

Analisis Hukum Pertanggungjawaban Pelaku *Doxxing* terhadap Pelanggaran Hak Privasi di Media Digital

Richard Anggiat Oloan¹, Aturkian Laia²

Ilmu Hukum, Hukum, Universitas Dirgantara Marsekal Suryadarma, Jakarta Timur, Indonesia¹

Ilmu Hukum, Hukum, Universitas Dirgantara Marsekal Suryadarma, Jakarta Timur, Indonesia²

*Email Korespodensi: richard.anggiat23@gmail.com

Sejarah Artikel:

Diterima 11-07-2026
Disetujui 17-07-2026
Diterbitkan 19-07-2026

ABSTRACT

Doxxing is the unauthorized gathering and dissemination of personal data in digital media to intimidate victims, yet the term remains unregulated under a standalone legal norm in Indonesia. This normative juridical research aims to analyze doxxing as a privacy violation, the perpetrator's legal liability, and regulatory effectiveness using statutory, conceptual, and case approaches. The results indicate that doxxing is qualified as a multi-layered criminal offense scattered across the Criminal Code (defamation), the Personal Data Protection Law (Article 65 juncto Article 67), and the Electronic Information and Transactions Law (Article 26). Criminal liability is cumulative-alternative, while victim recovery can be pursued through criminal channels, civil lawsuits for unlawful acts, or administrative sanctions. However, its effectiveness is hindered by fragmented norms, difficulties in digital evidence gathering, and perpetrator anonymity. This study recommends regulatory harmonization and capacity-strengthening for cyber law enforcement to ensure legal certainty for citizens' privacy rights in the digital space.

Keywords: *doxxing; right to privacy; personal data; criminal liability; cybercrime.*

ABSTRAK

Doxxing merupakan tindakan mengumpulkan dan menyebarluaskan data pribadi tanpa persetujuan di media digital demi mengintimidasi korban, namun istilah ini belum diatur eksplisit secara mandiri di Indonesia. Penelitian yuridis normatif ini bertujuan menganalisis *doxxing* sebagai pelanggaran privasi, pertanggungjawaban hukum pelaku, dan efektivitas regulasinya menggunakan pendekatan perundang-undangan, konseptual, dan kasus. Hasil penelitian menunjukkan *doxxing* dikualifikasikan sebagai tindak pidana berlapis yang tersebar dalam KUHP (penghinaan), UU Pelindungan Data Pribadi (Pasal 65 *juncto* Pasal 67), dan UU ITE (Pasal 26). Pertanggungjawaban pidana bersifat kumulatif-alternatif, sedangkan pemulihan korban dapat ditempuh lewat jalur pidana, gugatan perdata perbuatan melawan hukum, maupun sanksi administratif. Namun, efektivitasnya terhambat oleh fragmentasi norma, kesulitan pembuktian digital, dan anonimitas pelaku. Penelitian ini merekomendasikan harmonisasi regulasi serta penguatan kapasitas penegak hukum siber demi menjamin kepastian hukum privasi warga negara di ruang digital.

Katakunci: *doxxing; hak privasi; data pribadi; pertanggungjawaban pidana; kejahatan siber.*

PENDAHULUAN

Perkembangan media digital dan platform media sosial telah mengubah cara masyarakat berinteraksi, berkomunikasi, sekaligus berkonflik. Salah satu bentuk konflik yang semakin sering muncul di ruang siber adalah *doxxing*, yaitu tindakan mengumpulkan informasi pribadi seseorang, seperti nama lengkap, alamat rumah, nomor telepon, tempat kerja, atau identitas keluarga, kemudian menyebarkan secara terbuka tanpa persetujuan pemilik data dengan maksud mempermalukan, mengintimidasi, atau mengarahkan gangguan pihak lain kepada korban. *Doxxing* kerap muncul sebagai buntut dari perseteruan di media sosial, debat publik, maupun sebagai bentuk balas dendam pribadi, dan dapat menasar siapa saja, mulai dari warganet biasa, jurnalis, aktivis, hingga tokoh publik.

Karakteristik *doxxing* yang khas terletak pada penggunaan data yang sesungguhnya benar dan valid, bukan informasi palsu, sehingga berbeda dengan pencemaran nama baik konvensional yang umumnya berbasis pernyataan tidak benar. Justru karena data yang disebarkan bersifat akurat dan dapat diverifikasi, *doxxing* menjadi bentuk kejahatan yang unik karena memanfaatkan kebenaran itu sendiri sebagai senjata untuk membuka ruang privat seseorang kepada publik yang tidak berhak mengetahuinya, sehingga berpotensi memicu perundungan siber, ancaman fisik, hilangnya pekerjaan, hingga trauma psikologis bagi korban.

Meskipun dampaknya nyata dan serius, *doxxing* belum diatur sebagai delik tersendiri secara eksplisit dalam sistem hukum pidana Indonesia. Wura, Rabawati, dan Arman (2026) menegaskan bahwa Indonesia belum memiliki rumusan delik *doxxing* yang jelas, tidak membedakan unsur kesengajaan dan kelalaian dalam pertanggungjawaban pidana, serta belum menyediakan mekanisme perlindungan korban yang cepat dan komprehensif, berbeda dengan Singapura yang telah mengatur *doxxing* secara spesifik melalui *Protection from Harassment Act*. Kekosongan pengaturan yang eksplisit ini menimbulkan persoalan yuridis tersendiri, karena penegak hukum harus mengonstruksikan *doxxing* melalui berbagai ketentuan yang tersebar pada rezim hukum yang berbeda-beda, yaitu hukum pidana umum, hukum perlindungan data pribadi, dan hukum informasi elektronik.

