BAB II
UNSUR DOXING DALAM PERATURAN PERUNDANG-UNDANGAN

2.1 Sejarah Pengaturan Tindak Pidana Doxing Dalam UU ITE dan UU PDP

Konsep perlindungan data pribadi pertama kali dikenal dan dikembangkan pada sekitar tahun 1970 di beberapa negara Eropa, seperti Jerman dan Swedia, seiring dengan penggunaan komputer untuk menghimpun dan menyimpan data penduduk. Pada masa tersebut, data pribadi dipahami sebagai kumpulan informasi yang berkaitan dengan individu, meliputi fakta, komunikasi, maupun pendapat yang bersifat rahasia, privat, atau sensitif, sehingga pemilik data memiliki kepentingan untuk membatasi pihak lain dalam mengumpulkan, menggunakan, dan menyebarluaskannya.

Awalnya, pengumpulan data dilakukan untuk kepentingan administratif negara, seperti sensus penduduk, namun dalam praktiknya justru ditemukan berbagai pelanggaran terhadap keamanan dan kerahasiaan data. Kondisi tersebut mendorong pemerintah di berbagai negara untuk membentuk instrumen hukum yang secara khusus bertujuan melindungi data pribadi warga negara dari penyalahgunaan. Lalu sejalan dengan perkembangan tersebut, muncul kesadaran akademik dan yuridis mengenai pentingnya perlindungan terhadap hak privasi sebagai bagian dari hak asasi manusia.[20]

Konsep privasi modern pertama kali dirumuskan oleh Warren dan Brandeis melalui artikel ilmiah berjudul *The Right to Privacy* yang menegaskan bahwa kemajuan teknologi menuntut adanya pengakuan hukum atas hak individu untuk

---

[20] Edi Saputra Hasibuan, Lia Salsiah*, Urgensi Undang-Undang Perlindungan Data Pribadi Terhadap Kejahatan Pelanggaran Data Di Indonesia*, Jurnal Penelitian Bidang HukumUniversitas GresikVolume 11 Nomor 3, Oktober 2022, h. 65.

menikmati kehidupan pribadi tanpa gangguan, baik dari negara maupun dari pihak lain. Meskipun privasi merupakan konsep yang bersifat abstrak dan memiliki batasan yang berbeda-beda bagi setiap individu, esensinya terletak pada kebebasan seseorang untuk menentukan sejauh mana informasi mengenai dirinya dapat diakses atau digunakan oleh pihak lain. Pandangan ini memperkuat gagasan bahwa hukum memiliki kewajiban untuk mengakui dan melindungi hak privasi sebagai hak dasar.

Dalam perkembangannya, pemahaman mengenai data pribadi dan privasi juga memperoleh legitimasi dalam berbagai instrumen hukum internasional. Deklarasi Universal Hak Asasi Manusia secara tegas menyatakan bahwa setiap orang berhak atas perlindungan hukum dari gangguan sewenang-wenang terhadap kehidupan pribadi, keluarga, tempat tinggal, maupun korespondensi, serta dari serangan terhadap kehormatan dan reputasi. Prinsip tersebut menegaskan bahwa perlindungan privasi merupakan standar universal yang harus dijamin oleh negara melalui Peraturan Perundang-Undangan. Secara konseptual, privasi dipahami sebagai hak seseorang untuk bebas dari campur tangan yang tidak beralasan serta hak untuk mengendalikan arus informasi mengenai dirinya, termasuk dalam hubungan personal dan kehidupan sosial.[21]

Dalam konteks terminologi hukum, penggunaan istilah yang merujuk pada data pribadi menunjukkan adanya perbedaan antarnegara. Beberapa negara seperti Amerika Serikat, Kanada, dan Australia menggunakan istilah “informasi pribadi”, sedangkan Indonesia secara konsisten menggunakan istilah “data pribadi”,

[21] *Ibid,* h. 65-66.

sebagaimana tercermin dalam pengaturan mengenai perlindungan data dalam Undang-Undang tentang Informasi dan Transaksi Elektronik. Penggunaan istilah ini sejalan dengan praktik di negara-negara Uni Eropa yang juga menekankan perlindungan data pribadi sebagai bagian dari perlindungan hak privasi. Pemahaman tersebut menjadi landasan penting dalam pembentukan rezim hukum nasional terkait perlindungan data pribadi.

Indonesia sebagai negara hukum memiliki kewajiban konstitusional untuk melindungi rakyat Indonesia dan seluruh tumpah darah Indonesia. Hal ini tertuang dalam alinea ke-4 pembukaan UUD 1945 yang menyebutkan bahwa melindungi segenap bangsa Indonesia dan tumpah darah Indonesia dan untuk memajukan kesejahteraan umum, mencerdaskan kehidupan bangsa, dan ikut melaksanakan ketertiban dunia yang berdasarkan kemerdekaan, perdamaian abadi, dan keadilan sosial. [22]

Dalam perspektif hukum, doxing berkaitan erat dengan konsep perlindungan data pribadi dan hak privasi yang merupakan bagian dari hak asasi manusia. Hak privasi telah diakui oleh internasional sebagai instrumen hak asasi manusia yang juga dijamin oleh konstitusi negara Indonesia yang memberikan perlindungan terhadap kehormatan dan rasa aman individu. Perlindungan data pribadi berhubungan dengan konsep privasi, konsep privasi merupakan gagasan untuk menjaga integritas dan martabat pribadi. Substansi tindakan doxing memiliki relevansi dengan jaminan Hak privasi. Tindakan doxing menjadi sangat mendesak

[22] Bovin Tri Mahendra, Hafrida, Herry Liyus, *Kebijakan Hukum Pidana Terhadap Penyebaran Data Pribadi (Doxing) Jurnalis Dalam Rangka Perlindungan Data Pribadi Di Indonesia*, Rio Law Jurnal Volume. 1 Nomor. 2, Februari Juli 2025, h. 648.

untuk diatur melalui Peraturan Perundang-Undangan karena dapat menyebabkan dampak psikologis, sosial, hingga ekonomi bagi korban, seperti ancaman, intimidasi, penipuan, dan penguntitan (*stalking)*.[23]

Banyak kasus di Indonesia menunjukkan bahwa pelaku doxing seringkali memanfaatkan data pribadi seperti nomor telepon, alamat rumah, foto pribadi, hingga riwayat pekerjaan untuk mempermalukan atau menyerang korban. Hal inilah yang membuat pemerintah dan masyarakat melakukan pembahasan terkait pengaturan boxing dalam Undang-Undang Informasi dan Transaksi Elektronik dan Undang-Undang Perlindungan Data Pribadi.

