan tanggal 06-07-2026***ABSTRAK**

Perkembangan teknologi digital di Indonesia menyebabkan peningkatan kasus penyalahgunaan identitas digital, seperti phishing, deepfake, dan pencurian data pribadi yang mengancam keamanan siber nasional. Meskipun terdapat norma hukum siber yang berlaku termasuk UU bernomor 1 Tahun 2024 menyangkut Informasi pun Transaksi Elektronik (UU ITE), UU bernomor 27 Tahun 2022 menyangkut Perlindungan Data Pribadi, serta UU bernomor 1 Tahun 2023 menyangkut Kitab Undang-undang Hukum Pidana (KUHP), masih terdapat kekosongan substantif dalam pengaturan penyalahgunaan identitas digital secara spesifik. Kekosongan ini mencakup kurangnya definisi yang jelas, sanksi yang sesuai dengan teknologi baru, dan mekanisme penegakan hukum yang dapat diterapkan di berbagai yurisdiksi. Penelitian ini mengkaji kekosongan norma tersebut dari sudut pandang hukum siber di Indonesia berpendekatan yuridis normatif disertai analisis kepada aturan hukum, dan doktrin hukum di bermacam rujukan. Hasil studi mengungkap kekosongan norma tersebut berdampak pada rendahnya efektivitas penegakan hukum, sehingga diperlukan upaya reformulasi legislasi. Reformulasi tersebut mencakup pengesahan undang-undang khusus tentang identitas digital serta penguatan fungsi Badan Siber dan Sandi Negara (BSSN).

Kata kunci: identitas digital; kekosongan norma; hukum siber**ABSTRACT**

The development of digital technology in Indonesia has led to an increase in cases of digital identity abuse, such as phishing, deepfakes, and the theft of personal data that threaten national cyber security. Although there are applicable cyber law norms, including Law Number 1 of 2024 on Electronic Information and

Transactions (ITE Law), Law Number 27 of 2022 on Personal Data Protection, and Law Number 1 of 2023 on the Criminal Code (KUHP), there are still substantive gaps in the regulation of digital identity abuse specifically. These gaps include the lack of clear definitions, sanctions appropriate to new technologies, and law enforcement mechanisms that can be applied across various jurisdictions. This study examines these normative gaps by the perspective of cyber law in Indonesia used a normative juridical approach with an analysis of legal regulation also legal doctrines from any sources. The answers from this research indicating the absence of these norms affects the low effectiveness of law enforcement, thereby necessitating efforts to reformulate legislation. Such reformulation includes the enactment of specific laws concerning digital identity as well as the strengthening of the functions of the National Cyber also Crypto Agency (BSSN).

Keywords: *cyber law; digital identity; normative vacuum*

PENDAHULUAN

Kebermajuan teknologi komunikasi sekaligus informasi sudah mencipta wadah terbaru yakni “dunia maya/cyberspace”, sebagai wadah adanya proses berinteraksi publik, ekonomi, sampai tindakan kriminalitas. Konteks ini timbul ranah hukum terbaru yang dikenal hukum menyangkut siber (Wirogioto & Putra, 2026:1). Hukum menyangkut siber sebagai ranah ilmu dalam hukum di mana mengelola perilaku hukum di lingkup siber, terkhusus pemanfaatan teknologi informasi, komunikasi daring, beserta jaringan elektronik. Hukum siber adalah rumpun hukum dengan lingkup seluruh aspek di mana relevan terhadap individu per individu maupun subjek hukum selaku pengguna dan pengoperasi teknologi internet sejak awal online sampai masuk dunia maya. Hukum siber perlu guna menekan kriminal secara siber. Hukum tersebut relevan atas upaya mencegah tindakan pidana maupun upaya menanganinya.

Permasalahan mengenai kejahatan sibernya masih hangat dibahas dikalangan akademisi hukum karena kejahatan ini tergolong fenomena baru yang terus berkembang. UU bernomor 1 Tahun 2023 menyangkut Kitab Undang-Undang Hukum Pidana (berikutnya dinamakan KUHP 2023) lalu ada UU bernomor 27 Tahun 2022 menyangkut Perlindungan Data Pribadi (berikutnya dinamakan UU PDP) kerap menjadi titik sorotan baik di kritik maupun dipertahankan terkait sejauh

mana relevansinya guna penanganan perkara kriminal siber. Penegakan kebijakan kepada pelaku kriminal daring saat ini masih bergantung pada ketentuan dalam KUHP, khususnya pasal-pasal yang tidak lazim digunakan untuk jenis kejahatan ini. Hal ini memperlihatkan bahwa sistem hukum konvensional belum sepenuhnya mampu merespons kompleksitas serta dinamika perkembangan kejahatan siber yang terus berubah.