Perkembangan terbaru memperlihatkan bahwa kerangka hukum Indonesia sesungguhnya semakin lengkap untuk menjerat pelaku *doxxing*. Berlakunya Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi menjadi tonggak penting karena secara eksplisit melarang setiap orang memperoleh, mengungkapkan, atau menggunakan data pribadi milik orang lain secara melawan hukum. Demikian pula, mulai berlakunya Undang-Undang Nomor 1 Tahun 2023 tentang Kitab Undang-Undang Hukum Pidana sejak 2 Januari 2026 turut menghadirkan bab khusus mengenai tindak pidana pembukaan rahasia yang relevan dengan karakteristik *doxxing*. Namun demikian, keberadaan norma yang tersebar pada berbagai undang-undang tersebut justru memunculkan persoalan baru, yaitu potensi tumpang tindih, perbedaan penafsiran unsur melawan hukum, dan ketidakpastian mengenai rezim hukum mana yang paling tepat digunakan untuk menjerat pelaku dalam situasi konkret.

Ketidakpastian ini bahkan telah sampai pada tahap pengujian konstusionalitas. Mahkamah Konstitusi tengah memeriksa permohonan pengujian materiil terhadap Pasal 65 ayat (2) *juncto* Pasal 67 ayat (2) Undang-Undang Pelindungan Data Pribadi yang diajukan oleh koalisi masyarakat sipil, dengan argumen bahwa rumusan larangan mengungkapkan data pribadi tanpa pengecualian yang tegas berpotensi mengkriminalisasi kerja jurnalistik, akademik, dan kesenian yang sah (Mahkamah Konstitusi Republik Indonesia, 2025). Persoalan ini menegaskan bahwa batas antara *doxxing* yang melawan hukum dengan pengungkapan data pribadi yang sah demi kepentingan publik masih memerlukan penegasan yuridis lebih lanjut, sehingga kajian mendalam mengenai karakteristik dan pertanggungjawaban hukum pelaku *doxxing*

menjadi semakin relevan dan mendesak untuk dilakukan.

Sejumlah penelitian hukum telah mengkaji fenomena *doxxing* di Indonesia dalam sepuluh tahun terakhir. Bagiartha W. (2021) merupakan salah satu penelitian awal yang mengkaji perilaku *doxxing* dan pengaturannya dalam positivisme hukum Indonesia, menemukan bahwa *doxxing* pada dasarnya dapat disentuh oleh ketentuan umum mengenai penghinaan dan penyalahgunaan informasi elektronik meskipun belum ada delik yang secara spesifik menamainya sebagai *doxxing*.

Achmad, Farid, Januarti, dan Syavira (2023) meneliti perlindungan hukum terhadap korban kejahatan *doxxing* di Indonesia dan menemukan bahwa korban *doxxing* menghadapi hambatan signifikan dalam memperoleh pemulihan, khususnya karena proses pelaporan yang rumit dan minimnya pemahaman aparat penegak hukum mengenai karakteristik teknis kejahatan siber. Uweng Saripa, Wadjo, dan Saimima (2023) mengkaji perlindungan hukum pidana terhadap *doxxing* menurut Undang-Undang Informasi dan Transaksi Elektronik dan menyimpulkan bahwa Pasal 26 dan Pasal 27 undang-undang tersebut dapat digunakan untuk menjerat pelaku, meskipun penerapannya bergantung pada penafsiran hakim terhadap unsur tanpa hak dan melawan hukum.

Armando dan Soeskandi (2023) secara spesifik menganalisis pertanggungjawaban pidana bagi para pelaku *doxxing* menurut Undang-Undang Informasi dan Transaksi Elektronik serta Undang-Undang Pelindungan Data Pribadi, dan menyimpulkan bahwa kombinasi kedua undang-undang tersebut memberi landasan yang lebih kuat bagi praktisi hukum untuk mempidanakan pelaku *doxxing* dibandingkan mengandalkan Kitab Undang-Undang Hukum Pidana lama semata. Saly dan Sulthanah (2023) mengkaji perlindungan data pribadi dalam tindakan *doxxing* berdasarkan Undang-Undang Nomor 27 Tahun 2022 dan menegaskan bahwa kehadiran undang-undang tersebut mengisi kekosongan hukum yang sebelumnya menyulitkan penjeratan pelaku *doxxing* yang tidak menyertakan unsur pencemaran nama baik secara eksplisit.

Syuhada dan Ananta (2024) meneliti perlindungan data pribadi terhadap tindakan *doxxing* dalam perspektif hukum pidana dan menemukan bahwa unsur kesengajaan menjadi titik krusial yang paling sulit dibuktikan dalam praktik penegakan hukum. Satria dan Yusuf (2024) menganalisis secara yuridis tindakan kriminal *doxxing* berdasarkan Undang-Undang Nomor 27 Tahun 2022 dan menekankan pentingnya edukasi hukum bagi masyarakat mengenai batas sah dan tidak sahnya penyebaran data pribadi di ruang digital. Permata dan Nurhadiyanto (2024) mengkaji perilaku *doxxing* sebagai bentuk *cancel culture* pada pengguna media sosial X, menyoroti dimensi sosiologis *doxxing* sebagai instrumen sanksi sosial informal yang kerap melampaui proporsi kesalahan awal korban.

Mahendra, Hafrida, dan Liyus (2025) mengkaji kebijakan hukum pidana terhadap penyebaran data pribadi jurnalis dan menyoroti kerentanan khusus jurnalis sebagai kelompok yang paling sering menjadi sasaran *doxxing* akibat pekerjaannya, sekaligus menegaskan perlunya keseimbangan antara pelindungan data pribadi dan kebebasan pers. Ahmad, Jasmaniar, dan Tenriliweng (2026) meneliti problematika kekosongan hukum pidana terhadap *doxxing* di Indonesia dan menyimpulkan bahwa meskipun *doxxing* dapat dikualifikasikan sebagai tindak pidana melalui ketentuan yang tersebar dalam Undang-Undang Informasi dan Transaksi Elektronik, Kitab Undang-Undang Hukum Pidana, dan Undang-Undang Pelindungan Data Pribadi, pengaturan yang parsial tersebut menimbulkan kelemahan dalam kepastian unsur pidana dan mekanisme pembuktian. Wura, Rabawati, dan Arman (2026) melengkapi kajian tersebut dengan perbandingan hukum pidana Indonesia dan Singapura, merekomendasikan perumusan delik *doxxing* yang spesifik sebagai kebijakan hukum pidana ideal (*ius constituendum*) bagi Indonesia.