Tindak pidana doxing merupakan perbuatan mengungkap, menyebarluaskan, atau mempublikasikan data pribadi seseorang tanpa hak melalui media elektronik atau sarana digital lainnya, sehingga menimbulkan kerugian baik secara materiil maupun immateriil bagi pihak yang bersangkutan. Data pribadi yang disebarluaskan dalam praktik doxing dapat berupa identitas diri, alamat tempat tinggal, nomor telepon, nomor identitas kependudukan, informasi keluarga, maupun data sensitif lainnya. Perbuatan tersebut pada hakikatnya melanggar hak atas privasi dan rasa aman seseorang, serta berpotensi menimbulkan ancaman, intimidasi, perundungan digital, hingga kekerasan lanjutan terhadap korban. Oleh karena itu, doxing dipandang sebagai salah satu bentuk kejahatan siber yang berkembang seiring dengan pesatnya pemanfaatan teknologi informasi dalam kehidupan masyarakat.[24]

---

[23] *Ibid.*

[24] Leonardo Latsiano Dade, *Kajian Yuridis Tentang Tindak Pidana Penyebaran Data Pribadi Melalui Internet (Doxing) Di Indonesia*, Jurnal Fakultas Hukum Universitas Sam Ratulangi Lex Privatum Vol.13 No.3 Feb 2024.

Secara historis, praktik doxing tidak lahir dari sistem hukum nasional, melainkan berkembang dari budaya komunitas daring internasional yang menjadikan pembocoran dokumen pribadi sebagai sarana tekanan sosial atau balas dendam. Istilah doxing berasal dari kata *"docs"* atau dokumen, yang merujuk pada tindakan membuka akses publik terhadap informasi personal seseorang. Fenomena ini kemudian menyebar secara luas seiring meningkatnya penggunaan media sosial dan kemudahan dalam mengakses serta menyebarkan informasi. Seiring perkembangan zaman doxing didefinisikan sebagai tindakan berbasis internet yang bertujuan untuk menyebarluaskan informasi pribadi secara publik terhadap seseorang atau publik. Tindak pidana ini dilakukan untuk memperoleh informasi termasuk mencari data yang tersedia untuk umum, dan situs sosial. Dalam konteks di Indonesia, praktik doxing telah terjadi jauh sebelum adanya pengaturan khusus mengenai perlindungan data pribadi, namun penanganannya masih bergantung pada ketentuan hukum yang bersifat umum dan belum secara eksplisit mengatur mengenai larangan pembocoran data pribadi.

Terdapat tiga jenis doxing yang pertama adalah *deanomisasi* yaitu doxing yang dilakukan dengan mengungkapkan identitas seseorang yang sebelumnya atau dari awal menganonimkan diri artinya tidak menggunakan nama asli. Kedua *Targeting doxing* ini dilakukan dengan mengungkapkan informasi spesifik tentang seseorang yang memungkinkan untuk ditemui atau dihubungi. Yang ketiga adalah *doxing deligitimasi*, doxing ini dilakukan dengan mengungkapkan informasi yang bersifat sensitif tentang seseorang. Keberadaan ratusan juta data pribadi penduduk Indonesia di dunia maya perlu mendapatkan perhatian dari pemerintah sebab

kemudahan akses internet merupakan ancaman komersialisasi serta penggunaan data pribadi secara ilegal melalui dunia maya.

Pengaturan awal yang dapat dikaitkan dengan tindak pidana doxing di Indonesia terdapat dalam Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik sebagaimana telah diubah dengan UU Nomor 19 Tahun 2016 juncto UU Nomor 1 Tahun 2024 Tentang Perubahan Kedua atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE). Meskipun UU ITE tidak menyebutkan istilah doxing secara eksplisit, norma-norma di dalamnya dapat digunakan untuk menjerat perbuatan yang memiliki karakteristik doxing. Ketentuan mengenai distribusi dan transmisi informasi elektronik yang melanggar hukum, penyalahgunaan data elektronik, serta perbuatan yang merugikan orang lain melalui media elektronik menjadi dasar hukum awal dalam menangani praktik doxing.[25] Dengan demikian, UU ITE berfungsi sebagai instrumen hukum pertama yang secara tidak langsung mengatur perbuatan pembocoran data pribadi di ruang digital.

Namun demikian, pengaturan dalam UU ITE dinilai belum memberikan perlindungan yang optimal terhadap korban doxing karena belum adanya pengakuan yang tegas mengenai data pribadi sebagai objek perlindungan hukum yang berdiri sendiri. UU ITE lebih menekankan pada aspek perbuatan di ruang siber, bukan pada substansi perlindungan data pribadi dan hak subjek data. Kondisi tersebut menimbulkan kekosongan hukum yang berdampak pada lemahnya

[25] *Ibid.*

kepastian hukum, baik bagi korban maupun aparat penegak hukum dalam menafsirkan unsur tindak pidana doxing.

Perkembangan selanjutnya menunjukkan bahwa pengaturan dalam UU ITE Awal mula dari perubahan terhadap UU ITE melalui Undang-Undang Nomor 19 Tahun 2016 sebelum regulasi baru yaitu UU Nomor 1 Tahun 2024 Tentang Perubahan Kedua atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik mulai digunakan sebagai dasar hukum untuk menindak perbuatan yang memiliki karakteristik doxing, khususnya melalui ketentuan mengenai distribusi dan transmisi informasi elektronik yang merugikan orang lain. Selain itu, ketentuan mengenai penggunaan data pribadi seseorang melalui media elektronik tanpa persetujuan juga menjadi rujukan penting dalam praktik penegakan hukum.

Meskipun demikian, konstruksi hukum tersebut masih bersifat implisit karena UU ITE tidak memberikan definisi yang jelas mengenai data pribadi maupun larangan eksplisit terhadap pembocoran data pribadi. Hal ini menyebabkan penafsiran hukum terhadap tindak pidana doxing sering kali bergantung pada konstruksi pasal lain, seperti pencemaran nama baik atau perbuatan tidak menyenangkan di ruang digital. Hal ini menunjukkan adanya upaya pembaruan hukum dalam merespons dinamika kejahatan siber, namun perubahan tersebut belum menyentuh secara mendalam aspek perlindungan data pribadi.

Dalam UU ITE Tahun 2008 tidak mendefinisikan secara jelas yang dimaksud dengan data pribadi dan tidak memberikan batasan mengenai jenis data yang dilindungi, ruang lingkup perlindungan, maupun sanksi terhadap penyebaran data

pribadi. Kelemahan tersebut menyebabkan penegakan hukum terhadap kasus doxing menjadi tidak maksimal. Banyak kasus doxing yang tidak dapat dijerat karena pasal yang tidak secara tegas mengkualifikasikan tindakan penyebaran data pribadi sebagai tindak pidana tersendiri. Aparat penegak hukum seringkali menggunakan bahasa lain seperti pencemaran nama baik, fitnah, atau akses ilegal untuk pelaku penyebaran data pribadi.