Kejahatan siber di Indonesia banyak terjadi seperti kebocoran data pribadi, *phishing*, *defacing* situs pemerintah dan lain sebagainya. Salah satu kasus yang terjadi yaitu pada Mei 2021, Indonesia digemparkan oleh dugaan pelanggaran data BPJS Kesehatan mengejutkan Indonesia, dengan 279 juta informasi pribadi dilaporkan diperjualbelikan di Raid Forums seharga sampai Rp80 juta. Raid Forums dikenal sebagai situs daring tempat diperjualbelikannya sebagai basis data, termasuk yang berasal dari aksi peretasan. Informasi yang disebarluaskan mencakup nomor dari kartu, informasi pribadi keluarga ataupun tanggungan, hingga transaksi, mirip pendataan BPPJS Kesehatan. Kebocoran data BPJS teridentifikasi melalui akun Kotz, pelaku yang menjual dan membeli ulang data pribadi, memperdagangkan informasi tersebut melalui platform daring Raid Forums. Sebanyak 279 juta salinannya identitas penduduk dalam negeri diklaim dimiliki oleh pelaku dengan sekitar 100.000 data disediakan sebagai sampel. Kasus ini masih dalam tahapan analisis forensik digital, sehingga tanggung jawab hukum dari pihak BPJS Kesehatan belum dapat dibebankan hingga unsur-unsur pelanggaran dapat dibuktikan secara sah (Panggabean & Fitria, 2025: 1961).

Permasalahan terkait perlindungan data pribadi di Indonesia masih banyak terjadi sehingga menimbulkan banyak pertanyaan terkait perlindungan hukum terhadap penyalahgunaan identitas digital. Peneliti mendapatkan rumusan masalah pertama, apakah penyalahgunaan identitas digital dapat dikualifikasi sebagai perkara pidana dalam kacamata hukum positif dalam negeri? Dan yang kedua, apa bentuk konsep perlindungan hukum kepada korban penyalahgunaan identitas digital dalam ranah siber?. Rumusan masalah tersebut dapat ditarik judul “Kekosongan norma hukum terhadap penyalahgunaan identitas digital dalam

perspektif hukum siber Indonesia”. Urgensi dari studi letaknya di meningkatnya persentase juga kompleksitas kriminal retas di dalam negeri beserta belum maksimalnya bentuk perlindungan hukum pada korban penyalahgunaan hak aspek privasi. Penelitian ini mampu berkontribusi untuk mengembangkan penteorian hukum perlindungan data privasi, pun sebagaimana masukan aturan guna menguatkan sistem kebijakan pun tata kelolanya keamanan berbasis siber Indonesia. Berlandaskan rincian permasalahan sebelumnya, peneliti tertarik untuk membahas persoalan mengenai kekosongan norma hukum terhadap penyalahgunaan identitas digital dalam perspektif hukum siber Indonesia.

METODE PENELITIAN

Kajian bermetode yuridis normatif yakni penelitian hukum di mana menganalisis asas, kaidah, hingga norma hukum positifnya, peraturan perundang-undangan, serta studi pustaka untuk memecahkan permasalahan hukum. Jenis penelitian hukum menggunakan normatif, kajian hukum normatif fokus pada analisis ke hukum selayaknya sistem peraturan tertulis, dengan menganalisis aturan dalam UU, putusan hakim, juga doktrin dari hukum guna menggali penyelesaian perkara hukum. Tipe penelitian menggunakan penelitian hukum doktrinal, maksudnya kajian dengan basis kepustakaan dengan fokus analisa material hukum primer sekaligus sekunder.