Penelitian-penelitian terdahulu umumnya menganalisis *doxxing* melalui satu rezim hukum tertentu

secara terpisah, baik hanya dari perspektif Undang-Undang Informasi dan Transaksi Elektronik (Uweng Saripa dkk., 2023), hanya dari perspektif Undang-Undang Pelindungan Data Pribadi (Saly & Sulthanah, 2023; Satria & Yusuf, 2024), maupun hanya dari perspektif kekosongan hukum pidana secara umum tanpa menyertakan analisis mendalam mengenai bentuk pertanggungjawaban dan upaya pemulihan bagi korban secara terintegrasi (Ahmad dkk., 2026). Penelitian ini berbeda karena mengintegrasikan tiga rezim hukum sekaligus, yaitu Kitab Undang-Undang Hukum Pidana yang baru berlaku sejak 2 Januari 2026, Undang-Undang Pelindungan Data Pribadi, dan Undang-Undang Informasi dan Transaksi Elektronik, untuk memetakan secara sistematis karakteristik *doxxing*, konstruksi pertanggungjawaban hukumnya, serta bentuk pemulihan bagi korban, sekaligus menganalisis perkembangan aktual berupa pengujian konstitusionalitas norma pelindungan data pribadi yang sedang berlangsung di Mahkamah Konstitusi, sehingga menghasilkan pemetaan yuridis yang lebih mutakhir dan menyeluruh dibandingkan penelitian-penelitian sebelumnya.

Berdasarkan latar belakang yang telah dipaparkan, rumusan masalah dalam penelitian ini berfokus pada tiga persoalan utama. Pertama, bagaimana karakteristik *doxxing* sebagai bentuk pelanggaran hak privasi di media digital menurut hukum positif Indonesia. Kedua, bagaimana bentuk pertanggungjawaban hukum pelaku *doxxing* terhadap pelanggaran hak privasi di media digital tersebut. Ketiga, sejauh mana efektivitas pengaturan hukum di Indonesia dalam memberikan perlindungan hukum bagi korban *doxxing* sekaligus dalam menindak pelakunya.

Sejalan dengan rumusan masalah tersebut, penelitian ini memiliki tiga tujuan utama yang ingin dicapai. Pertama, untuk menganalisis secara mendalam konsep dan karakteristik *doxxing* sebagai bentuk penyebaran data pribadi tanpa persetujuan yang melanggar hak privasi dan menjadi bentuk kejahatan siber menurut hukum positif Indonesia. Kedua, untuk menganalisis secara komprehensif bentuk pertanggungjawaban hukum yang dapat dibebankan kepada pelaku *doxxing* berdasarkan Kitab Undang-Undang Hukum Pidana, Undang-Undang Pelindungan Data Pribadi, dan Undang-Undang Informasi dan Transaksi Elektronik. Ketiga, untuk menganalisis efektivitas pengaturan hukum Indonesia dalam memberikan perlindungan dan pemulihan bagi korban *doxxing* serta menindak pelakunya, sekaligus mengidentifikasi berbagai tantangan nyata yang dihadapi dalam proses penegakannya di era digital.

METODE PENELITIAN

Penelitian ini menggunakan metode penelitian hukum yuridis normatif (*normative legal research*), yaitu penelitian yang mengkaji hukum sebagai norma tertulis melalui penelaahan peraturan perundang-undangan, doktrin, dan bahan pustaka, tanpa meneliti perilaku sosial secara langsung di lapangan. Pendekatan yang digunakan meliputi pendekatan perundang-undangan (*statute approach*) untuk menelaah ketentuan yang relevan dengan *doxxing* pada berbagai undang-undang, pendekatan konseptual (*conceptual approach*) untuk menelaah konsep hak privasi, data pribadi, dan pertanggungjawaban pidana, serta pendekatan kasus (*case approach*) untuk menelaah contoh empiris praktik *doxxing* yang telah menjadi perhatian publik sebagai bahan analisis penerapan norma.

Bahan hukum primer yang digunakan meliputi Undang-Undang Dasar Negara Republik Indonesia Tahun 1945, Undang-Undang Nomor 39 Tahun 1999 tentang Hak Asasi Manusia, Undang-Undang Nomor 1 Tahun 2023 tentang Kitab Undang-Undang Hukum Pidana, Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi, dan Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik sebagaimana diubah terakhir dengan Undang-Undang Nomor 1 Tahun 2024. Bahan

hukum sekunder mencakup buku-buku hukum pidana, hukum privasi, dan hukum siber, serta jurnal ilmiah hukum nasional yang membahas *doxxing* dan perlindungan data pribadi dalam sepuluh tahun terakhir. Bahan hukum tersier berupa kamus hukum, publikasi resmi Mahkamah Konstitusi, dan pemberitaan media arus utama yang kredibel digunakan untuk memperjelas istilah teknis dan melengkapi data kontekstual perkembangan penegakan hukum *doxxing* di Indonesia.