Pada tahun 2016 pemerintah melakukan revisi terhadap UU ITE melalui Undang-Undang Nomor 19 tahun 2016. Revisi UU ITE dilakukan akibat munculnya berbagai persoalan hukum yang memunculkan kontroversi dalam penegakan UU ITE, termasuk banyaknya pelanggaran privasi. Salah satu perubahan penting yang dilakukan oleh pemerintah adalah mengenai hak penghapusan informasi elektronik. Pak ini memungkinkan seseorang meminta penyelenggara sistem elektronik untuk menghapus informasi yang sudah tidak relevan, tidak akurat atau yang dapat merugikan.

Revisi UU ITE 2016 belum memberikan pengaturan lebih rinci mengenai penyalahgunaan data pribadi. Tindak pidana doxing belum diatur secara khusus sehingga aparat penegak hukum masih kesulitan menjerat pelaku doxing sehingga masih harus menggunakan pasal lain yang sebenarnya memiliki unsur berbeda. Artinya masih ada kekosongan hukum terkait pengaturan substansi terkait doxing. Hal ini memperlihatkan bahwa UU ITE belum mampu menjadi instrumen hukum yang efektif untuk menangani pelanggaran data pribadi seperti doxing.

Selain UU ITE terdapat Peraturan Perundang-Undangan lain seperti PP Nomor 82 Tahun 2012 tentang penyelenggaraan sistem dan transaksi elektronik,

yang kemudian digantikan oleh PP nomor 71 tahun 2019. Dalam PP ini mulai memuat prinsip perlindungan data pribadi seperti kewajiban pengendali data untuk menjaga kerahasiaan informasi dan memberikan pemberitahuan jika terjadi kebocoran data. Namun demikian, peraturan ini masih bersifat administratif dan belum mengatur aspek pidana secara spesifik terhadap pelaku penyebaran data pribadi.

Pembahasan rancangan Undang-Undang perlindungan data pribadi dimulai sejak tahun 2016, memerlukan waktu enam tahun sebelum akhirnya disahkan pada Tahun 2022. Proses ini memakan waktu panjang Karena banyaknya isu hukum yang diatur seperti definisi data pribadi, hak subjek data, kewajiban pengendali data, mekanisme pemrosesan data, hingga perdebatan terkait sanksi pidana dan denda. Pengesahan UU PDP menandai Babak baru perlindungan data pribadi di Indonesia regulasi ini menjadi payung hukum yang lebih rinci dan komprehensif dibandingkan UU ITE.

Dalam UU PDP memberikan pengaturan yang jauh lebih tegas terhadap penyalahgunaan data pribadi, termasuk tindakan doxing, beberapa pasal yang relevan antara lain, pada Pasal 65 yang melarang setiap orang memperoleh dan mengumpulkan data pribadi dengan cara yang tidak sah serta melarang pengungkapan data pribadi tanpa persetujuan subjek data. Selain itu sanksi pidana untuk pelanggaran tersebut diatur dalam Pasal 67 hingga Pasal 70 mengatur mengenai pidana penjara dan atau denda bagi pelaku yang menyebarkan data pribadi tanpa hak. Dengan adanya ketentuan ini, toxing menjadi perbuatan yang dapat dikualifikasikan sebagai tindak pidana secara langsung karena memenuhi

unsur penyebaran data pribadi tanpa persetujuan. Keamanan data melibatkan kepentingan masyarakat luas yang juga dapat mempengaruhi stabilitas negara.

Dalam perspektif historis, UU PDP dapat dipahami sebagai respons terhadap meningkatnya kompleksitas kejahatan siber yang tidak lagi dapat ditangani secara efektif melalui regulasi umum seperti UU ITE. Pengaturan pidana dalam UU PDP memberikan kejelasan mengenai perbuatan yang dilarang, subjek hukum yang dapat dimintai pertanggungjawaban, serta sanksi yang dapat dijatuhkan. Dengan demikian, praktik doxing yang sebelumnya hanya dapat ditafsirkan secara tidak langsung melalui UU ITE, kini memiliki dasar hukum yang lebih tegas dan spesifik dalam UU PDP.

Hubungan antara UU ITE dan UU PDP dalam mengatur tindak pidana doxing menunjukkan adanya evolusi kebijakan hukum pidana di Indonesia. UU ITE berperan sebagai instrumen awal yang mengatur perilaku di ruang digital secara umum, sedangkan UU PDP hadir sebagai regulasi khusus yang memberikan perlindungan substantif terhadap data pribadi. Dalam konteks ini, UU PDP berfungsi sebagai pelengkap sekaligus penyempurna terhadap kelemahan pengaturan sebelumnya, sehingga menciptakan sistem hukum yang lebih adaptif terhadap perkembangan teknologi informasi. Secara keseluruhan, sejarah pengaturan tindak pidana doxing dalam UU ITE dan UU PDP mencerminkan proses bertahap pembentukan hukum yang mengikuti kebutuhan sosial dan perkembangan teknologi. Dari pengaturan yang bersifat implisit dan terbatas dalam UU ITE hingga pengaturan yang eksplisit dan komprehensif dalam UU PDP,

terlihat adanya upaya negara untuk meningkatkan kepastian hukum dan perlindungan hak atas privasi.

Jenis data pribadi yang diatur dalam UU PDP dikelompokkan ke dalam dua kategori utama sebagaimana diatur dalam Pasal 4 Ayat (1), yaitu data pribadi yang bersifat spesifik dan data pribadi yang bersifat umum. Data pribadi yang bersifat spesifik mencakup informasi yang memiliki tingkat sensitivitas tinggi dan memerlukan perlindungan khusus, antara lain data dan informasi terkait kesehatan, data biometrik, data genetika, data yang berkaitan dengan tindak pidana atau kejahatan, data anak, data keuangan, serta jenis data lain yang ditetapkan sesuai dengan ketentuan Peraturan Perundang-Undangan. Sementara itu, data pribadi yang bersifat umum meliputi identitas dasar seseorang, seperti nama lengkap, jenis kelamin, kewarganegaraan, agama, status perkawinan, alamat surat elektronik, serta data pribadi lain yang apabila dikombinasikan dapat digunakan untuk mengidentifikasi individu tertentu.[26]

Merujuk pada keterangan penjelasan atas UU PDP Pembentukan Undang-Undang tentang Pelindungan Data Pribadi merupakan pelaksanaan dari amanat konstitusi sebagaimana tercantum dalam Pasal 28G ayat (1) Undang-Undang Dasar Negara Republik Indonesia Tahun 1945, yang menjamin hak setiap orang atas perlindungan diri pribadi, keluarga, kehormatan, martabat, serta rasa aman dari segala bentuk ancaman. Permasalahan perlindungan data pribadi muncul seiring meningkatnya kekhawatiran terhadap potensi pelanggaran data yang dapat dialami oleh orang perseorangan maupun badan hukum. Pelanggaran tersebut tidak hanya

[26] *Ibid,* Taufik Hidayat Telaumbanua, h. 7.

menimbulkan kerugian yang bersifat materiil, tetapi juga kerugian nonmateriil yang berdampak pada martabat dan kehidupan sosial korban.

