Indonesian Journal of Law

Vol. 2, No. 8, Juli 2025
Hal 132-139

E-ISSN: 3032-3622
P-ISSN: 3032-3614

Site: https://jurnal.intekom.id/index.php/inlaw

Reformulasi Regulasi Tentang Kejahatan Siber Dalam Bentuk Doxing yang Berbasis Perlindungan Hukum Terhadap Korban

Rahmayanti[1], Rifqi Fairuz Ula[2], Abdi Ridho[3], Nurul Aini[4]

[1,2,3,4] Fakultas Hukum,Universitas Pembangunan Panca Budi, Medan, Indonesia

Article Info

Article history:

Received Juli 2, 2025
Revised Juli 2, 2025
Accepted Juli 2, 2025

Kata Kunci:

Reformulasi,
Kejahatan Siber,
Doxing,
Korban

Keywords:

Reformulation,
Cybercrime,
Doxing,
Victim

ABSTRAK

Transformasi digital yang pesat turut memunculkan tantangan hukum baru dalam bentuk kejahatan siber, salah satunya adalah doxing, yakni pengungkapan dan penyebaran data pribadi seseorang secara ilegal yang dapat menimbulkan dampak psikologis, sosial, hingga fisik bagi korban. Meskipun praktik ini kian sering terjadi, kerangka hukum di Indonesia belum secara tegas mengakomodasi perlindungan hukum yang memadai bagi korban. Penelitian ini mengeksplorasi 2 (dua) isu utama: Pertama, ketidakcukupan regulasi yang ada dalam menjerat pelaku doxing di ranah siber; dan kedua, kebutuhan untuk membangun kerangka hukum baru yang berfokus pada perlindungan terhadap korban. Metodologi yang digunakan adalah penelitian hukum normatif dengan pendekatan peraturan perundang-undangan dan konsep hukum. Analisis terhadap Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE) dan Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi (UU PDP) mengindikasikan bahwa meskipun terdapat norma yang dapat digunakan untuk menjerat pelaku, keduanya belum mengatur secara spesifik mengenai doxing sebagai delik tersendiri. Oleh karena itu, dibutuhkan reformulasi regulasi yang lebih progresif, yang tidak hanya menegaskan larangan terhadap doxing, tetapi juga menyediakan mekanisme hukum yang berorientasi pada pemulihan hak-hak korban dan penguatan sistem perlindungan data pribadi di era digital.

ABSTRACT

The rapid pace of digital transformation has brought about new legal challenges, particularly in the form of cybercrimes such as doxing—defined as the unlawful disclosure and dissemination of an individual's personal data, which can result in psychological, social, and even physical harm to victims. Although this practice is increasingly prevalent, the existing legal framework in Indonesia does not yet provide sufficient legal protection for victims. This study explores two main issues: first, the inadequacy of current regulations in prosecuting doxing perpetrators in cyberspace; and second, the urgent need to establish a new legal framework centered on victim protection. This research employs a normative legal methodology, utilizing statutory and conceptual legal approaches. An analysis of Law No. 11 of 2008 concerning Electronic Information and Transactions (ITE Law) and Law No. 27 of 2022 concerning Personal Data Protection (PDP Law) indicates that while certain provisions may be applied to prosecute offenders, neither law explicitly defines doxing as a distinct criminal offense. Consequently, there is a pressing need for a more progressive regulatory reform—one that not only explicitly criminalizes doxing but

E-ISSN : 3032-3622
P-ISSN : 3032-3614

also provides legal mechanisms focused on restoring victims' rights and enhancing the personal data protection system in the digital era.

Corresponding Author:

Rahmayanti
Fakultas Hukum, Universitas Pembangunan Panca Budi
Medan, Indonesia
Email: fairuzrifqiula@gmail.com

1. PENDAHULUAN

Perkembangan teknologi informasi dan komunikasi di era digital telah menghadirkan perubahan yang signifikan dalam pola interaksi sosial, termasuk cara individu memperoleh, menyimpan, dan menyebarluaskan informasi. Kemajuan ini, di satu sisi, membawa berbagai kemudahan dan efisiensi; namun di sisi lain juga menciptakan ruang baru bagi munculnya bentuk-bentuk kejahatan yang sebelumnya tidak dikenal dalam sistem hukum konvensional.[1]. Salah satu fenomena kejahatan yang semakin marak terjadi di ruang siber adalah *doxing*.