Penelitian berpendekatan perundang-undangan (*statute approach*) yaitu merupakan upaya telaah ke aturan UU berkenaan dengan bahasan sentral kajian, berikutnya pendekatan kasus (*case approach*) di mana upaya telaahnya kepada perkara yang berkenaan atas perkara hukum yang ditangani. Sumber data yang digunakan meliputi materi hukum primer atau putusan resminya institusi hukum contohnya UU, pengadilan, beserta aturan yang dibuat landasan doktrin hukum, berikutnya materi hukum sekunder yakni rujukan penjelas UU pun aturan dari hakim di mana sukar dimengerti, menyajikan revisi hukum, pun memberi kesadaran menyangkut revisi hukum, beserta materi non hukum merupakan elemen dari perekonomian, sosial, politik, agama, hingga moral yang mengetergantung isi

materi hukum sebelum diformalkan (Efendi et al., 2023: 84). Teknik menghimpun materi hukum dengan kajian pustaka, artinya menelaah dan menganalisa aturan dari dokumenter hukum, karya ilmiah, pun bacaan relevan.

HASIL PENELITIAN DAN PEMBAHASAN

Pengaturan Hukum Penyalahgunaan Identitas Pada Hukum Siber Indonesia

Bentuk instrumen hukumnya guna melindungi data privasi kepada penduduk lokal konsisten belum mendapat atensi dari konstitusi secara memadai pun menyeluruh. Aturan perlindungannya tidak mendapat pengakuan layaknya hak asasi manusia di mana wajib dijunjung pun dilindungi. Konstitusi Indonesia memberi hormat juga memperkokoh HAM, tetapi realitas perlindungan informasi pribadi layaknya privasi, gagal dikelola tegas. Aturan ini hanyalah tersirat di Pasal 28H Ayat (4) UUD1945, bahwasanya negara memberi kemerdekaan guna menjaga informasi pun lindungan data sekaligus informasi di mana melekat terhadapnya (Trisandi & Sofian., 2024). Ragam aturan konstitusi berkenaan atas hukum ranah siber dapat digunakan untuk menjerat pelaku melalui UU ITE, UU PDP, dan KUHP 2023. Dimasa yang serba digital KUHP 2023 masih menjadi pedoman dalam menangani kasus penipuan dan pemalsuan, akan tetapi dalam penerapannya sering kali harus dipadukan dengan UU ITE karena objeknya berupa data, akun, dokumen elektronik, atau transaksi melalui internet. Praktiknya, untuk kasus penipuan pasal yang berlaku dalam KUHP 2023 adalah pasal 492, sedangkan pemalsuan dokumen elektronik biasanya disesuaikan dengan pasal 35 UU ITE jo pasal 51, meski unsur pemalsuan surat dalam KUHP 2023 juga bisa diterapkan apabila tindakannya memenuhi ketentuan dalam pasal tersebut. Pemalsuan di era digital umumnya terjadi dalam bentuk manipulasi data, dokumen, tanda tangan elektronik, atau identitas digital agar terlihat asli dan nyata. UU ITE mengatur beberapa aspek kejahatan digital, termasuk penyalahgunaan data, namun regulasi yang secara spesifik mengatur tentang pemalsuan identitas masih minim. UU ITE dan peraturan terkait cenderung bersifat umum dan belum mengakomodasi modus-modus baru dalam pemalsuan identitas digital, seperti penggunaan akun palsu untuk pencucian

uang, penipuan keuangan, atau manipulasi data pribadi secara langsung untuk kepentingan criminal (Faisal et al., 2025: 1).

Ada ketiga subyek dalam kelola UU PDP tentang data personal, yakni pemegang data (disebut pula subjek informasi personal), pengendali atau penghimpun data (mencakup seluruh individu, institusi hukum maupun badan internasional) kemudian ada informasi prosesor (subyek yang mengelola data pasca terhimpun). UU PDP mengelola tentang institusi pengawas data personal. Pasal 58 UU PDP mengungkap tata kelola data personal dikelola pun tanggung jawab terhadap presiden. Pasal 65 UU PDP mengungkap tiap individu dilarang menyimpang hukum dengan menjangkau data personal yang bukanlah miliknya demi kepentingan pribadi. Pelanggaran terhadap larangan ini dapat dikenakan pidana bui terlama 5 tahun maupun didenda terbanyak Rp 5 Miliar. Sementara itu, individu secara sadar menipu data personal demi urgensi pribadi dikenakan bui terlama 6 tahun ataupun didenda maksimalnya Rp 6 Miliar (Faisal et al., 2025: 7). Undang-undang Perlindungan Data Pribadi (PDP) bertujuan guna menduduki kekosongan standar dan kriteria perlindungannya data pribadi yang belum ada sebelumnya. Namun, pengaturannya tetap lebih berfokus pada perlindungan data pribadi secara umum, bukan pada identitas digital sebagai bentuk kejahatan yang berdiri sendiri. Dalam praktiknya, Indonesia memiliki dasar hukum untuk menjerat pelaku penyalahgunaan identitas digital melalui UU ITE dan UU PDP, akan tetapi belum optimal karena tidak ada pengaturan khusus yang mengatur penyalahgunaan identitas digital sebagai delik tersendiri dan masih terdapat kekosongan dalam sistem pembuktian.