Perumusan pengaturan mengenai perlindungan data pribadi dilandasi oleh kebutuhan untuk memberikan perlindungan hukum terhadap hak individu dalam masyarakat, khususnya dalam kaitannya dengan pemrosesan data pribadi yang dilakukan baik secara elektronik maupun nonelektronik. Pemrosesan data tersebut, apabila tidak diatur secara memadai, berpotensi disalahgunakan dan menimbulkan pelanggaran terhadap hak privasi. Oleh karena itu, perlindungan yang efektif atas data pribadi diharapkan dapat menumbuhkan kepercayaan masyarakat untuk memberikan data pribadinya guna kepentingan yang lebih luas, tanpa rasa khawatir akan penyalahgunaan atau pelanggaran hak pribadi.

Pengaturan perlindungan data pribadi juga dimaksudkan untuk menciptakan keseimbangan antara kepentingan individu dan kepentingan masyarakat yang diwakili oleh negara. Dengan adanya keseimbangan tersebut, pengelolaan data pribadi dapat dilakukan secara bertanggung jawab, transparan, dan akuntabel, sehingga mampu mendukung terciptanya ketertiban serta kemajuan dalam masyarakat informasi. Dalam rangka menghindari tumpang tindih pengaturan perlindungan data pribadi, Undang-Undang Pelindungan Data Pribadi ditetapkan sebagai standar perlindungan data pribadi yang bersifat umum, baik terhadap data yang diproses secara sebagian maupun keseluruhan, baik melalui sistem elektronik maupun nonelektronik. Setiap sektor selanjutnya dapat menerapkan perlindungan data pribadi sesuai dengan karakteristik dan kebutuhan sektoral masing-masing.

Lebih lanjut, pengaturan mengenai perlindungan data pribadi bertujuan untuk melindungi dan menjamin hak dasar warga negara atas perlindungan diri pribadi, sekaligus menjamin hak masyarakat dalam memperoleh pelayanan dari korporasi, badan publik, organisasi internasional, maupun pemerintah. Selain itu, pengaturan ini juga diarahkan untuk mendorong pertumbuhan ekonomi digital dan industri teknologi informasi dan komunikasi, serta meningkatkan daya saing industri nasional di tingkat global. Dalam kaitannya dengan tindak pidana doxing, keberadaan Undang-Undang Pelindungan Data Pribadi memberikan landasan hukum yang lebih kuat dan komprehensif dalam mencegah serta menindak perbuatan penyalahgunaan dan penyebarluasan data pribadi tanpa hak, sehingga memperkuat perlindungan hukum bagi subjek data di era digital.

Tindakan doxing dilakukan dengan tujuan untuk merugikan mempermalukan atau mengancam pihak lain. Doxing marak dilakukan seiring peningkatan penggunaan internet dan media sosial. Di Indonesia istilah doxing tidak disebut secara eksplisit dalam peraturan perundang-undangan. Namun substansi perbuatan doksin telah lama diatur sebagai bentuk pelanggaran privasi dan penyalahgunaan data pribadi. Doksin menjadi salah satu bentuk kejahatan siber *(cyber harassment)* yang semakin kompleks karena pelaku dapat dengan mudah mengakses, mengunduh dan membagikan data pribadi secara luas melalui internet maupun platform digital lain.

Kesadaran akan pentingnya perlindungan data pribadi semakin meningkat setelah jumlah kasus kebocoran data pribadi terjadi di Indonesia, seperti kebocoran NIK, data pelanggan aplikasi digital, dan data pengguna layanan kesehatan.

Kebocoran data tersebut menimbulkan keresahan publik, karena data tersebut dapat disalahgunakan untuk doxing, penipuan atau tindak pidana lainnya. Kondisi ini menegaskan bahwa UUD tidak cukup untuk melindungi masyarakat. Indonesia membutuhkan aturan hukum khusus agar mampu menghadapi perkembangan teknologi sekaligus melindungi warga dari penyalahgunaan data pribadi. Perkembangan teknologi informasi mengubah pola pemikiran mengenai batas wilayah, waktu, logika berpikir, pola kerja, dan batas perilaku sosial dari yang bersifat manual menjadi digital.

2.2 Perbedaan Konsepsi Tindak Pidana Doxing Dalam UU ITE dengan UU PDP

Perkembangan teknologi informasi yang berlangsung sangat cepat telah membawa perubahan signifikan dalam pola kehidupan masyarakat di berbagai bidang, termasuk cara berkomunikasi, berinteraksi, dan melakukan aktivitas sosial maupun ekonomi. Perubahan tersebut secara langsung memunculkan bentuk-bentuk perbuatan hukum baru yang sebelumnya belum dikenal dalam sistem hukum konvensional. Pemanfaatan teknologi informasi, di satu sisi memberikan kemudahan dan efisiensi dalam mobilitas kehidupan manusia, namun di sisi lain juga membuka peluang terjadinya penyalahgunaan teknologi yang berdampak pada pelanggaran hak individu. Oleh karena itu, pengembangan dan pengaturan teknologi informasi perlu diarahkan untuk melindungi kepentingan nasional, memperkuat integrasi sosial, serta menjamin kepastian hukum sesuai dengan sistem hukum yang berlaku di Indonesia.