Transformasi digital global telah merevolusi cara manusia berinteraksi, namun bersamaan dengan itu muncul pula tantangan hukum baru berupa kejahatan digital yang kompleks. Salah satu manifestasi kejahatan digital yang mengalami eskalasi signifikan adalah praktik doxing, yaitu tindakan memperoleh dan menyebarkan data pribadi individu melalui media elektronik tanpa persetujuan yang sah. Tindakan ini bukan semata pelanggaran etika, tetapi berimplikasi langsung pada dimensi hukum, sosial, dan psikologis korbannya. [2].

Berbeda dari kriminalitas konvensional, kejahatan siber seperti doxing bersifat borderless, anonim, dan sering kali sulit dilacak, serta memanfaatkan kerentanan sistem digital. Pendekatan represif terhadapnya memerlukan kerangka hukum yang fleksibel dan responsif terhadap perkembangan teknologi. [3]. Namun, sistem hukum Indonesia, melalui instrumen seperti UU Informasi dan Transaksi Elektronik (ITE) dan UU Perlindungan Data Pribadi (PDP), belum sepenuhnya mampu mengakomodasi karakteristik unik kejahatan ini. Kendala yuridis seperti lemahnya norma pemidanaan, ketiadaan unsur formil yang eksplisit, serta keharusan pembuktian kerugian material menjadi hambatan utama dalam implementasi aturan yang ada. [4].

Berikutnya, merujuk pada Data Breach Investigation Report (2024) menunjukkan bahwa mayoritas tindakan pencurian data di tingkat global dilakukan untuk motif ekonomi (96%), sementara selebihnya didorong oleh motif politik, iseng, atau pembalasan pribadi. Temuan tersebut memperkuat argumen bahwa doxing bukanlah kejahatan tanpa tujuan, melainkan merupakan instrumen strategis yang sering digunakan untuk mendiskreditkan, mengintimidasi, atau memanipulasi korban demi keuntungan tertentu. [5].

Fenomena ini juga telah mengemuka dalam konteks lokal. Laporan dari Otoritas Jasa Keuangan (OJK) mencatat lebih dari 15.000 kasus pelanggaran data pribadi oleh penyedia layanan pinjaman daring antara Januari 2024 hingga Maret 2025, di mana praktik doxing digunakan untuk mempermalukan atau menekan peminjam. Pada saat yang sama, Kepolisian RI menerima berbagai laporan doxing yang menunjukkan pola serangan sistematis terhadap individu melalui eksposur informasi sensitif. Saat ini, regulasi nasional di Indonesia belum secara eksplisit mengatur kejahatan *doxing* sebagai suatu bentuk tindak pidana khusus. [6].

Berikutnya, Undang-Undang Nomor 19 Tahun 2016 tentang Perubahan atas Undang-Undang No. 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE), meskipun memuat ketentuan

mengenai penyebaran data pribadi, namun belum memberikan definisi maupun norma hukum yang tegas terhadap perbuatan *doxing*. [7]. Ketiadaan norma *lex scripta* yang secara tegas mengatur doxing sebagai delik berdampak pada ketidakpastian hukum, baik bagi korban maupun aparat penegak hukum. Hal ini mengindikasikan perlunya *legal reengineering*, baik melalui revisi regulasi eksisting maupun penemuan hukum (*rechtsvinding*) oleh aparat yudikatif. Dalam perspektif teori hukum progresif, sebagaimana dikemukakan Sabian Utsman dan Sudikno Mertokusumo, hukum harus dipahami sebagai entitas dinamis yang merefleksikan ketegangan antara *das sollen* (norma ideal) dan *das sein* (realitas sosial). Maka dari itu, ketidaksesuaian antara hukum yang tertulis dengan kompleksitas kejahatan digital seperti doxing menuntut reinterpretasi dan aktualisasi norma hukum yang lebih kontekstual dan transformatif.

2. METODE

Dalam rangka menelusuri jawaban atas rumusan masalah yang diajukan dalam kajian ini, pendekatan yang diadopsi adalah pendekatan yuridis normatif. Pendekatan ini berakar dari pemahaman bahwa hukum dipandang sebagai suatu sistem norma, sehingga proses penelitiannya berfokus pada penelaahan dokumen-dokumen hukum formal sebagai bahan utama. Menurut Soerjono Soekanto, pendekatan ini bertumpu pada penelaahan terhadap kerangka hukum positif, yakni peraturan perundang-undangan yang berlaku, yang dianalisis melalui kajian pustaka secara sistematis dan mendalam. Model penelitian ini dipilih sebagai kerangka konseptual dalam membedah dan merumuskan ulang regulasi mengenai tindak kejahatan siber dalam bentuk doxing, dengan titik tekan pada perlindungan hukum yang menyeluruh bagi individu yang menjadi korban.