Teknik analisis data dilakukan secara kualitatif dengan metode deskriptif-analitis, yaitu menguraikan norma dan bahan hukum yang terkumpul kemudian menganalisisnya secara sistematis untuk menjawab rumusan masalah. Penarikan kesimpulan menggunakan pola pikir deduktif, yaitu bertolak dari premis mayor berupa norma umum dalam Kitab Undang-Undang Hukum Pidana, Undang-Undang Pelindungan Data Pribadi, dan Undang-Undang Informasi dan Transaksi Elektronik, kemudian dihubungkan dengan premis minor berupa karakteristik dan pola perbuatan *doxxing* di ruang digital, sehingga diperoleh kesimpulan khusus mengenai karakteristik pelanggaran, bentuk pertanggungjawaban hukum, dan efektivitas perlindungan hukum bagi korban.

HASIL DAN PEMBAHASAN

Konsep *Doxxing* sebagai Bentuk Penyebaran Data Pribadi Tanpa Persetujuan

Doxxing, yang berasal dari singkatan istilah *dropping documents*, merujuk pada tindakan mengumpulkan informasi identitas seseorang dari berbagai sumber, baik melalui penelusuran daring maupun rekayasa sosial, kemudian menyebarkannya secara terbuka kepada publik tanpa persetujuan pemilik data. Informasi yang disebarakan dapat berupa nama lengkap, nomor induk kependudukan, alamat domisili, nomor telepon, tempat kerja, foto keluarga, hingga akun media sosial pribadi yang sebelumnya tidak diketahui publik secara luas. Ciri utama yang membedakan *doxxing* dari bentuk pelanggaran privasi lainnya adalah bahwa data yang disebarakan pada dasarnya benar dan akurat, bukan informasi rekaan, sehingga pelaku memanfaatkan validitas data tersebut sebagai instrumen untuk mengeksploitasi ruang privat korban.

Dari perspektif hukum perlindungan data pribadi, *doxxing* pada hakikatnya merupakan bentuk pemrosesan data pribadi tanpa dasar hukum yang sah. Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi mensyaratkan bahwa setiap pemrosesan data pribadi wajib didasarkan pada persetujuan eksplisit dari subjek data atau dasar hukum lain yang ditentukan secara limitatif dalam undang-undang. Pasal 65 ayat (1), ayat (2), dan ayat (3) undang-undang tersebut secara tegas melarang setiap orang memperoleh atau mengumpulkan, mengungkapkan, dan menggunakan data pribadi yang bukan miliknya secara melawan hukum. Ketiga bentuk larangan ini secara konseptual mencerminkan tiga tahap yang lazim terjadi dalam praktik *doxxing*, yaitu tahap pengumpulan data (*reconnaissance*), tahap pengungkapan data kepada publik (*exposure*), dan tahap pemanfaatan data oleh pihak ketiga untuk melakukan perundungan atau intimidasi lanjutan (*exploitation*).

Konstruksi ini penting secara analitis karena menunjukkan bahwa *doxxing* bukan sekadar peristiwa tunggal berupa unggahan data pribadi, melainkan rangkaian perbuatan yang dapat melibatkan lebih dari satu pelaku pada tahap yang berbeda. Pihak yang mengumpulkan data awal dapat berbeda dengan pihak yang menyebarkannya secara masif, dan dapat pula berbeda lagi dengan pihak ketiga yang memanfaatkan data tersebut untuk melakukan tindakan lanjutan seperti ancaman atau pelecehan. Pemisahan tahap ini relevan dalam menentukan pertanggungjawaban hukum masing-masing pihak, karena Pasal 67 Undang-Undang Pelindungan Data Pribadi memberikan ancaman pidana yang berbeda untuk

setiap bentuk perbuatan tersebut, yaitu pidana penjara paling lama lima tahun untuk perbuatan memperoleh atau mengumpulkan data pribadi secara melawan hukum, pidana penjara paling lama empat tahun untuk perbuatan mengungkapkan data pribadi, dan pidana penjara paling lama lima tahun untuk perbuatan menggunakan data pribadi secara melawan hukum, yang seluruhnya disertai ancaman pidana denda hingga miliaran rupiah.

Sifat khas *doxxing* yang memanfaatkan data valid juga menempatkannya pada posisi yang berbeda dari delik penyebaran berita bohong maupun pencemaran nama baik konvensional yang mensyaratkan unsur ketidakbenaran informasi. *Doxxing* justru menimbulkan kerugian melalui keterbukaan informasi yang sesungguhnya bersifat privat, sehingga letak kesalahan hukumnya bukan pada kebenaran atau ketidakbenaran isi informasi, mutlak pada ketiadaan hak dan persetujuan untuk mengungkapkannya kepada publik yang lebih luas dari yang semestinya berhak mengetahui.

Karakteristik *Doxxing* sebagai Pelanggaran Hak Privasi dan Kejahatan Siber

Hak atas privasi merupakan hak konstitusional yang dijamin oleh Pasal 28G ayat (1) Undang-Undang Dasar Negara Republik Indonesia Tahun 1945, yang menegaskan hak setiap orang atas perlindungan diri pribadi, keluarga, kehormatan, martabat, dan harta benda yang berada di bawah kekuasaannya, serta hak atas rasa aman dan perlindungan dari ancaman ketakutan untuk berbuat atau tidak berbuat sesuatu yang merupakan hak asasi. Ketentuan ini diperkuat oleh Pasal 21 Undang-Undang Nomor 39 Tahun 1999 tentang Hak Asasi Manusia yang menjamin kebebasan pribadi setiap orang. *Doxxing* secara langsung melanggar hak konstitusional ini karena mengekspos ruang privat seseorang kepada publik tanpa kendali dan persetujuan pemiliknya.