Sebagai negara hukum, Indonesia merespons perkembangan tersebut dengan aturan yang dimuat dalam UU ITE. UU ITE dirancang sebagai instrumen hukum

untuk mengatur berbagai aktivitas yang berkaitan dengan penggunaan informasi dan transaksi elektronik, sekaligus sebagai dasar penyelesaian permasalahan hukum yang timbul di ruang digital. Dalam konteks tindak pidana doxing, UU ITE tidak mengatur secara eksplisit istilah doxing, namun menempatkan perbuatan tersebut sebagai bagian dari penyalahgunaan informasi elektronik, khususnya yang berkaitan dengan penggunaan data pribadi seseorang tanpa persetujuan yang sah sebagaimana diatur dalam Pasal 26 ayat (1) UU ITE. [27]

Dalam praktiknya, doxing didefinisikan sebagai tindakan mengungkapkan atau menyebarluaskan informasi data pribadi seseorang kepada publik melalui media internet tanpa persetujuan pemilik data, dengan tujuan untuk mempermalukan, mengintimidasi, mengancam, atau memberikan tekanan sosial terhadap individu tertentu. Perbuatan ini sering kali dilakukan melalui media sosial dan platform digital lainnya yang memiliki daya sebar luas dan cepat. Konsepsi doxing dalam UU ITE menitikberatkan pada aspek perbuatan di ruang siber dan dampak sosial yang ditimbulkan, seperti penyebaran kebencian, fitnah, dan serangan terhadap kehormatan seseorang, sehingga penegakan hukumnya kerap dikaitkan dengan pasal-pasal lain dalam UU ITE maupun ketentuan pidana umum.

Informasi data pribadi sangat rentan terjadinya penyalahgunaan data jika tidak dilakukan dengan prinsip penghormatan hak individual masyarakat. Pesatnya perkembangan teknologi informasi menyebabkan isu mengenai perlindungan data menjadi hal yang serius karena penyebarannya dapat dilakukan dengan mudah dan

---

[27] Intan Saripa Uweng, dkk, *Perlindungan Hukum Pidana Terhadap Doxing Menurut Undang-Undang Informasi Dan Transaksi Elektronik*, Pattimura Law Study Review, Volume 1 Nomor 1 Agustus 2023, h. 169-170.

cepat sehingga mengakibatkan kebocoran pada pengelolaan data dan informasi pada pengelolaan data pribadi semakin tinggi. Berbagai kejahatan siber yang dapat terjadi seperti kejahatan tradisional meliputi penipuan atau pencurian data di ruang siber hingga serangan siber yang menyerang infrastruktur penting yang mengancam keamanan nacional suatu negara.

Dua regulasi yang paling relevan mengatur tindak pidana doxing adalah UU ITE dan UU PDP, kedua Undang-Undang tersebut memiliki pendekatan konseptual yang berbeda dalam merumuskan perbuatan pidananya. UU ITE memposisikan doxing sebagai bagian dari kejahatan penyalahgunaan informasi elektronik dan data pribadi dalam ruang digital. Sementara itu, UU PDP menempatkan doxing dalam kerangka perlindungan hak subjek data dari tindakan pengumpulan dan pemrosesan data secara melawan hukum. Perbedaan pendekatan ini menunjukkan adanya perbedaan ratio legis dalam pembentukan masing-masing Undang-Undang. Oleh karena itu, analisis perbedaan konsep tindak pidana doxing dalam UU ITE dan UU PDP menjadi penting untuk memahami batasan dan akibat hukumnya. Pemahaman ini juga diperlukan untuk mencegah tumpang tindih penegakan hukum dalam proses peradilan.

Sebelum lahirnya UU PDP, pengaturan mengenai perlindungan data dan privasi di Indonesia tersebar dalam berbagai Peraturan Perundang-Undangan yang bersifat sektoral. Salah satu regulasi penting adalah Peraturan Menteri Komunikasi dan Informatika Nomor 20 Tahun 2016 tentang Perlindungan Data Pribadi dalam Sistem Elektronik. Peraturan tersebut menegaskan bahwa pemrosesan data pribadi hanya dapat dilakukan atas dasar persetujuan pemilik data, baik secara tertulis,

manual, maupun elektronik, setelah pemilik data memperoleh penjelasan yang lengkap mengenai tindakan perolehan, pengumpulan, pengolahan, penyimpanan, penampilan, pengumuman, pengiriman, serta penyebarluasan data pribadi, termasuk jaminan kerahasiaannya. Ketentuan ini menunjukkan bahwa sejak awal perlindungan data pribadi dalam rezim UU ITE masih berorientasi pada persetujuan sebagai elemen utama perlindungan hukum.

Lebih lanjut, perlindungan atas privasi sebagai landasan konsepsi doxing juga memiliki dasar konstitusional dalam Pasal 28G Ayat (1) UUD 1945, yang menjamin hak setiap orang atas perlindungan diri pribadi, kehormatan, martabat, serta rasa aman dari ancaman lalu ketentuan ini diperkuat oleh Undang-Undang Nomor 14 Tahun 2008 tentang Keterbukaan Informasi Publik yang secara tegas mengecualikan informasi pribadi tertentu dari kategori informasi yang dapat diakses publik, seperti data keluarga, kondisi kesehatan, keuangan, evaluasi kapasitas intelektual, serta catatan pendidikan. Hal ini menunjukkan bahwa secara normatif, hukum Indonesia telah lama mengakui data pribadi sebagai informasi yang bersifat rahasia dan wajib dilindungi.[28]

Konsep doxing dalam konteks hukum cyber dipahami sebagai tindakan mengumpulkan, mengungkapkan, dan menyebarluaskan data atau informasi pribadi seseorang melalui media elektronik tanpa persetujuan yang sah, yang mengakibatkan kerugian atau ancaman terhadap korban. Tindakan doxing berbeda

[28] Cindi Novita Putri, *Kajian Kriminologi Kejahatan Penyebaran Data Pribadi (Doxing) Melalui Media Sosial,* Skripsi, Fakultas Hukum Universitas Lampung Bandar Lampung, 2023, h. 4-5.

dengan penyebaran informasi biasa, Doxing memiliki unsur kesengajaan dan motif tertentu yang menjadikan perbuatan ini masuk dalam kategori *cybercrime.*

Suatu tindakan dikategorikan sebagai tindakan doxing apabila memenuhi tiga unsur, yaitu:

a. adanya data pribadi sebagai objek yang dilindungi;
b. adanya perbuatan mengakses, memperoleh, atau menyebarkan data; dan
c. tidak adanya persetujuan dari pemilik data atau tindakan dilakukan secara melawan hukum.

Unsur-unsur inilah yang menjadi pembeda antara doxing dengan penyebaran informasi secara publik biasa. Tindakan doxing memiliki dampak hukum maupun sosial. Doxing dapat mengakibatkan pelanggaran hak privasi yang dapat menimbulkan pertanggungjawaban pidana maupun perdata.

Pengaturan tindak pidana doxing yang diatur dalam UU ITE lebih menitikberatkan pada aspek distribusi, transmisi, atau akses terhadap informasi elektronik yang bermuatan data pribadi. Perbuatan pidana dalam konteks ini terjadi ketika seseorang dengan sengaja dan tanpa hak menyebarluaskan data pribadi orang lain melalui sistem elektronik. Fokus utama UU ITE adalah pada penggunaan media elektronik sebagai sarana terjadinya tindak pidana. Unsur utama yang ditekankan adalah adanya perbuatan tanpa haka tau tanpa izin serta adanya dampak terhadap kehormatan, privasi, atau keamanan subjek data. Doxing dalam UU ITE dipahami sebagai bentuk pelanggaran terhadap hak privasi yang dilakukan melalui ruang siber. Akibat hukum dari perbuatan tersebut lebih diarahkan pada perlindungan ketertiban dan keamanan dalam penggunaan teknologi informasi. Oleh karena itu, UU ITE memandang doxing sebagai kejahatan berbasis sarana elektronik, bukan hanya kejahatan terhadap data pribadi.

Konsep doxing atau penyebaran data pribadi seseorang pada media elektronik awalnya diatur dalam pasal 26 Ayat (1) UU ITE yang berbunyi kecuali ditentukan lain oleh Peraturan Perundang-Undangan, penggunaan setiap informasi melalui media elektronik yang menyangkut data pribadi seseorang harus dilakukan dengan persetujuan orang yang bersangkutan. Persetujuan dalam penggunaan data pribadi seseorang sangat penting dan diperlukan pada UU ITE. Dalam pemanfaatan Teknologi Informasi, perlindungan data pribadi merupakan salah satu bagian dari hak pribadi *(privacy right)*. Hal pribadi mengandung pengertian, bahwa:

1. Hak pribadi merupakan hak untuk menikmati kehidupan pribadi dan bebas dari segala macam gangguan;
2. Hak pribadi merupakan hak untuk dapat berkomunikasi dengan orang lain tanpa tindakan memata-matai; dan
3. Hak pribadi merupakan hak untuk mengawasi akses informasi tentang kehidupan pribadi dan data seseorang.

Karakteristik lain dari konsep doxing dalam UU ITE adalah adanya penekanan pada aspek penyalahgunaan informasi yang telah ada atau telah diperoleh sebelumnya. UU ITE tidak secara rinci mengatur proses awal perolehan data pribadi, melainkan lebih fokus pada tindakan penggunaan dan penyebarannya. Hal ini menyebabkan doxing dalam UU ITE sering dikaitkan dengan perbuatan menyebarkan data pribadi di media sosial, forum daring, atau platform digital lainnya. pelaku doxing dianggap melakukan pelanggaran hukum karena memanfaatkan data pribadi tanpa persetujuan pemiliknya. Unsur kesengajaan menjadi unsur penting dalam pembuktian tindak pidana tersebut.

Selain itu, UU ITE juga mensyaratkan adanya kerugian atau potensi kerugian yang ditimbulkan terhadap korban. Dengan demikian, pendekatan UU ITE terhadap doxing bersifat represif terhadap dampak yang ditimbulkan. Konsep ini

menunjukkan bahwa UU ITE lebih berorientasi pada akibat perbuatan dibandingkan proses pengelolaan data. Namun di dalam UU ITE penggunaan data pribadi seseorang memungkinkan untuk dilakukan apabila mendapat persetujuan orang yang bersangkutan. UU ITE menyebut data pribadi dengan data elektronik dan dokumen elektronik. Pada Pasal 1 Ayat 1 menjelaskan bahwa informasi elektronik adalah sekumpulan data elektronik yang telah diolah dan memiliki arti atau dapat dipahami. Pada pasal 26 ayat 1 UU ITE menjelaskan tentang keharusan adanya persetujuan penggunaan informasi data pribadi seseorang pada media elektronik.

Dalam UU PDP, doxing dapat diartikan sebagai bagian dari tindakan pengumpulan, penggunaan, pemrosesan, dan penyebaran data pribadi yang dilakukan secara melawan hukum. UU PDP tidak hanya mempermasalahkan tujuan perbuatan hukum berupa penyebaran data, tetapi juga focus pada proses sejak data tersebut dikumpulkan. Dengan demikian, pelanggaran hukum dapat terjadi meskipun data tersebut belum disebarluaskan kepada publik. UU PDP menempatkan hak subjek data sebagai pusat perlindungan hukum. Setiap tindakan pengumpulan dan penggunaan data harus didasarkan pada persetujuan yang sah dari pemilik data. Tanpa adanya dasar hukum yang sah, perbuatan tersebut telah memenuhi unsur tindak pidana. Hal ini menunjukkan bahwa UU PDP memiliki pendekatan preventif dalam melindungi data pribadi.

Terkait penyalahgunaan data pribadi seseorang di Indonesia diatur melalui uu PDP. Dalam UU PDP yang dimaksud dengan data pribadi adalah data tentang orang perseorangan yang teridentifikasi atau dapat diidentifikasi secara tersendiri atau

dikombinasi dengan informasi lainnya baik secara langsung maupun tidak langsung melalui sistem elektronik atau non elektronik. Selain itu, UU PDP data pribadi dibagi menjadi dua yaitu, data pribadi yang bersifat spesifik, dan data pribadi yang bersifat umum.

Larangan penggunaan data pribadi seseorang tanpa izin orang yang bersangkutan atau tindakan doxing dalam UU PDP diatur dalam Pasal 65 Ayat (1) sampai dengan ayat (3) yang menyatakan bahwa setiap orang dilarang secara melawan hukum memperoleh dan mengumpulkan data pribadi, mengungkapkan data pribadi yang bukan miliknya, dan menggunakan data pribadi yang bukan miliknya dengan tujuan menguntungkan diri sendiri atau orang lain yang dapat mengakibatkan kerugian subjek data pribadi.

Dalam UU PDP tindakan sebagaimana yang tercantum dalam Pasal 65 Ayat (1) sampai (3) perbuatan yang dilakukan harus memenuhi unsur melawan hukum. Sedangkan dalam UU ITE penggunaan data pribadi harus mendapatkan persetujuan pemilik data pribadi tersebut. Ketika data pribadi dikumpulkan atau digunakan di luar tujuan yang telah disepakati, maka perbuatan tersebut dianggap melawan hukum. Dalam hal ini, doxing tidak semata-mata dipahami sebagai penyebaran data ke publik, tetapi juga sebagai penyalahgunaan data dalam bentuk apa pun. UU PDP mengkriminalisasi perbuatan pengolahan data yang tidak sah, terlepas dari media yang digunakan. Dengan demikian, tindak pidana doxing dalam UU PDP tidak selalu bergantung pada penggunaan sistem elektronik. Hal ini memperluas cakupan perlindungan hukum terhadap subjek data. Pendekatan tersebut menunjukkan bahwa UU PDP lebih menekankan perlindungan substantif terhadap data pribadi.

Dari sudut pandang pendekatan pengaturan, objek perlindungan, serta konstruksi deliknya. Dalam UU ITE, doxing diposisikan sebagai bagian dari kejahatan siber yang berfokus pada perbuatan melawan hukum dalam pemanfaatan sistem dan media elektronik. Pendekatan ini menitikberatkan pada cara dan sarana perbuatan, yakni distribusi, transmisi, akses ilegal, atau pengalihan informasi elektronik tanpa hak, termasuk informasi yang bersifat rahasia atau data pribadi. Oleh karena itu, pelaku doxing dapat dijerat melalui berbagai ketentuan UU ITE yang mengatur perbuatan mentransfer, menyebarkan, atau membuat dapat diaksesnya informasi elektronik yang dilindungi, serta ketentuan mengenai akses ilegal, penerobosan, atau pelampauan sistem pengamanan elektronik milik orang lain. Karakter delik dalam UU ITE menekankan aspek teknis perbuatan yang dilakukan di ruang siber, sehingga unsur utama yang diuji adalah adanya kesengajaan, tanpa hak, dan penggunaan sarana elektronik sebagai media utama terjadinya pelanggaran.

Berbeda dengan itu, UU PDP menghadirkan konsepsi yang lebih substansial dan berorientasi pada perlindungan hak atas data pribadi sebagai hak fundamental setiap orang. Dalam kerangka UU PDP, doxing dipahami sebagai bagian dari pelanggaran terhadap prinsip pelindungan data pribadi, khususnya perbuatan mengumpulkan, mengungkapkan, menggunakan, atau memalsukan data pribadi tanpa dasar hukum yang sah. Pendekatan UU PDP tidak semata-mata bertumpu pada penggunaan media elektronik, melainkan mencakup pula perbuatan yang dilakukan secara non-elektronik, sepanjang berkaitan dengan data pribadi orang perseorangan yang teridentifikasi atau dapat diidentifikasi. Dengan demikian, fokus

utama UU PDP terletak pada substansi pelanggaran hak subjek data dan dampak kerugian yang ditimbulkan, baik secara materiel maupun immateriel, akibat penyalahgunaan data pribadi tersebut.

Perbedaan konsepsi ini tercermin pula dalam pengaturan sanksi pidana. UU ITE mengaitkan ancaman pidana dengan jenis perbuatan siber tertentu, seperti distribusi tanpa hak, akses ilegal, atau perusakan dan pengalihan data elektronik, dengan variasi ancaman pidana penjara dan denda yang disesuaikan dengan tingkat keseriusan perbuatan. Sementara itu, UU PDP secara lebih tegas merumuskan sanksi pidana terhadap pelaku yang secara sengaja melanggar kewajiban pelindungan data pribadi, termasuk pengungkapan dan penggunaan data pribadi bukan miliknya, serta pemalsuan data pribadi untuk keuntungan diri sendiri atau orang lain yang menimbulkan kerugian. Ancaman pidana dalam UU PDP menunjukkan orientasi perlindungan yang lebih kuat terhadap kepentingan korban sebagai subjek data, dengan penekanan pada pemulihan hak dan pencegahan penyalahgunaan data di masa mendatang.[29]

Konsep tindak pidana doxing dalam UU ITE dan UU PDP memiliki perbedaan yang mendasar. UU ITE memandang doxing sebagai penyalahgunaan dan penyebaran data pribadi tanpa izin melalui media elektronik. Fokus peraturan pada perbuatan hukum dan akibat yang ditimbulkan dalam ruang siber. Sementara itu, UU PDP memandang doxing sebagai bagian dari tindakan pengumpulan dan penggunaan data pribadi yang melawan hukum. UU PDP lebih menekankan perlindungan terhadap hak subjek data sejak tahap awal pengelolaan data.

[29] Landasan Hukum Pidana Bagi Pelaku Doxing, diakses pada Tanggal 13 Januari 2026.

Perbedaan ini mencerminkan perbedaan tujuan pembentukan Undang-Undang. UU ITE berorientasi pada pengaturan aktivitas elektronik, sedangkan UU PDP berorientasi pada perlindungan hak asasi atas data pribadi.

2.3 Perbedaan Penerapan Tindak Pidana Doxing dalam UU ITE dengan UU PDP

Dalam perkembangan teknologi informasi dan komunikasi telah membawa perubahan mendasar dalam cara manusia berinteraksi, berkomunikasi, dan mengelola informasi dalam kehidupan sehari-hari. Di satu sisi, kemajuan ini memberikan kemudahan dan efisiensi dalam berbagai aktivitas sosial, ekonomi, dan budaya, namun di sisi lain juga melahirkan bentuk-bentuk pelanggaran hukum baru yang sebelumnya tidak dikenal dalam sistem hukum konvensional. Salah satu fenomena yang muncul sebagai konsekuensi dari pemanfaatan teknologi digital adalah doxing, yaitu tindakan pengungkapan dan penyebarluasan data pribadi seseorang kepada publik tanpa persetujuan yang sah.

Dalam praktiknya kerap dilakukan melalui media digital dengan tujuan tertentu, seperti mempermalukan, mengintimidasi, mengancam, atau memberikan tekanan sosial terhadap individu yang menjadi sasaran. Oleh karena itu, doxing tidak hanya menimbulkan kerugian secara materiil, tetapi juga berdampak serius terhadap hak atas privasi, rasa aman, dan martabat manusia yang dilindungi dalam prinsip-prinsip hak asasi manusia. Dalam konteks tersebut, negara memiliki kewajiban untuk menghadirkan instrumen hukum yang mampu memberikan perlindungan efektif terhadap warga negara dari penyalahgunaan teknologi informasi. Pengaturan mengenai tindak pidana doxing menjadi bagian dari upaya hukum untuk menyeimbangkan antara kebebasan berekspresi dan perlindungan hak

atas privasi di ruang digital. Perbedaan pendekatan pengaturan dan penerapan hukum terhadap doxing dalam berbagai rezim hukum mencerminkan perkembangan kebijakan legislasi yang menyesuaikan diri dengan kompleksitas kejahatan berbasis teknologi.