Kekosongan Norma Hukum terhadap Penyalahgunaan Identitas Digital

UU ITE tidak menyebutkan lengkap aturan identity theft sebagaimana delik terkhusus, beberapa ketentuan dijadikan landasan pertanggung jawaban kepidanaan. Tentang tindak mencuri identitas dengan mengakses tanpa izin dalam jaringan elektronik, membuat tindakannya dikualifikasi sejalan Pasal 30 ayat (1), (2), beserta (3) UU ITE, diikuti ancaman bui sejalan regulasi Pasal 46 UU ITE. Komponen “mengakses tanpa hak” pun “mengakses informasi elektronik”

menyambung jika pelakunya meretas ataupun mencuri jaringan elektronik demi mendapat data identitasnya target (Suciara et al., 2026: 5387). KUHP 2023 tidak memiliki regulasi mengenai data sebagai objek kejahatan, akibatnya tidak ada norma yang mengatur pencurian data atau identitas digital secara spesifik, dampak dari kekosongan norma ini menciptakan fragmentasi antar lembaga dan kelemahan dalam penegakan hukum (Prabowo., 2025). Konstruksi pertanggung jawaban pidana di mana sifatnya tidak langsung menggambarkan terdapatnya kekosongan normatif di hukum kepidanaan siber nasional. Realita menggambarkan urgensi revisi regulasi hukum kepidanaan dengan merumuskan delik terkhusus pembobolan identitas, demi memastikan adanya kepastian dalam hukum, memperkuat perlindungan untuk korban, beserta meningkatkan keefektifan peminimalan kriminal siber dari tahap dini (Suciara et al., 2026: 5387).

Ketiadaan pengaturan khusus tentang penyalahgunaan identitas digital menimbulkan kekosongan norma, akibatnya penegak hukum harus menafsirkan berbagai pasal dalam beberapa undang-undang untuk menjatuhkan hukuman pada pelaku (Hapsari dan Pambayun, 2023). Karena tidak ada pasal yang jelas yang menyatakan delik penyalahgunaan identitas digital dan sanksi yang sesuai maka penerapan hukum biasanya bersifat reaktif dan berdasarkan kasus masing-masing, sehingga menimbulkan ketidakpercayaan publik terhadap kemampuan hukum dalam melindungi hak privasi dan identitas di era digital. Demikian diperlukan keselarasan antar UU ITE, UU PDP, KUHP 2023, serta pembuatan peraturan khusus yang secara jelas mengatur tindak pidana penyalahgunaan identitas digital agar hukum dapat diterapkan dengan lebih konsisten efektif dan adil.

Konsep Perlindungan Hukum Terhadap Korban Penyalahgunaan Identitas Digital pada Ruang Siber

UU PDP ada sebagaimana respon atas meningkatnya kriminal dunia siber di mana menyalahgunakan informasi privasi. UU tersebut mempertegas bahwasanya perlindungan informasi privasi menjadi hak konstitusional sehingga perlu dijaga, beserta memberi kerangka hukum yang tegas melalui terbentuknya institusi perlindungan data privasi, mekanisme peninjauan administratif, beserta

aturan kepidanaan yang kuat. Pelanggarannya sebagai contoh pembobolan, penyebaran, hingga memalsukan data privasi di luar izin dikenai sanksi pidana bui ataupun denda milyar rupiah, beserta pidana tambahan yakni pergantian kerugian untuk korban (Daeng et al., 2023: 2905). Cakupan UU ITE yakni aspek perlindungan data privasi, keamanan informasi, pembayaran daring, serta pencegahan kriminal siber. UU ITE dapat digunakan untuk proses pidana apabila terdapat unsur akses ilegal, manipulasi data, atau penyebaran informasi elektronik secara melawan hukum. Semakin banyaknya kasus siber sudah meraih perhatian pihak berwenang untuk langsung mengesahkan UU guna menjebak actor/pelaku criminal siber. Pemerintah dalam negeri sudah menambah muatan materi tentang siber di UU ITE lebih lanjut diharap mampu mengatasi, menekan, beserta meniadakan tindak kriminalitas di jejaring media maya (Firdaus, 2024:90).