Sebagai bentuk kejahatan siber, *doxxing* memiliki karakteristik yang membedakannya dari kejahatan konvensional. Pertama, sifat lintas batas (*borderless*), karena pelaku dan korban dapat berada pada yurisdiksi yang berbeda, bahkan pelaku dapat menyembunyikan identitasnya melalui akun anonim atau palsu, sebagaimana disoroti dalam kajian mengenai *doxing* pada konteks Pemilu 2024 yang menemukan bahwa aparat penegak hukum kesulitan membuktikan unsur pidana ketika pelaku anonim atau menggunakan identitas palsu. Kedua, sifat masif dan cepat menyebar (*virality*), karena begitu data pribadi terunggah di media sosial, penyebarannya dapat berlangsung di luar kendali pelaku awal melalui tindakan pihak ketiga yang turut membagikan ulang informasi tersebut. Ketiga, sifat permanen (*persistence*), karena data yang telah tersebar di ruang digital sangat sulit dihapus secara menyeluruh meskipun unggahan awal telah dihapus oleh pelaku maupun platform.

Karakteristik lain yang relevan secara yuridis adalah kedudukan *doxxing* sebagai delik yang berpotensi menimbulkan tindak pidana lanjutan. Data pribadi yang tersebar dapat dimanfaatkan pihak lain untuk melakukan perundungan siber, ancaman kekerasan, penguntitan (*stalking*), maupun kejahatan finansial seperti penipuan berbasis rekayasa sosial. Karakteristik berlapis ini menjadikan *doxxing* sebagai perbuatan yang secara konseptual dapat dikategorikan sebagai delik yang menimbulkan bahaya abstrak sekaligus bahaya konkret, karena pengungkapan data itu sendiri sudah merupakan pelanggaran hak privasi, sementara akibat lanjutan yang timbul daripadanya dapat berupa kerugian materiil maupun immateriil yang lebih besar bagi korban.

Dalam konteks Kitab Undang-Undang Hukum Pidana yang baru, yaitu Undang-Undang Nomor 1 Tahun 2023 yang resmi berlaku sejak 2 Januari 2026, karakteristik *doxxing* dapat dianalisis melalui dua kelompok delik yang relevan, yaitu Bab XVII mengenai Tindak Pidana Penghinaan dan Bab XVIII mengenai Tindak Pidana Pembukaan Rahasia. Kelompok delik pembukaan rahasia secara konseptual lebih

tepat menggambarkan inti perbuatan *doxxing*, karena fokusnya terletak pada perbuatan membuka atau mengungkapkan sesuatu yang seharusnya dirahasiakan, sejalan dengan karakteristik *doxxing* yang mengekspos informasi privat kepada pihak yang tidak berhak mengetahuinya. Sementara itu, kelompok delik penghinaan lebih relevan diterapkan apabila pengungkapan data pribadi tersebut disertai dengan narasi yang merendahkan kehormatan atau nama baik korban.

Pertanggungjawaban Hukum Pelaku Doxxing Berdasarkan Hukum Pidana, Perlindungan Data Pribadi, dan Hukum Informasi Elektronik

Pertanggungjawaban hukum pelaku *doxxing* di Indonesia bersifat kumulatif-alternatif karena dapat dikonstruksikan melalui tiga rezim hukum yang saling melengkapi, bergantung pada bentuk perbuatan, media yang digunakan, dan akibat yang ditimbulkan.

Pertama, pertanggungjawaban berdasarkan Undang-Undang Pelindungan Data Pribadi. Pasal 67 undang-undang tersebut merupakan dasar hukum paling spesifik untuk menjerat pelaku *doxxing*, karena secara eksplisit mengancam pidana bagi setiap orang yang dengan sengaja dan melawan hukum memperoleh, mengungkapkan, atau menggunakan data pribadi yang bukan miliknya. Unsur dengan sengaja dan melawan hukum menjadi elemen krusial yang harus dibuktikan, dan dalam konteks inilah letak kompleksitas hukum *doxxing* muncul, sebagaimana ditunjukkan oleh perdebatan dalam pengujian konstiusionalitas Pasal 65 ayat (2) *juncto* Pasal 67 ayat (2) di Mahkamah Konstitusi, yang mempersoalkan perlunya tafsir ketat dan tegas (*lex stricta*) atas unsur melawan hukum tersebut agar tidak mengkriminalisasi pengungkapan data pribadi yang dilakukan demi kepentingan publik yang sah, seperti kerja jurnalistik atau akademik (Mahkamah Konstitusi Republik Indonesia, 2025). Konsekuensinya, penerapan Pasal 67 Undang-Undang Pelindungan Data Pribadi terhadap pelaku *doxxing* memerlukan pembuktian yang cermat bahwa pengungkapan data dilakukan tanpa dasar hukum yang sah dan tanpa kepentingan publik yang dapat dibenarkan, bukan semata-mata karena data tersebut diungkapkan tanpa persetujuan.

Kedua, pertanggungjawaban berdasarkan Kitab Undang-Undang Hukum Pidana. Sebelum berlakunya Undang-Undang Pelindungan Data Pribadi, penjeratan pelaku *doxxing* lazim mengandalkan ketentuan umum mengenai penghinaan dalam Kitab Undang-Undang Hukum Pidana lama. Uweng Saripa, Wadjo, dan Saimima (2023) mencatat bahwa pendekatan ini kerap tidak sepenuhnya tepat karena delik penghinaan mensyaratkan unsur maksud menyerang kehormatan atau nama baik, sementara *doxxing* tidak selalu disertai narasi yang merendahkan korban secara eksplisit. Berlakunya Kitab Undang-Undang Hukum Pidana baru sejak awal tahun 2026 membuka ruang penerapan yang lebih relevan melalui Bab XVIII mengenai Tindak Pidana Pembukaan Rahasia, yang secara konseptual lebih dekat dengan karakteristik inti *doxxing* dibandingkan delik penghinaan, karena fokusnya adalah perbuatan mengungkapkan sesuatu yang bersifat rahasia atau privat tanpa hak, terlepas dari ada tidaknya unsur penghinaan di dalamnya.