3. HASIL DAN PEMBAHASAN

3.1. Kelemahan Regulasi Tindak Pidana Doxing dalam Ranah Siber di Indonesia

Fenomena eskalasi kejahatan digital—terutama praktik *doxing* (pembongkaran dan penyebarluasan data pribadi secara tanpa izin di ruang siber)—menandai masih terbelakangnya kesiapan negara merespons risiko yang muncul dari disrupsi teknologi informasi. Doxing bukan sekadar pelanggaran sopan santun daring, namun merupakan serangan langsung terhadap hak privasi, keamanan personal, bahkan kebebasan berekspresi warga.[8]. Analisis kebijakan mencatat bahwa peningkatan kasus *doxing* di Indonesia berjalan seiring dengan penetrasi internet dan masifnya migrasi aktivitas sosial-ekonomi ke ranah digital, sedangkan kerangka regulasi terlambat beradaptasi. [9]. Di masa pra-UU ITE dan sebelum hadirnya UU Perlindungan Data Pribadi (UU PDP), aparat penegak hukum hanya bisa menambal kekosongan hukum dengan menafsirkan Pasal 362 KUHP tentang pencurian—norma yang sebenarnya dirancang untuk "barang berwujud", sehingga tidak mampu memuat kompleksitas pencurian data non-fisik dan kejahatan bermotif pengungkapan informasi pribadi. [10].

Ketika UU ITE disahkan pada 2008 (direvisi 2016), harapan publik akan adanya instrumen komprehensif perlindungan hak digital ternyata belum terpenuhi. Secara empiris, proses perumusan UU ITE lebih banyak diwarnai kalkulasi (bahkan kompromi) politik-ekonomi yang difokuskan pada kemudahan transaksi elektronik dan kepastian bisnis *e-commerce*. UU ITE memang mengatur beberapa tindak pidana berbasis teknologi informasi, tetapi konstruksi pasal-pasalnya masih bersifat generik dan multitafsir, sehingga menyisakan ruang abu-abu untuk kasus-kasus pelanggaran privasi seperti **doxing**. [11]. Secara normatif, ini menciptakan defisit perlindungan hukum: asas legalitas (*nullum crimen, nulla poena sine lege*) menuntut kejelasan delik, sedangkan pasal-pasal UU ITE kurang spesifik mengkriminalkan bentuk penyerangan atas data pribadi non-transaksional. Sebagai akibatnya, penegakan hukum kerap berjalan reaktif, terfragmentasi, dan rawan disalahgunakan karena bergantung pada konstruksi delik "pencemaran nama baik" atau "akses ilegal" yang tidak selalu pas dengan karakter *doxing*.

Pertama, titik lemah utama terletak pada kesulitan mendasar dalam menetapkan titik koordinat hukum atas tindak pidana, baik dari sisi *locus delicti* (tempat kejadian perkara) maupun *tempus delicti* (waktu terjadinya peristiwa). Dalam konteks kejahatan siber, ruang dan waktu menjadi entitas yang cair—pelaku mampu mengaburkan lokasi geografis aksi kejahatannya melalui manipulasi perangkat digital, bahkan menghapus atau mengacak jejak-jejak digital yang menjadi petunjuk kunci. Demikian pula, waktu kejadian pun tidak bisa dirujuk secara pasti karena pelaku memiliki kapasitas teknis untuk memalsukan atau merekayasa waktu dan tanggal eksekusi tindak pidana tersebut. [12].

Kedua, persoalan barang bukti digital menimbulkan dilema tersendiri. Sistem elektronik dan jaringan internet, yang bersifat terbuka dan rentan dibobol, menjadi medium sempurna bagi pelaku kejahatan untuk menghapus, mengubah, atau menyamarkan identitas digitalnya. Bukti-bukti penting, mulai dari perangkat keras, perangkat lunak, hingga hasil digital dari suatu perbuatan pidana, dapat dengan mudah dihapus atau dimodifikasi. Teknologi digital memberi ruang bagi manipulasi canggih, di mana batas antara data otentik dan data rekayasa semakin kabur.