Lembaga penegak hukum di berbagai negara telah membentuk tim khusus di bawah naungan Kementerian Komunikasi dan Digital. untuk menangani kejahatan siber yang terdiri dari ahli teknologi informasi, analis kejahatan siber, dan investigator yang dilatih khusus untuk menangani serangan keamanan siber(Komdigi, 2020). Strategi kebijakan perlindungan dan penegakan hukum siber di Indonesia dimulai dengan upaya harmonisasi regulasi agar seluruh aspek kejahatan dunia maya berada dalam landasan hukum yang menyeluruh. Langkah ini diharapkan menutup potensi tumpang tindih kewenangan antar lembaga dan mempercepat respon terhadap insiden siber sehingga kebijakan nasional bisa lebih adaptif terhadap kecepatan perkembangan teknologi(Firdaus, 2024: 104).

Mekanisme pemulihan dan ganti rugi bagi individu yang menjadi korban penyalahgunaan identitas digital adalah elemen penting dalam perlindungan hukum di dunia maya, karena tidak hanya menitikberatkan pada hukuman bagi pelaku tetapi juga pada pemulihan hak-hak individu yang dirugikan. Penyalahgunaan identitas digital dapat menyebabkan berbagai bentuk kerugian, baik yang bersifat material maupun non material, seperti kerugian finansial, pencemaran nama baik, hilangnya akses ke akun digital, serta dampak psikologis. Oleh karena itu, hukum harus menyediakan mekanisme yang memungkinkan para korban untuk

mendapatkan pemulihan yang komprehensif. Dalam konteks hukum di Indonesia, pemulihan dapat ditempuh melalui jalur pidana maupun jalur perdata. Dengan jalur pidana para korban dapat melaporkan kasus penyalahgunaan identitas pada penegak hukum berdasarkan UU ITE, yang mengatur berbagai jenis kejahatan di dunia siber, sehingga pelaku dapat diadili dan dikenai hukuman pidana. Selain itu korban juga berpeluang untuk menuntut ganti rugi melalui gugatan perdata jika terbukti penyalahgunaan identitas tersebut menyebabkan kerugian nyata. Di samping itu perlindungan untuk korban diperkuat oleh UU PDP yang memberikan hak kepada subjek data untuk menuntut pemulihan terhadap pelanggaran data pribadi mereka, termasuk hak untuk mengajukan keberatan, meminta agar data yang disalahgunakan dihapus, serta menuntut ganti rugi jika terjadi pelanggaran dalam pengelolaan data pribadi. Praktiknya pemulihan juga dapat dilakukan melalui kerja sama dengan penyelenggara sistem elektronik atau platform digital di mana identitas tersebut disalahgunakan, dengan mengambil langkah seperti melaporkan untuk menghapus konten, memblokir akun pelaku, memulihkan akses ke akun korban yang diretas. Dengan demikian mekanisme pemulihan dan ganti rugi bukan hanya diartikan sebagai pemberian kompensasi finansial, tetapi juga meliputi pemulihan nama baik, pengembalian kontrol atas identitas digital, serta perlindungan terhadap data pribadi korban agar tidak disalahgunakan dimasa mendatang. Oleh karena itu, pembentukan aturan khusus mengenai penyalahgunaan identitas digital menjadi penting untuk mengisi kekosongan norma. Aturan khusus dapat menyatukan pengaturan mengenai unsur tindak pidana, bentuk sanksi, dan mekanisme pemulihan korban secara lebih jelas dan konsisten. Melalui mekanisme ini diharapkan korban akan memperoleh keadilan secara hukum dan jaminan perlindungan atas hak-haknya sebagai individu.

KESIMPULAN

Pengaturan tentang perlindungan data pribadi dalam KUHP 2023 tidak cukup spesifik mengingat pesatnya perkembangan teknologi informasi yang mempengaruhi cara data pribadi dikumpulkan, diproses, dan disebarkan.