Ketiga, pertanggungjawaban berdasarkan Undang-Undang Informasi dan Transaksi Elektronik. Pasal 26 ayat (1) undang-undang ini menegaskan bahwa penggunaan setiap informasi melalui media elektronik yang menyangkut data pribadi seseorang harus dilakukan atas persetujuan orang yang bersangkutan, sehingga penyebaran data pribadi tanpa izin melalui media digital pada dasarnya juga melanggar ketentuan ini. Apabila penyebaran data pribadi tersebut disertai muatan yang melanggar kesusilaan, memuat ancaman kekerasan, atau bertujuan memeras dan mengintimidasi korban, ketentuan pidana dalam Pasal 27 dan Pasal 29 undang-undang ini turut relevan untuk diterapkan secara kumulatif bersama pelanggaran Pasal 26. Armando dan Soeskandi (2023) menegaskan bahwa kombinasi antara Undang-Undang Informasi dan Transaksi Elektronik dan Undang-Undang Pelindungan Data Pribadi

memberikan basis hukum yang jauh lebih kuat bagi praktisi hukum untuk mempidanakan pelaku *doxxing* dibandingkan hanya mengandalkan satu undang-undang saja.

Penerapan ketiga rezim hukum tersebut secara kumulatif-alternatif memungkinkan penegak hukum memilih dasar hukum yang paling sesuai dengan karakteristik perbuatan konkret, namun sekaligus menuntut kecermatan dalam menentukan dakwaan agar tidak terjadi tumpang tindih pemidanaan (*concursum*) yang keliru. Sebagai ilustrasi, apabila pelaku hanya mengumpulkan dan menyebarkan data pribadi tanpa disertai narasi yang merendahkan, penerapan Pasal 67 Undang-Undang Pelindungan Data Pribadi *juncto* Pasal 26 Undang-Undang Informasi dan Transaksi Elektronik lebih tepat digunakan. Sebaliknya, apabila penyebaran data pribadi disertai narasi yang secara eksplisit merendahkan kehormatan korban, ketentuan mengenai tindak pidana penghinaan dalam Kitab Undang-Undang Hukum Pidana dapat diterapkan secara kumulatif bersama Undang-Undang Pelindungan Data Pribadi.

Bentuk Perlindungan Hukum dan Upaya Pemulihan bagi Korban Doxxing

Perlindungan hukum bagi korban *doxxing* dapat ditempuh melalui tiga jalur yang bersifat komplementer, yaitu jalur pidana, jalur perdata, dan jalur administratif.

Jalur pidana ditempuh melalui pelaporan kepada kepolisian, khususnya unit yang menangani kejahatan siber, dengan dasar hukum berupa pelanggaran Undang-Undang Pelindungan Data Pribadi, Kitab Undang-Undang Hukum Pidana, dan/atau Undang-Undang Informasi dan Transaksi Elektronik sebagaimana diuraikan di atas. Namun demikian, Achmad, Farid, Januarti, dan Syavira (2023) menemukan bahwa korban *doxing* menghadapi hambatan signifikan dalam jalur ini, khususnya karena proses pelaporan yang rumit dan minimnya pemahaman aparat penegak hukum mengenai karakteristik teknis kejahatan siber, sehingga banyak kasus *doxing* yang tidak berlanjut ke tahap penyidikan secara efektif.

Jalur perdata memberikan alternatif pemulihan melalui gugatan ganti kerugian berdasarkan perbuatan melawan hukum sebagaimana diatur dalam Kitab Undang-Undang Hukum Perdata, dengan lima unsur yang harus dibuktikan, yaitu adanya perbuatan, sifat melawan hukum, unsur kesalahan, kerugian yang timbul, dan hubungan kausal antara perbuatan dan kerugian tersebut. Jalur ini relevan khususnya bagi korban yang mengalami kerugian materiil nyata, seperti kehilangan pekerjaan atau biaya pemulihan psikologis, karena gugatan perdata memungkinkan penghitungan dan pembebanan ganti rugi secara lebih konkret dibandingkan proses pidana yang berorientasi pada pemidanaan pelaku.

Jalur administratif merupakan jalur baru yang dibuka oleh Undang-Undang Pelindungan Data Pribadi, yaitu pengaduan kepada lembaga pengawas pelindungan data pribadi yang berwenang menerima keluhan subjek data, memeriksa dugaan pelanggaran, dan menjatuhkan sanksi administratif kepada pihak yang melanggar kewajiban pemrosesan data pribadi. Jalur ini memiliki keunggulan berupa proses yang secara teoretis lebih cepat dibandingkan proses pidana maupun perdata, meskipun efektivitasnya masih bergantung pada kematangan kelembagaan otoritas pengawas yang relatif baru dibentuk.

Di luar ketiga jalur hukum formal tersebut, korban *doxing* juga dapat menempuh upaya mitigasi cepat berupa pengamanan bukti digital melalui tangkapan layar yang mencantumkan waktu dan tautan unggahan, pelaporan kepada penyelenggara platform media sosial untuk penghapusan konten yang melanggar ketentuan privasi, serta permintaan penghapusan data pribadi kepada pengendali data sebagaimana dijamin sebagai hak subjek data dalam Undang-Undang Pelindungan Data Pribadi. Kombinasi antara upaya mitigasi teknis dan penempuhan jalur hukum formal ini penting mengingat sifat data digital yang cepat menyebar dan sulit dihapus secara menyeluruh begitu telah beredar luas di ruang siber.

Efektivitas Pengaturan Hukum dan Tantangan Penegakan terhadap Praktik Doxxing

Meskipun kerangka hukum Indonesia saat ini secara kumulatif telah mampu menjangkau sebagian besar bentuk perbuatan *doxxing* melalui kombinasi Kitab Undang-Undang Hukum Pidana, Undang-Undang Pelindungan Data Pribadi, dan Undang-Undang Informasi dan Transaksi Elektronik, efektivitas penerapannya di lapangan masih menghadapi sejumlah tantangan struktural yang signifikan.