Ketiga, tindak pidana siber cenderung bersifat individualistik dan tersembunyi, dilakukan secara soliter di balik layar komputer tanpa kehadiran fisik atau interaksi langsung. Hal ini mengakibatkan minimnya saksi mata yang bisa memberikan keterangan konkret, sehingga aparat penegak hukum kerap hanya bergantung pada keterangan korban. Dalam kasus-kasus yang menyentuh sektor keuangan, seperti sistem perbankan, sering kali terdapat kecenderungan lembaga korban untuk tidak membuka fakta ke publik guna menjaga citra dan menghindari kepanikan nasabah, yang pada akhirnya menghambat proses hukum. [13].

Jika dianalisis dari perspektif kebijakan publik, kondisi ini mencerminkan dua kelemahan mendasar. Pertama, pendekatan regulasi yang bersifat sektoral—menonjolkan kepentingan ekonomi di atas perlindungan hak dasar—menghasilkan kebijakan parsial dan inkonsisten. Kedua, proses legislasi minim partisipasi substantif dari komunitas keamanan siber, pakar privasi, maupun organisasi masyarakat sipil, sehingga kebutuhan atas jaminan hak-hak digital warga kurang terakomodasi. Kedua kelemahan ini berkontribusi pada kesenjangan antara tujuan (*protection gap*) dan kinerja regulasi (*implementation gap*).

Pada tataran normatif hukum, solusi idealnya ialah merumuskan Undang-Undang Khusus Tindak Pidana Siber (*cybercrime act*) sebagai *lex specialis* yang memuat (i) definisi formal setiap bentuk kejahatan digital, termasuk doxing, (ii) pedoman pemidanaan berbasis proporsionalitas kerugian korban, (iii) hukum acara pidana siber (*digital forensics*, penyitaan data, penggeledahan sistem elektronik) yang selaras dengan prinsip due process, dan (iv) mekanisme kerja sama internasional—ekstradisi dan mutual *legal assistance*—mengingat sifat lintas-batas kejahatan siber. Dalam desain yang sama, mandat penegakan sebaiknya diberikan pada satuan siber terpadu (*cyber fusion center*) yang menggabungkan fungsi investigasi, intelijen digital, dan kecepatan respon insiden. [14].

Pengesahan UU No. 27 Tahun 2022 tentang Perlindungan Data Pribadi patut diapresiasi sebagai tonggak awal, regulasi ini untuk pertama kalinya menempatkan hak atas data pribadi dalam rezim penal (pidana) serta mengakui "pemrosesan dan pengungkapan data tanpa hak" sebagai delik khusus. UU PDP berkedudukan sebagai *lex specialis* untuk kejahatan yang menyasar "data pribadi"—termasuk skema doxing—dan menyediakan instrumen administratif hingga pidana, disertai kewajiban pelaku pengendali/pemroses data. Namun, UU PDP belum memuat seluruh katalog kejahatan siber non-data seperti serangan integritas (*integrity attacks*), gangguan ketersediaan (*denial of service*), dan penipuan digital, serta belum menyentuh metodologi penegakan hukum acara siber secara holistik. Kesenjangan inilah yang menegaskan urgensi pembentukan UU Tindak Pidana Siber terintegrasi. [15].

Menggabungkan dua perspektif tersebut, strategi legislasi ke depan perlu bergeser dari positivisme sempit menuju paradigma regulasi hak digital berbasis nilai HAM dan keamanan nasional. Artinya, setiap norma pidana digital wajib dirancang melalui proses partisipatif, lintas-disiplin, dan berbasis bukti (*evidence-based policy*). Kebijakan kriminalisasi harus diimbangi dengan program

literasi keamanan data, standar teknis perlindungan siber sektor publik-privat, serta kerangka pengawasan independen yang mencegah penggunaan regulasi untuk membungkam ekspresi. Hanya dengan demikian, perundang-undangan Indonesia akan mampu merespons evolusi ancaman doxing—dan kejahatan siber lain—tanpa mengorbankan prinsip keadilan, perlindungan hak asasi, dan kepastian hukum bagi seluruh pemangku kepentingan di ranah digital.

3.2. Reformulasi Regulasi Kejahatan Siber Doxing yang Berbasis Perlindungan Hukum terhadap Korban Ke Depan

Dalam kerangka perlindungan hukum terhadap korban kejahatan siber doxing di Indonesia, reformulasi regulasi menjadi langkah penting yang harus segera diambil. Saat ini, ketentuan peraturan perundang-undangan yang berlaku seperti UU ITE Pasal 37 menyebutkan: *"Setiap Orang dengan sengaja melakukan perbuatan yang dilarang sebagaimana dimaksud dalam Pasal 27 sampai dengan Pasal 36 di luar wilayah Indonesia terhadap Sistem Elektronik yang berada di wilayah yurisdiksi Indonesia."* Ketentuan ini belum secara eksplisit mengatur tindak doxing sebagai perbuatan pidana yang berdiri sendiri, meskipun dilakukan dari luar wilayah negara, tetap dapat dikenai sanksi jika menyerang sistem elektronik yang berada dalam batas yurisdiksi Indonesia. [16].

Meskipun secara normatif hal ini menunjukkan perluasan cakupan hukum nasional ke ranah lintas negara, pada praktiknya, pendekatan konvensional dalam hukum internasional masih bergantung pada prinsip teritorial. Sementara itu, kejahatan siber justru menantang prinsip tersebut karena bersifat lintas batas, menyebar melalui jaringan global, dan tidak mengenal sekat geografis yang jelas. Alhasil, negara-negara, termasuk Indonesia, hingga kini masih menghadapi ambiguitas serius dalam menerapkan yurisdiksi terhadap pelaku kejahatan digital lintas negara, khususnya yang memanfaatkan kompleksitas teknologi informasi dan komunikasi modern. [17].

Berikutnya, alam UU PDP khususnya Pasal 67 ayat (1) menyatakan: *"Bahwa seseorang yang dengan sengaja dan secara ilegal mengakses atau mengumpulkan data pribadi yang bukan miliknya dengan maksud untuk memperoleh keuntungan dapat mengakibatkan kerugian bagi subjek data pribadi tersebut, dan sebagai konsekuensinya, dapat dikenakan pidana penjara dengan jangka waktu maksimal lima tahun dan/atau pidana denda dengan jumlah maksimal Rp 5.000.000.000 (lima miliar rupiah)".* Pengaturan ini pun juga belum melengkapi aturan terkait kepastian yurisdiksi, penegakan hukum yang mana hal ini bisa berkaitan dengan kompetensi relatif di persidangan.

Di era digital saat ini, praktik *doxing* tentu menjadi semakin kompleks, menyasar aspek kerahasiaan, keamanan, bahkan integritas korban di ruang publik. Oleh karena itu, perlu adanya reformulasi regulasi yang secara tegas mengklasifikasikan doxing sebagai bentuk kejahatan siber dengan perumusan pasal-pasal baru yang lebih preskriptif, jelas, dan berperspektif pada korban. Oleh karena itu reformulasi sangat diperlukan yang mencakup pengakuan eksplisit terhadap tindakan doxing, perluasan definisi data pribadi, perumusan elemen tindak pidana secara rinci, serta pengaturan tentang hak-hak korban, termasuk hak atas rehabilitasi dan pemulihan. Sehingga demikian, berikut adalah usulan reformulasi Pasal regulasi doxing ke depan:

Tabel 1. Usulan Reformulasi Regulasi ke Depan

Aspek	Ketentuan Saat Ini (UU ITE & UU PDP)	Usulan Reformulasi ke Depan
Definisi Doxing	Tidak diatur secara eksplisit	Menambahkan definisi doxing dalam UU ITE sebagai: *"Tindakan mengungkap, menyebarluaskan, atau membocorkan data pribadi seseorang tanpa persetujuan yang sah dengan tujuan merugikan, mengintimidasi, atau mempermalukan korban."*
Pasal Terkait	Pasal 26 (perlindungan data pribadi terbatas), Pasal 27 ayat (3), Pasal 28 ayat (2), dan Pasal 29 (ancaman)	Menyusun pasal khusus mengenai doxing, misalnya Pasal 27C: "*Setiap orang yang dengan sengaja dan tanpa hak menyebarluaskan data pribadi orang lain yang menyebabkan kerugian, diancam pidana...*"
Unsur Pidana	Multitafsir dan tidak spesifik terhadap tindakan **doxing**	Dirumuskan secara eksplisit: (a) penyebaran data pribadi, (b) tanpa izin, (c) dengan niat merugikan atau menimbulkan ketakutan, (d) dampak terhadap korban
Sanksi Pidana	Maksimal 4-6 tahun penjara tergantung pasal yang dikenakan	Diformulasikan sanksi pidana spesifik untuk doxing: minimal 2 tahun dan maksimal 7 tahun penjara serta/atau denda Rp500 juta-Rp2 miliar, tergantung tingkat kerugian atau dampak korban
Perlindungan Korban	Belum ada ketentuan khusus tentang pemulihan korban kejahatan siber doxing	Menambahkan hak korban atas informasi, perlindungan identitas, pendampingan hukum, dan rehabilitasi psikis dalam bab khusus atau pasal perlindungan tersendiri
Keterkaitan dengan UU PDP	Belum sinkron Pasal 67 ayat (1) sepenuhnya, hanya merujuk bahwa data pribadi harus dilindungi	Harmonisasi norma UU ITE dan UU PDP dalam satu regulasi teknis, seperti melalui Peraturan Pemerintah atau Peraturan Presiden yang mengatur mekanisme perlindungan dan pelaporan doxing secara komprehensif

Sumber: Bahan Hukum diolah Sendiri oleh Peneliti

Dalam pendekatan *victim-oriented criminal law*, hukum pidana seharusnya tidak hanya menitikberatkan pada penghukuman pelaku, melainkan juga harus mampu memberikan perlindungan nyata bagi korban. Ketidaktegasan hukum dalam mengatur doxing menunjukkan kelemahan dalam sistem perlindungan hukum nasional terhadap hak privasi warga negara. Melalui pendekatan ini, penelitian ini mengusulkan agar regulasi kejahatan siber di Indonesia—terutama UU ITE—direformulasi dengan mengadopsi perspektif perlindungan korban secara lebih nyata, baik dari segi pencegahan, penindakan, maupun pemulihan hak-hak korban. Perubahan ini juga seharusnya bersinergi dengan UU PDP dan prinsip-prinsip perlindungan HAM, mengingat privasi merupakan bagian dari HAM yang diakui secara universal. Dengan demikian, reformulasi ini bertujuan untuk menjadikan

hukum pidana siber di Indonesia lebih responsif dan adaptif terhadap bentuk-bentuk kejahatan digital yang berkembang, khususnya doxing. Msenambahkan pasal yang lebih eksplisit dan perlindungan yang lebih kuat terhadap korban, maka sistem hukum nasional akan lebih berpihak pada keadilan substantif dan hak asasi manusia, terutama hak atas privasi dan rasa aman di ruang digital.

4. KESIMPULAN

Kejahatan siber, khususnya doxing, di Indonesia telah menjadi persoalan sosial yang berkembang seiring kemajuan teknologi digital dan transformasi masyarakat menuju masyarakat siber (*cybersociety*). Fenomena ini menimbulkan implikasi hukum yang signifikan, khususnya karena *doxing* mencederai hak atas privasi dan data pribadi warga negara. Meskipun Indonesia telah memiliki kerangka hukum melalui UU ITE dan UU PDP, namun keduanya belum sepenuhnya responsif dan efektif dalam menanggulangi doxing secara spesifik. Oleh karena itu, diperlukan langkah reformasi regulasi melalui pendekatan sistematis, baik terhadap norma umum maupun khusus, agar mampu menghadirkan kepastian hukum, perlindungan terhadap korban, serta memperkuat mekanisme penegakan hukum dalam menghadapi dinamika kejahatan di ruang digital.

REFERENSI

[1] Angelita, Valerie, And Varsha Savilla Akbari Candra Suradipraja. "Dampak Sosial Doxing Terhadap Hak Privasi Pelaku Kejahatan Berdasarkan Undang-Undang Nomor 27 Tahun 2024." *Jurnal Legislatif*, 2024, Pp. 1–18.

[2] Firnanda, Wahyuni, et.al. "Analisis Efektivitas Penetapan Surat Dakwaan Subsidair Pada Pemidanaan Pelaku Kejahatan Cyber (Cybercrime)." *Jurnal Landraad*, Vol. 4, No. 1, 2025, Pp. 77–86.

[3] Iswardhana, Muhammad Ridha, And Suyud Widiono. "Diplomasi Siber Dan Teknologi Mobile Pada Multidisiplin." *Gaes-Pace Book Publisher*, 2023, Pp. 1–8.

[4] Mahendra, Bovin Tri, et.al. "Kebijakan Hukum Pidana Terhadap Penyebaran Data Pribadi (Doxing) Jurnalis Dalam Rangka Perlindungan Data Pribadi Di Indonesia." *Rio Law Jurnal*, Vol. 6, No. 1, 2025, Pp. 643–50.

[5] Maskun, S. H. *Kejahatan Siber (Cyber Crime): Suatu Pengantar*. Prenada Media, 2022.

[6] Muchamad, Masduki Khamdan. *Kejahatan Siber Ancaman Dan Permasalahannya: Tinjauan Yuridis Pada Upaya Pencegahan Dan Pemberantasannya Di Indonesia*. Syiah Kuala University Press, 2023.

[7] Muttaqi, Nabila Ihza Nur, And Muhammad Subhan. "Perlindungan Hukum Bagi Korban Penyebaran Data Pribadi Oleh Penyedia Jasa Pinjaman Online Illegal Dalam Perspektif Viktimologi." *Delicti: Jurnal Hukum Pidana Dan Kriminologi*, Vol. 2, No. 1, 2024, Pp. 28–41.

[8] Ngantung, Frilly Maria. "Perlindungan Hukum Terhadap Korban Doxing Perusahaan Pinjaman Online Legal." *Lex Privatum*, Vol. 13, No. 5, 2024.

[9] Pramana, Juliantio Dwi, et.al. "Law Enforcement Of Criminal Acts Of Dissemination Of Population Document Data By Dinas Dukcapil Kab. Mukomuko (Study Of Mukomuko District Police Legal Area." *Jurnal Hukum Sehasen*, Vol. 10, No. 1, 2024, Pp. 329–38.

[10] Prisdallini, Diaz Marsillo, And Andrie Irawan. "Analisis Pengaturan Hukum Terhadap Kejahatan Siber Doxing Di Indonesia." *Indonesian Journal Of Islamic Jurisprudence, Economic And Legal Theory*, Vol. 2, No. 3, 2024, Pp. 1494–501.

[11] Saly, Jeane Neltje, And Lubna Tabriz Sulthanah. "Pelindungan Data Pribadi Dalam Tindakan Doxing Berdasarkan Undang-Undang Nomor 27 Tahun 2022." *Jurnal Kewarganegaraan*, Vol. 7, No. 2, 2023, Pp. 1708–13.

[12] Samad, M. Yusuf, And Pratama Dahlian Persadha. "Pendekatan Intelijen Strategis Sebagai Upaya Memberikan Perlindungan Di Ruang Siber Dalam Konteks Kebebasan Menyatakan Pendapat."

Kajian, Vol. 27, No. 1, 2022, Pp. 31–42.

[13] Shafira, Anargya, And Dian Narwastuty. "Perlindungan Data Pribadi Pelaku Cyberbullying Di Bawah Umur Dihubungkan Dengan Tindakan Doxing Oleh Pengguna Media Sosial Menurut Uu Pdp." *Unes Journal Of Swara Justisia*, Vol. 9, No. 1, 2025, Pp. 37–44.

[14] Syailendra, Moody Rizqi, et.al. "Studi Kasus Sebuah Ancaman Terhadap Privasi Kasus Doxing Di Indonesia Dalam Perspektif Hukum Dan Etika." *Multilingual: Journal Of Universal Studies*, Vol. 4, No. 4, 2024, Pp. 32–45.

[15] Syuhada, Esa Arung, And Pramudya Fikri Ananta. "Perlindungan Data Pribadi Terhadap Tindakan Doxing Dalam Perspektif Hukum Pidana." *Jurnal Humaniora*, Vol. 2, No. 1, 2024, Pp. 37–46.

[16] Uweng, Intan Saripa, et.al. "Perlindungan Hukum Pidana Terhadap Doxing Menurut Undang-Undang Informasi Dan Transaksi Elektronik." *Pattimura Law Study Review*, Vol. 1, No. 1, 2023, Pp. 168–79.

[17] Wulandari, Laely, And Idi Amin. "Perlindungan Hukum Terhadap Pengguna Pinjaman Online Yang Menjadi Korban Tindak Pidana Pencurian Data Pribadi." *Parhesia*, Vol. 3, No. 1, 2025, Pp. 1–15.