Kekosongan hukum menyebabkan pertanggung jawaban pidana pelaku masih bersifat tidak utuh dan belum menyeluruh. Penegakan hukum yang dilakukan masih sangat bergantung pada penafsiran terhadap berbagai norma yang tersebar dalam UU sektoral. Sementara itu dari sisi legislasi belum ada regulasi terpadu yang dirumuskan. Hal ini menunjukkan kekosongan norma untuk menangani kejahatan digital yang bersifat dinamis. Situasi ini menciptakan celah dalam kepastian hukum, melemahkan efek jera, serta mengurangi efektivitas perlindungan hukum bagi korban kejahatan siber. Oleh karena itu, perubahan pada kebijakan hukum pidana sangat penting melalui perbuatan delik khusus untuk pencurian identitas yang menyeluruh, terintegrasi, dan dapat menyesuaikan dengan kemajuan teknologi. Sifat terintegrasinya memungkinkan penyelarasan dengan UU ITE, UU PDP, serta KUHP melalui mekanisme rujukan silang dan dibantu oleh Satgas siber. Adaptivitasnya memungkinkan untuk menghadapi ancaman baru, dengan pembaruan yang dilakukan melalui Peraturan Pemerintah Pengganti Undang-Undang (Perppu).

DAFTAR PUSTAKA

- Daeng, Y., Linra, N., Darham, A., Handrianto, D., Sianturi, R. R., Martin, D., ... & Saputra, H. (2023). *Perlindungan Data Pribadi dalam Era Digital: Tinjauan Terhadap Kerangka Hukum Perlindungan Privasi*. *Innovative: Journal Of Social Science Research*, 3(6), 2898-2905.
- Efendi, A., Susanti, D.O., Tektona, R.I. (2023). *Penelitian Hukum Doktrinal*. Yogyakarta: Laksbang Justitia.
- Faisal, N., Aswari, A., Ilham, M.A. (2025). *Penegakan Hukum Terhadap Eksistensi Tindak Pidana Pemalsuan Identitas di Era Digital*. *Legal Dialogica*, 1(1), 1-7.
- Firdaus, R. A. (2024). *Perlindungan hukum dan pencegahan kejahatan siber di era digital dalam sistem hukum di Indonesia*. *STAATSRECHT: Jurnal Hukum Kenegaraan dan Politik Islam*, 4(1), 79-104.
- Komdigi. (2020). *Badan Cyber Nasional Demi Indonesia Digital*. <https://www.komdigi.go.id/berita/sorotan-media/detail/badan-cyber-nasional-demi-indonesia-digital>.

- Panggabean, M.V., & Fitria, A. (2025). Perlindungan Hukum Data Pribadi di Indonesia (Kasus Kebocoran Badan Penyelenggara Jaminan Sosial Kesehatan). *Arus Jurnal Sosial dan Humaniora*, 5(2), 1958-1965.
- Suciara, A., Michelin, D., et al. (2026). Pencurian Identitas Digital Sebagai Bentuk Kejahatan Pendahuluan Dalam Cybercrime, *Al-zayn: Jurnal Ilmu Sosial dan Hukum*, 4(2), 5387.
- Wirogioto, A.J., & Belgradoputra, R.J. (2026). *Memahami Hukum Siber*. Bekasi: CV Intelektual writer.
- Hapsari, R. D., & Pambayun, K. G. (2023). Ancaman cybercrime di indonesia: Sebuah tinjauan pustaka sistematis. *Jurnal Konstituen*, 5(1), 1-17.
- Trisandi, D., & Sofian, A. (2024). TINDAK PIDANA PENYALAHGUNAAN DATA PRIBADI DALAM HUKUM SIBER INDONESIA. *Journal of Syntax Literate*, 9(2).
- Prabowo, D., (2025). *Perlindungan Hukum Terhadap Korban Tindak Pidana Pencurian Identitas Di Ruang Siber Dalam Perspektif Hukum Pidana Nasional*. Repository Panca Budi.

Peraturan Perundang-Undangan

Undang-Undang Dasar Negara Republik Indonesia Tahun 1945

Undang-Undang Nomor 1 Tahun 2023 Tentang Kitab Undang-Undang Hukum Pidana

Undang-Undang Nomor 27 Tahun 2022 Tentang Perlindungan Data Pribadi

Undang-Undang Nomor 1 Tahun 2024 Perubahan Kedua Atas Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik