BAB II

KAJIAN PUSTAKA

A. Tinjauan Umum tentang Doxing

1. Pengertian Doxing

Penjelasan secara universal doxing merupakan kegiatan dalam mengumpulkan dan menyebarkan informasi atau data pribadi lewat daring. Dikutip dari kamus *Oxford British and World English Dictionary SAFEnet* menerangkan bahwa doxing sebagai "mencari dan mempublikasikan informasi pribadi atau identitas tentang individu tertentu di internet, dan tindakan itu biasanya didorong dengan niat jahat".[9]

Dalam penjelasan kamus Cambridge Dictionary menerangkan juga bahwa doxing merupakan perbuatan untuk mendapatkan dan menyiarkan informasi yang bersifat pribadi mengenai seseorang tanpa adanya hak secara norma maupun hukum, perbuatan ini dilakukan dengan cara yang mengungkapkan nama, alamat, dan berbagai identitas pribadi.[10]

Perbuatan doxing ini bukan hanya melanggar hak privat korban. Namun juga menimbulkan fasilitas pelecehan terhadap korban di dunia maya dan tidak menutup kemungkinan munculnya intimidasi dan kekerasan secara nyata disebabkan identitas pribadi dan tempat kediaman korban yang telah terpublikasi.[11]

---

[9] Banimal, Abu Hasan., Juniarto, Damar., Ningtyas, Ika. *Peningkatan serangan doxing dan tantangan perlindungannya di Indonesia,* SAFEnet, Jakarta, 2020.
[10] https://dictionary.cambridge.org/dictionary/english/doxing, diakses pada tanggal 1 November 2025.
[11] Willard, N.E. (2007). *Cyberbullying and Cyberthreats: Responding to the Challenge of Online Social Aggression, Threats, and Distress*, Research Press: Champaign, IL, USA.

Doxing menghubungkan cyberbullying dengan pelecehan di kehidupan nyata. Doxing di dunia maya meningkatkan resiko kekerasan fisik, terutama jika informasi pribadi seperti alamat rumah atau alamat kantor dipublikasikan dan digunakan untuk mendorong orang lain mengambil tindakan aktif terhadap para korban. Doxing juga menunjukkan power antara pelaku dan korban, karena pelaku seringkali anonim, sedangkan korban lebih terlihat dan dapat diakses publik, baik di dunia maya maupun dunia nyata.[12]

Definisi doxing menurut para ahli:

a. Roney Matthews, Doxing adalah publikasi informasi pribadi untuk konsumsi publik (tanpa persetujuan) untuk tujuan menyebabkan rasa malu dan penghinaan di Internet, yang dilakukan dengan cara membahayakan privasi korban dan juga orang yang dicintai korban. (teman, anggota keluarga, dan lain-lain).[13]
b. Peter Synder, Doxing adalah serangan di mana informasi pribadi korban diungkapkan kepada publik melalui media online. Peter menyebut serangan doxing ini merupakan bentuk pelecehan online.[14]

[12] Mengtong Chen., Anne Shann Yue Cheung., Ko Ling Chan. (2019). *Doxing: What adolescents look for and their intentions*, International Journal of Environment Research and Public Health, 16, 218: 1-14
[13] Roney Matthews, *A Study of Doxing, its Security Implications and Mitigation Strategies for Organizations,* Information Systems Security, 2007.
[14] Peter Snyder, Periwinkle Doerfler, Chris Kanich, and Damon McCoy. *Fifteen Minutes of Unwanted Fame: Detecting and Characterizing Doxing.* In Proceedings of IMC '17.ACM, 2017

c. David M. Douglas, Menurut karya tulis yang dikutip dari David Douglas menerangkan bahwa doxing dipakai oleh pihak lain sebagai alat "penguntit dunia maya", dengan maksud dan tujuan mengekstraksi informasi, data informasi yang terkumpul tersebut dapat didistribusikan kembali dalam konteks dengan berbagai media maupun formatnya, hal demikian menimbulkan korban yang berakal sehat mengkhawatirkan nyawa mereka.8

Istilah “doxing” berasal dari ungkapan “menjatuhkan dokumen” atau “menjatuhkan dox” terhadap seseorang yang merupakan bentuk balas dendam pada tahun 1990-an. Doxing mulai dikenal pada tahun 1990, dilakukan oleh para peretas yang memiliki sifat keberadaan anonim dengan tujuan menyebarkan informasi mengenai korban. Seiring perkembangan teknologi menyebabkan perbuatan doxing menjadi suatu hal yang mudah untuk dilakukan berkat teknologi digital yang bekembang pesat. Pihak yang melakukan doxing tersebut menyebarkan informasi mengenai korbannya kepada khalayak umum untuk diketahui melalui internet maupun media sosial.

Umumnya, Tindakan doxing timbul dikarenakan ada tindakan yang tidak selaras dengan pelaku doxing yang menyebabkan korban yang tidak disukai pelaku melakukan aksi balas dendam dengan perbuatan doxing. Diantara perbuatan doxing terdapat salah satu yang sering menjadi motif perbuatan tersebut yaitu, keinginan untuk mengungkap kesalahan seseorang dan meminta pertanggungjawabannya. Di Indonesia, regulasi kejahatan dunia maya terkait doxing tertuang dalam UndangUndang ITE,

yang mengatur kegiatan yang dilarang dan sanksinya. Doxing juga diatur dalam Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi.

Kejahatan yang disebabkan oleh kemudahan seseorang mengakses internet sering disebut sebagai penjahat dunia maya/cybercrime. Istilah cybercrime mengacu pada aktivitas kriminal yang menggunakan komputer atau internet sebagai alat untuk melakukan tindakan kriminal. Contoh kejahatan yang termasuk dalam cybercrime antara lain adalah cyberstalking, cyberbullying, dan doxing. Doxing adalah bentuk cyberbullying dan cyberstalking dimana informasi pribadi orang dicari dan dibagikan, sehingga melanggar privasi mereka dan mengarah ke pelecehan lebih lanjut. Komnas HAM menyebutkan bahwa doxing merupakan salah satu bentuk pelanggaran HAM di bidang digital, hal ini disebabkan doxing dapat menyebabkan pelecehan baik secara online maupun offline Perbuatan doxing yang dilakukan oleh seseorang tentu dengan maksud dan tujuan tertentu. Dalam permasalahan yang sudah sering terjadi, doxing dilakukan untuk menakuti maupun mengintimidasi korban. Seperti misalnya, oknum debt collector melakukan hal tersebut dengan sengaja untuk mempermalukan nasabahnya di depan umum dan menimbulkan efek jera bagi nasabah tersebut agar segera melunasi hutangnya. Hal tersebut tentunya dapat dilakukan dengan sangat mudah karena didukung oleh teknologi terkini dan juga karena mudahnya seseorang mengakses internet sehingga dapat dengan mudah mencari, mengumpulkan dan menyebarkan informasi pribadi. Doxing juga biasa digunakan untuk mengungkapkan

kemarahan seseorang untuk berbagai keperluan dan untuk mengatasi situasi yang ada.

Menurut interpretasi David Doughlas menerangkan bahwa doxing dilakukan dengan pemerasan, fitnah, dan gosip. Ia menyebutkan bahwa tindakan doxing tidak dilakukan untuk memperoleh imbalan, tetapi biasanya dilakukan karena alasan tertentu seperti bosan, cemburu, rasa ingin mengancam, protes atau tindakan untuk mengungkapkan kesalahan yang dilakukan. Doxing merupakan kejahatan yang umum terjadi di Indonesia. namun banyak masyarakat awam yang tidak menyadari bahwa dirinya sendiri telah menjadi pelaku atau korban doxing. Setiap tahun jumlah korban kejahatan doxing ini bertambah.

Kasus doxing tidak lepas dari konsep keamanan dan perizinan. Privasi adalah sesuatu yang sangat sakral bagi individu, kelompok, dan organisasi. Namun, jika informasi pribadi yang tidak ingin dibagikan oleh seseorang dan diketahui publik, tetapi telah diungkapkan dan diketahui khalayak luas, maka kejadian ini akan menjadi sangat serius dan dapat membahayakan posisi dan kredibilitas yang bersangkutan. Privasi atau tidak adalah masalah perdebatan untuk menentukan apakah privasi perlu diterapkan di internet atau tidak. Di satu sisi, privasi adalah hak asasi manusia, di lain sisi fasilitas untuk ini sering disalahgunakan dengan tujuan iseng atau balas dendam misalnya posting anonim dengan pesan yang disertai flame. Hal-hal yang dicari *doxers*, biasanya berupa hal-hal berikut :

1) Nama asli
2) Nomor telepon

3) Alamat
4) Nomor kartu kredit
5) Nomor rekening
6) Foto pribadi
7) Profil media social

Douglas membagi *doxing* menjadi tiga jenis, yakni membuka identitas anonim *(deanonymization),* menjadikan target *(targeting),* dan mendelegitimasi *(delegitimization)*. Segala jenis doxing pada dasarnya adalah tindakan mencoba menghapus atau menghancurkan sesuatu milik korban. Seperti anonimitas, ketidakjelasan, dan kredibilitas korban. Setiap jenis doxing juga menciptakan peluang baru untuk lebih mengganggu kehidupan orang-orang yang menjadi sasarannya.

2. Jenis-jenis Doxing

David M. Douglas berpendapat bahwa jenis-jenis dari doxing menjadi tiga jenis, yakni:

1. Membuka Identitas *Anonym (Deanonymization)*

   Tindakan doxing yang mempublikasikan informasi berupa identitas pribadi milik seseorang dan/atau sekelompok orang yang identitasnya tidak diketahui (anonim) oleh publik atau dikenal dengan memiliki nama samaran. *Deanonymizing* sangat memengaruhi kerahasiaan identitas seseorang dan dapat mengintimidasi bagi seseorang dan/atau sekelompok orang yang memang tidak ingin diketahui identitasnya oleh publik sebagai

bentuk kebebasan berekspresi. [15] tindakan mengumpulkan, mengungkapkan, dan menyebarkan informasi pribadi seseorang atau sekelompok orang tanpa izin, biasanya melalui media digital. Informasi yang dipublikasikan dapat berupa nama asli, alamat, nomor telepon, akun media sosial, hingga data sensitif lain yang sebelumnya tidak diketahui publik.

Ketika identitas seseorang yang semula anonim atau menggunakan nama samaran dibuka secara paksa, proses ini dikenal sebagai *deanonymizing.* Tindakan tersebut memiliki dampak serius terhadap kerahasiaan identitas dan kebebasan berekspresi.

Deanonymization adalah kategori paling luas dari tiga kategori doxing karena dapat memengaruhi setiap jenis pengetahuan identitas dan meniadakan setiap alasan untuk menjaga anonimitas. Bergantung pada alasan subjek menjaga anonimitas dan jenis informasi identitas yang diungkapkan, tindakan ini mungkin tidak menyebabkan kerugian signifikan, dan mungkin saja ada alasan kepentingan publik yang masuk akal untuk mengungkapkannya. Misalnya, ada setidaknya alasan kepentingan publik *prima facie* untuk mengungkap identitas seseorang ketika anonimitas atau pseudonim digunakan untuk menipu orang lain demi keuntungan pribadi (misalnya penipu yang menyamar

[15] Jeane Neltje Saly and Lubna Tabriz Sulthanah. 2023. *Pelindungan Data Pribadi Dalam Tindakan Doxing Berdasarkan Undang-Undang Nomor 27 Tahun 2022*. Jakarta. Jurnal Kewarganegaraan. Vol.7 No. 2. Universitas Tarumanegara. Hal.1711.

sebagai orang lain untuk mendapatkan uang atau prestise). Penipuan sastra adalah salah satu contoh yang akan saya bahas lagi ketika membahas potensi justifikasi untuk *doxing*.

Unsur utama dari *deanonymizing* yaitu, Pertama Objeknya ialah Individu/Kelompok yang memilih anonimitas atau pseudonimitas untuk perlindungan, kenyamanan, atau alasan profesional/psikososial. Kedua, Perbuatan yang dilakukan yaitu Pengumpulan, verifikasi, dan publikasi informasi pengenal (nama asli, foto wajah, afiliasi, alamat surel yang dapat dihubungkan ke identitas, dsb). Ketiga, Niat atau tujuan dari deanonymization ini tidak selalu perlu niat jahat; Douglas menilai tindakan dari efek nyata, apakah menyebabkan hilangnya privasi, intimidasi, atau pembungkaman. Kelima, Pada konteks publik peralihan dari ruang tertutup (komunitas terbatas, jurnal pribadi) ke ruang terbuka (media sosial, forum publik, berita) yang membuat kerusakan lebih luas dan sulit dibalik.

2. Menjadikan Target *(Targeting)*

Tindakan *doxing* jenis ini dilakukan dengan mempublikasikan informasi mengenai keberadaan fisik seseorang, dalam artian tindakan ini dapat melacak sampai ditemukan lokasi tempat keberadaaannya dalam waktu yang nyata. Melalui targeting dapat meningkatkan kemungkinan seseorang dan/atau sekelompok orang secara fisik dapat ditemukan dan diketahui domisili tempat dia tinggal. Hal ini dapat membahayakan karena bisa jadi

mengakibatkan seseorang dalam kondisi terancam terutama bahaya secara fisik seperti serangan. Targeting doxing meningkatkan akses fisik terhadap subjek dengan menghilangkan ketidakjelasan mengenai tempat seseorang tinggal atau bekerja. Hilangnya ketidakjelasan ini membuat seseorang lebih rentan terhadap pelecehan fisik karena identitas spesifik yang ia miliki. Tindakan doxing ini dilakukan setelah dilakukannya deanonymizing. seseorang sering memilih untuk anonim agar mengurangi risiko menjadi target. Pengetahuan identitas yang diungkap melalui deanonymizing doxing mempermudah penyingkapan informasi identitas lebih lanjut, seperti lokasi fisik subjek dan tempat kerjanya.

Bentuk-bentuk pelecehan yang dimungkinkan oleh targeting doxing berkisar dari lelucon yang mengganggu hingga serangan fisik (atau lebih buruk). Lelucon yang relatif tidak berbahaya namun menjengkelkan dapat berupa telepon dari dealer mobil yang menanggapi minat palsu terhadap sebuah mobil, hingga harus membatalkan pengiriman barang yang tidak diinginkan yang dipesan atas nama subjek. Bahkan tindakan yang tampaknya sepele sekalipun dapat menjadi sangat mengganggu.[16]

3. Mendelegitimasi *(Delegitimization).*

[16] *Doxing: a conceptual analysis.* Ethics Inf Technol. 2016. Hal.204

Tindakan ini berupa mempublikasikan informasi pribadi seseorang dan/atau sekelompok orang dengan tujuan untuk merusak atau menjatuhkan kredibilitas, reputasi ataupun karakter. Maksud dilakukannya *doxing* ini adalah untuk mempermalukan, menghina, dan menjatuhkan seseorang dengan menggunakan data pribadinya yang mudah disalahpahami atau informasi yang memang rahasia.[17]

3. Motif dan Tujuan *Doxing*

Praktik *doxing* pada dasarnya tidak dilakukan secara acak, tetapi digerakkan oleh berbagai motif yang berkaitan dengan dinamika sosial, psikologis, dan kekuasaan dalam ekosistem digital. Motif-motif tersebut menunjukkan bahwa *doxing* bukan hanya isu teknis terkait penyebaran data, melainkan cerminan dari perilaku sosial manusia ketika berinteraksi melalui media digital. [18]Secara umum, terdapat beberapa tujuan utama yang melatarbelakangi praktik *doxing*, yaitu:

a. Intimidasi atau Ancaman terhadap Korban

Salah satu motif paling dominan dalam *doxing* adalah untuk menciptakan rasa takut dan tekanan psikologis pada korban. Pelaku menyebarkan informasi pribadi seperti alamat rumah, kontak keluarga, tempat bekerja, atau identitas sosial dengan tujuan untuk membuat korban merasa tidak aman dan terancam. Motif intimidasi ini sering digunakan untuk membungkam kritik,

[17] Jeane Neltje Saly and Lubna Tabriz Sulthanah. *Op.cit.* Hal.1712
[18] What is Doxing? Definition and Explanation, https://www.kaspersky.com/resource-center/definitions/what-is-doxing. Diakses pada 07 Desember 2025.

memaksa korban menghentikan aktivitas tertentu, atau menundukkan korban agar patuh terhadap keinginan pelaku. Fenomena ini dikenal juga sebagai *online harassment escalation*, di mana pelecehan digital meningkat menjadi ancaman nyata (*offline risk*).

b. Balas Dendam Pribadi

Motif lain yang sering ditemukan adalah *revenge* atau balas dendam atas konflik interpersonal, hubungan yang berakhir buruk, atau perselisihan daring. Dalam kasus seperti ini, pelaku menganggap *doxing* sebagai alat untuk "menghukum" atau mempermalukan korban. Contoh bentuk balas dendam digital adalah:

1) Mengungkap identitas anonim seseorang setelah terjadi konflik opini.
2) Membocorkan foto, alamat, atau riwayat pribadi akibat perselisihan hubungan.
3) Menyerang reputasi dengan mengaitkan data pribadi korban dengan narasi negatif.

Jenis *doxing* bermotif balas dendam termasuk kategori yang paling sering dijumpai, karena pelaku merasa memiliki justifikasi emosional atas perbuatannya. Fenomena ini sejalan dengan konsep *cyber-vigilantism,* yaitu tindakan individu yang

"mengadili" orang lain melalui media digital tanpa proses hukum.[19]

c. Eksposur Publik untuk Kepentingan Tertentu

Motif berikutnya adalah untuk mengungkap identitas seseorang demi tujuan sosial, politik, atau ideologis. Pada situasi tertentu, pelaku merasa bahwa membuka identitas seseorang adalah tindakan "moral" untuk kepentingan publik

Julia M. MacAllister melalui tulisan dalam jurnalnya (2017) mengklasifikasikan beberapa tujuan dilakukannya yaitu:

a) *Doxing* untuk tujuan jahat. Jenis doxing ini adalah dimana individu melakukan doxing pada orang lain hanya untuk menimbulkan kerugian, kesusahan atau rasa malu yang dapat dimotivasi oleh balas dendam, kemarahan, atau sebatas hanyakeinginan untuk melecehkan seseorang. Melalui internet, memungkinkan doxing yang dilakukan akan menimbulkan kerugian yang besar dibandingkan dengan pelecehan secara langsung.
b) *Doxing* untuk tujuan politik. *Doxing* dengan tujuan politik untuk meningkatkan transparansi, mengungkap apa yang mereka anggap tidak adil atau menungkap informasi yang layak diberitakan untuk kepentingan publik.

[19] *Doxing: The Resource Guide*.https://www.cuny.edu/about/administration/offices/transformation/diversity-equity-and-inclusion-hub/doxing/#:~:text=Doxing%20(or%20doxxing)%20is%20the,often%20obtained%20from%20public%20records. Diakses pada 07 Desember 2025.

c) *Doxing* untuk tujuan pengaturan mandiri. Pengungkap yang memanfaatkan kategori doxing ini untuk mengungkap identitas orang lain yang kehilangan dukungan rekan-rekannya karena berbagai alasan.[20]

4. Dampak *Doxing* terhadap Korban

Doxing memiliki dampak yang serius terhadap korban. Beberapa dampak yang sering terjadi antara lain:

a. Hilangnya privasi

Data pribadi yang seharusnya bersifat rahasia menjadi konsumsi publik, seperti yang diketehaui bahwa data pribadi ini ialah hak fundamental setiap individu untuk mengendalikan informasi pribadi mengenai dirinya, termasuk siapa yang boleh mengakses, menyimpan, atau menyebarkan informasi tersebut. Dalam praktik doxing, privasi ini dirusak secara langsung karena data pribadi yang seharusnya hanya diketahui oleh individu atau pihak tertentu tiba-tiba dipublikasikan ke ruang publik tanpa persetujuan.

b. Risiko Pencurian Identitas

Informasi sensitif bisa digunakan untuk kejahatan seperti penipuan Pencurian identitas (*identity theft*) adalah tindakan ketika seseorang menggunakan data pribadi orang lain secara ilegal untuk memperoleh keuntungan, melakukan penipuan, atau melakukan tindakan yang merugikan korban. Dalam konteks doxing, risiko

[20] Jeane Neltje Saly and Lubna Tabriz Sulthanah. *Op.cit.* Hal.1713

pencurian identitas meningkat secara signifikan karena data sensitif korban diekspos secara publik. Risiko pencurian identitas ini menjadikan doxing bukan sekadar pelanggaran privasi, tetapi **ancaman serius terhadap keamanan personal dan sosial seseorang**.

c. Tekanan Psikologis dan Sosial

Korban bisa merasa stres, tertekan, hingga takut menggunakan internet Praktik doxing tidak hanya berdampak pada aspek hukum dan privasi, tetapi juga menimbulkan konsekuensi psikologis serta sosial yang signifikan bagi korbannya. Ketika data pribadi diekspos secara publik, korban tidak hanya menghadapi ancaman fisik dan digital, tetapi juga mengalami tekanan mental yang berkepanjangan.