Dalam penerapan tindak pidana doxing dalam sistem hukum Indonesia terdapat perbedaan yang mendasar antara UU ITE dan UU PDP, kedua Undang-Undang tersebut merupakan dasar hukum dalam menangani pelanggaran terhadap data pribadi. UU ITE dibentuk untuk mengatur aktivitas dan kejahatan di ruang siber, sehingga penerapan tindak pidana doxing lebih difokuskan pada penyalahgunaan data pribadi melalui sistem elektronik. Sedangkan, UU PDP dibentuk khusus untuk melindungi data pribadi sebagai hak privasi subjek data. Perbedaan tujuan pembentukan tersebut berdampak langsung pada penerapan tindak pidana doxing. Perbedaan ini juga memengaruhi mekanisme pertanggungjawaban pidana dan pemulihan hak korban. Oleh karena itu, pembahasan mengenai perbedaan penerapan tindak pidana doxing dalam kedua undang-undang ini menjadi relevan untuk memberikan kepastian hukum. Penyalahgunaan data pribadi berkaitan dengan kejahatan di dunia siber lainnya seperti penipuan, pemalsuan dokumen, hingga terorisme. Kejahatan siber dapat dikelompokkan menjadi beberapa bentuk yaitu:[30]

1. *Illegal content*, kejahatan ini dilakukan dengan memasukkan data atau informasi ke internet tentang sesuatu yang tidak benar, tidak etis, dan dapat dianggap melanggar hukum atau mengganggu ketertiban umum.

[30] Jenis Kejahatan Siber yang Diakui dalam Hukum Indonesia: Regulasi dan Situasinya, diakses pada Tanggal 16 Januari 2026.

2. *Data Forgery*, kejahatan yang dilakukan dengan memalsukan data pada dokumen dokumen penting yang tersimpan melalui internet
3. *Infringement of privacy*, kejahatan yang ditujukan terhadap informasi seseorang yang merupakan hal sangat pribadi dan rahasia.

Perlindungan data pribadi kerap dikaitkan dengan perlindungan terhadap hak privasi. Dalam penjelasan UU ITE hak privasi mencakup hak untuk mengawasi akses informasi tentang kehidupan seseorang dan data seseorang. Subyek data pada dasarnya memiliki kontrol penuh atas informasi tentang dirinya. Dalam penerapan tindak pidana doxing dalam UU ITE berkaitan erat dengan kedudukan korban sebagai pihak yang dirugikan. UU ITE memberikan ruang bagi korban penyalahgunaan data pribadi untuk mengajukan gugatan ganti rugi. Mekanisme ganti rugi tersebut ditempatkan dalam ranah hukum perdata dan diajukan secara terpisah oleh korban.

Dengan demikian, pemulihan hak korban dalam UU ITE sangat bergantung pada inisiatif korban. Aparat penegak hukum dalam perkara pidana hanya berfokus pada pembuktian tindakan hukum pelaku. sehingga, kepentingan pemulihan kerugian korban tidak secara otomatis terakomodasi dalam putusan pidana. Hal ini memisahkan pertanggungjawaban pidana dan perdata dalam UU ITE. kondisi ini menyulitkan korban karena harus menempuh dua proses hukum sekaligus. Oleh karena itu, penerapan UU ITE dinilai kurang memberikan perlindungan hukum yang maksimal terhadap korban doxing.

Perlindungan privasi merupakan hak setiap warga negara yang harus dihormati dan diberikan perlindunhan. Sebagaimana tercantum dalam pasal 28G ayat (1) UUD NRI 1945 yang berbunyi “setiap orang berhak atas perlindungan diri pribadi, keluarga, kehormatan, martabat, dan harta benda yang di bawah

kekuasaannya, serta berhak atas rasa aman dan perlindungan dari ancaman ketakutan untuk berbuat atau tidak berbuat sesuatu yang merupakan hak asasi".

Dalam UU ITE Penggunaan setiap informasi melalui media atau sistem elektronik yang menyangkut data pribadi seseorang harus dilakukan dengan orang yang bersangkutan. Sehingga dibutuhkan jaminan pemenuhan perlindungan diri pribadi dengan mewajibkan setiap penyelenggara sistem elektronik untuk menghapus informasi elektronik yang berada di bawah kendali penyelenggara sistem elektronik tersebut. Ketentuan pidana tindak pidana penyalahgunaan data pribadi. Dalam UU ITE, tindak pidana penyalahgunaan data pribadi dikaitkan dengan maksud dan tujuan dari penyalahgunaan data pribadi. apabila pelaku menggunakan data pribadi seseorang dengan tujuan pemerasan atau ancaman maka dapat dikenakan pasal 45 Ayat (4) Undang - Undang Nomor 19 Tahun 2016. Selain itu berdasarkan ketentuan pasal 26 Ayat (2) UU Nomor 19 Tahun 2016, korban tindak pidana doxing dapat mengajukan gugatan atas kerugian yang ditimbulkan.

Dalam UU PDP larangan penggunaan data pribadi sebagaimana yang diatur dalam Pasal 65 Ayat (1) sampai dengan Ayat (3) dan Pasal 66 dimana setiap orang dilarang secara melawan hukum memperoleh atau mengumpulkan data pribadi, mengungkapkan, menggunakan data pribadi yang bukan miliknya, dan membuat data pribadi palsu dengan tujuan menguntungkan diri sendiri atau orang lain. Ketentuan pidana terkait tindak pidana sebagaimana dimaksud dalam Pasal 65 dan Pasal 66 diatur dalam pasal 67 hingga Pasal 73 apabila tindak pidana tersebut dilakukan oleh korporasi maka hukuman pidana diberikan kepada pengurus, pemegang kendali, pemberi perintah, pemilik manfaat korporasi. selain itu pelaku

tindak pidana doxing dapat dijatuhi pidana tambahan berupa pembayaran ganti kerugian.

Salah satu perbedaan penting dalam penerapan tindak pidana doxing antara UU ITE dan UU PDP terletak pada pengaturan mengenai ganti kerugian. Dalam UU PDP, pembayaran ganti kerugian kepada korban dapat dijatuhkan sebagai pidana tambahan. Artinya, pemulihan kerugian korban menjadi bagian dari putusan pidana. Berbeda dengan UU ITE, korban tindak pidana doxing dalam UU PDP tidak perlu mengajukan gugatan perdata secara terpisah untuk memperoleh ganti rugi.

Penerapan sanksi ini menunjukkan adanya kemanfaatan hukum antara pemidanaan pelaku dan perlindungan hak korban. Dengan demikian, UU PDP memberikan posisi yang lebih kuat kepada korban dalam proses peradilan pidana. Pendekatan ini mencerminkan perlindungan terhadap korban. Negara secara aktif menjamin pemulihan hak korban melalui instrumen pidana. Hal ini menjadi kelebihan utama UU PDP dibandingkan UU ITE dalam penerapan hukum terhadap tindak pidana doxing.