Tantangan pertama adalah fragmentasi norma. *Doxxing* di Indonesia dijerat melalui ketentuan yang tersebar pada sekurang-kurangnya tiga undang-undang berbeda, tanpa adanya delik *doxing* yang berdiri sendiri dengan unsur yang dirumuskan secara spesifik. Wura, Rabawati, dan Arman (2026) menunjukkan bahwa kondisi ini berbeda signifikan dengan Singapura yang telah merumuskan delik *doxing* secara eksplisit melalui *Protection from Harassment Act*, lengkap dengan unsur perbuatan, maksud jahat, dan akibat hukum yang terperinci, sehingga memberikan kepastian hukum yang lebih tinggi bagi penegak hukum maupun masyarakat.

Tantangan kedua adalah kekaburan unsur melawan hukum, sebagaimana tercermin dalam pengujian konstitusionalitas Pasal 65 ayat (2) *juncto* Pasal 67 ayat (2) Undang-Undang Pelindungan Data Pribadi yang tengah diperiksa Mahkamah Konstitusi. Ketidadaan rumusan pengecualian yang tegas bagi pengungkapan data pribadi demi kepentingan publik yang sah berpotensi menimbulkan dua risiko yang saling bertentangan, yaitu risiko kriminalisasi berlebihan terhadap kerja jurnalistik dan akademik di satu sisi, serta risiko pelemahan perlindungan korban *doxing* apabila pelaku berlindung di balik dalih kepentingan publik secara tidak proporsional di sisi lain (Mahkamah Konstitusi Republik Indonesia, 2025).

Tantangan ketiga adalah kesulitan pembuktian digital dan anonimitas pelaku. Sifat data elektronik yang mudah dihapus, dimodifikasi, atau disamarkan menyulitkan proses pembuktian di persidangan, terlebih apabila pelaku menggunakan akun anonim atau identitas palsu sebagaimana ditemukan dalam kajian mengenai *doxing* pada konteks Pemilu 2024. Syuhada dan Ananta (2024) turut menegaskan bahwa unsur kesengajaan menjadi elemen yang paling sulit dibuktikan dalam praktik penegakan hukum *doxing*, mengingat pelaku dapat berdalih bahwa penyebaran data dilakukan tanpa maksud jahat.

Tantangan keempat adalah rendahnya pemahaman aparat penegak hukum dan masyarakat mengenai karakteristik teknis kejahatan siber, sebagaimana ditemukan oleh Achmad, Farid, Januarti, dan Syavira (2023), yang menyebabkan proses pelaporan korban *doxing* seringkali tidak berlanjut secara efektif ke tahap penyidikan. Tantangan kelima adalah kerentanan kelompok tertentu, khususnya jurnalis, sebagaimana disoroti oleh Mahendra, Hafrida, dan Liyus (2025), yang menghadapi risiko *doxing* lebih tinggi akibat sifat pekerjaannya yang menuntut keterbukaan informasi, namun belum memperoleh perlindungan hukum yang secara khusus mempertimbangkan konteks profesinya.

Untuk mengatasi tantangan-tantangan tersebut, penelitian ini merekomendasikan tiga langkah kebijakan. Pertama, harmonisasi regulasi melalui perumusan delik *doxing* yang spesifik, baik melalui revisi terbatas atas Kitab Undang-Undang Hukum Pidana maupun peraturan pelaksana Undang-Undang Pelindungan Data Pribadi, dengan unsur perbuatan, maksud, dan akibat yang dirumuskan secara jelas sebagaimana direkomendasikan oleh Wura, Rabawati, dan Arman (2026). Kedua, penegasan tafsir ketat dan tegas (*lex stricta*) atas unsur melawan hukum dalam Pasal 65 dan Pasal 67 Undang-Undang Pelindungan Data Pribadi melalui putusan Mahkamah Konstitusi maupun peraturan pelaksana, guna memberikan kepastian hukum yang seimbang antara pelindungan data pribadi dan kebebasan berekspresi yang sah. Ketiga, penguatan kapasitas aparat penegak hukum siber melalui pelatihan khusus mengenai forensik digital dan karakteristik teknis *doxing*, disertai penyederhanaan mekanisme pelaporan bagi korban agar proses penegakan hukum dapat berjalan lebih responsif dan efektif.

KESIMPULAN

Berdasarkan analisis yang telah diuraikan, penelitian ini menyimpulkan tiga hal pokok. Pertama, *doxxing* merupakan bentuk pelanggaran hak privasi yang khas karena memanfaatkan data pribadi yang valid dan akurat, bukan informasi palsu, untuk mengekspos ruang privat seseorang kepada publik tanpa persetujuan, sehingga karakteristiknya berbeda dari delik penyebaran berita bohong maupun pencemaran nama baik konvensional. Sebagai bentuk kejahatan siber, *doxxing* memiliki karakteristik lintas batas, masif, permanen, dan berpotensi menimbulkan tindak pidana lanjutan, yang secara konseptual paling relevan dikualifikasikan sebagai bentuk pelanggaran hak konstitusional atas privasi berdasarkan Pasal 28G ayat (1) Undang-Undang Dasar Negara Republik Indonesia Tahun 1945.

Kedua, pertanggungjawaban hukum pelaku *doxxing* bersifat kumulatif-alternatif melalui tiga rezim hukum yang saling melengkapi, yaitu Undang-Undang Pelindungan Data Pribadi melalui Pasal 65 *juncto* Pasal 67 sebagai dasar hukum paling spesifik, Kitab Undang-Undang Hukum Pidana melalui ketentuan mengenai tindak pidana pembukaan rahasia dan penghinaan, serta Undang-Undang Informasi dan Transaksi Elektronik melalui Pasal 26, Pasal 27, dan Pasal 29, dengan pemilihan dasar hukum yang bergantung pada bentuk perbuatan konkret dan akibat yang ditimbulkan.

Ketiga, efektivitas pengaturan hukum Indonesia dalam melindungi korban dan menindak pelaku *doxxing* masih terhambat oleh fragmentasi norma antarundang-undang, kekaburan unsur melawan hukum sebagaimana tercermin dalam pengujian konstitusionalitas yang tengah berlangsung di Mahkamah Konstitusi, kesulitan pembuktian digital dan anonimitas pelaku, serta rendahnya kapasitas aparat penegak hukum dalam menangani kejahatan siber. Guna memperkuat efektivitas perlindungan hukum di masa mendatang, diperlukan perumusan delik *doxing* yang spesifik, penegasan tafsir ketat atas unsur melawan hukum dalam Undang-Undang Pelindungan Data Pribadi, serta penguatan kapasitas penegak hukum siber, agar hak privasi warga negara di ruang digital dapat terlindungi secara adil dan proporsional tanpa mengorbankan kebebasan berekspresi yang sah.

DAFTAR PUSTAKA

- Achmad, D., Farid, M., Januarti, R. P., & Syavira, A. (2023). Legal protection against victims of doxing crime in Indonesia. *Jurnal Bina Mulia Hukum*, 8(1), 92–105. <https://doi.org/10.23920/jbmh.v8i1.1218>
- Ahmad, M. A. R., Jasmaniar, & Tenriliweng, A. D. (2026). Doxing di Indonesia dan problematika kekosongan hukum pidana. *Legal Dialogica*, 1(2), 1–10.
- Armando, M. A. C., & Soeskandi, H. (2023). Pertanggungjawaban pidana bagi para pelaku doxing menurut UU ITE dan UU PDP. *Bureaucracy Journal: Indonesia Journal of Law and Social-Political Governance*, 3(1), 559–568. <https://doi.org/10.53363/buan.v3i1.215>
- Bagiarttha W., I. P. P. (2021). Perilaku doxing dan pengaturannya dalam positivisme hukum Indonesia. *Widya Kerta: Jurnal Hukum Agama Hindu*, 4(2), 91–104. <https://doi.org/10.53977/wk.v4i2.368>
- Indonesia. (1847). *Kitab Undang-Undang Hukum Perdata* [Burgerlijk Wetboek]. Burgerlijke Stand.
- Indonesia. (1945). *Undang-Undang Dasar Negara Republik Indonesia Tahun 1945*. Sekretariat Negara.
- Indonesia. (1999). *Undang-Undang Nomor 39 Tahun 1999 tentang Hak Asasi Manusia*. Lembaran Negara Republik Indonesia Tahun 1999 Nomor 165. Sekretariat Negara.
- Indonesia. (2008). *Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik*. Lembaran Negara Republik Indonesia Tahun 2008 Nomor 58. Sekretariat Negara.

- Indonesia. (2016). *Undang-Undang Nomor 19 Tahun 2016 tentang Perubahan atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik*. Lembaran Negara Republik Indonesia Tahun 2016 Nomor 251. Sekretariat Negara.
- Indonesia. (2022). *Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi*. Lembaran Negara Republik Indonesia Tahun 2022 Nomor 196. Sekretariat Negara.
- Indonesia. (2023). *Undang-Undang Nomor 1 Tahun 2023 tentang Kitab Undang-Undang Hukum Pidana*. Lembaran Negara Republik Indonesia Tahun 2023 Nomor 1. Sekretariat Negara.
- Indonesia. (2024). *Undang-Undang Nomor 1 Tahun 2024 tentang Perubahan Kedua atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik*. Lembaran Negara Republik Indonesia Tahun 2024 Nomor 1. Sekretariat Negara.
- Mahendra, B. T., Hafrida, & Liyus, H. (2025). Kebijakan hukum pidana terhadap penyebaran data pribadi (doxing) jurnalis dalam rangka perlindungan data pribadi di Indonesia. *Rio Law Jurnal*, 6(1), 643–650.
- Mahkamah Konstitusi Republik Indonesia. (2025). *Larangan ungkap data pribadi dalam UU PDP perlu tafsir ketat dan tegas*. <https://www.mkri.id>
- Permata, M. A., & Nurhadiyanto, L. (2024). Perspektif perilaku doxing sebagai bentuk cancel culture pada pengguna media sosial X. *Jurnal Ilmu Hukum, Humaniora dan Politik*, 4(4), 673–680. <https://doi.org/10.46339/jihhp.v4i4.1354>
- Saly, J. N., & Sulthanah, L. T. (2023). Pelindungan data pribadi dalam tindakan doxing berdasarkan Undang-Undang Nomor 27 Tahun 2022. *Jurnal Kewarganegaraan*, 7(2), 1708–1713.
- Satria, K. M., & Yusuf, H. (2024). Analisis yuridis tindakan kriminal doxing ditinjau berdasarkan Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi. *JICN: Jurnal Intelek dan Cendekiawan Nusantara*, 1(3), 2442–2456.
- Syuhada, E. A., & Ananta, P. F. (2024). Perlindungan data pribadi terhadap tindakan doxing dalam perspektif hukum pidana. *Jurhum: Jurnal Humaniora*, 2(1), 37–46. <https://doi.org/10.56957/jurhum.v2i1.134>
- Uweng Saripa, I., Wadjo, H. Z., & Saimima, J. M. (2023). Perlindungan hukum pidana terhadap doxing menurut Undang-Undang Informasi dan Transaksi Elektronik. *Pattimura Law Study Review*, 1(1), 168–179.
- Wura, H. H., Rabawati, D. W., & Arman, Y. (2026). Kebijakan formulatif tindak pidana doxing: Perbandingan hukum pidana Indonesia dan Singapura dalam perspektif ius constitutum dan ius constituendum. *DIVERSI: Jurnal Hukum*, 11(2), 243–268.