Efek ini menunjukkan bahwa doxing bukan sekadar tindakan iseng, tetapi bisa merusak kehidupan seseorang di dunia nyata.[21]

B. Tinjauan Umum tentang Tindak Pidana

1. Pengertian Hukum Pidana

Tindak pidana merupakan konsep penting dalam hukum pidana yang membutuhkan penjelasan lebih mendalam untuk memahami arti dan hakikatnya. Roeslan Saleh menyatakan bahwa *pidana adalah respons terhadap delik, berupa penderitaan yang secara sengaja dijatuhkan oleh negara kepada pelaku perbuatan tersebut*. Sementara itu, Muladi dan Barda Nawawi mengemukakan bahwa pidana memiliki beberapa unsur pokok, yaitu:

[21] Halif, H. (2023). Regulating Doxing and Personal Data Dissemination in Cyberspace. *Journal of Cyber Policy and Human Rights*, 4(1), 22-35. https://doi.org/10.3390/jihhp.v4i4.2044

a. Pada dasarnya pidana merupakan bentuk penderitaan atau akibat lain yang tidak menyenangkan;
b. Pidana diberikan secara sengaja oleh pihak atau lembaga yang memiliki kewenangan;
c. Pidana dijatuhkan kepada seseorang yang telah melakukan perbuatan yang dikategorikan sebagai tindak pidana menurut undang-undang.

Menurut Hermien Hadiati Koeswadji yang dikutip oleh A. Fuad Usfa dan Tongat, istilah *tindak pidana* dalam literatur hukum pidana Indonesia merupakan terjemahan dari istilah Belanda *strafbaar feit*. Dasar utama pemberian pidana bagi pelaku perbuatan pidana adalah keberadaan norma tertulis, yang tercermin dalam asas *tiada pidana tanpa kesalahan*. Asas legalitas ini tercantum dalam Pasal 1 KUHP yang menyatakan bahwa

> "*Tidak ada perbuatan yang dapat dipidana tanpa adanya ketentuan pidana yang mengaturnya terlebih dahulu* (*Nullum delictum nulla poena sine praevia lege poenali*)".

Wirjono Prodjodikoro mendefinisikan tindak pidana sebagai perbuatan seseorang yang dapat dikenai sanksi pidana. Subjek tindak pidana tidak hanya terbatas pada individu, tetapi dapat pula berupa badan hukum yang dianggap mampu bertanggung jawab atas tindakan yang dilakukan. Konsep ini menegaskan bahwa setiap pelanggaran terhadap norma hukum dapat dikenakan sanksi sesuai ketentuan yang

berlaku, sehingga pelaku tindak pidana akan menerima konsekuensi hukum yang sepadan.

Dalam perkembangan teknologi modern, muncul berbagai bentuk tindak pidana baru, termasuk tindak pidana siber. Tindak pidana siber mencakup perbuatan yang memanfaatkan teknologi informasi dan komunikasi untuk merugikan pihak lain. Salah satu bentuknya yang semakin sering terjadi adalah *doxing*, yaitu tindakan mengungkapkan data pribadi seseorang seperti nama, alamat, nomor telepon, hingga informasi sensitif lainnya tanpa persetujuan pemilik data. Tindakan ini dapat menimbulkan dampak serius, baik bagi korban maupun masyarakat secara luas.

Pemerintah Indonesia telah memberikan dasar hukum untuk mengatasi hal tersebut melalui Undang-Undang Nomor 19 Tahun 2016 sebagai perubahan atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE). UU ITE mengatur berbagai bentuk penyalahgunaan teknologi informasi, termasuk *doxing*. Dalam pasal-pasalnya ditegaskan bahwa penyebaran data pribadi tanpa izin merupakan pelanggaran yang dapat dikenai sanksi pidana. Ketentuan ini dibuat untuk melindungi privasi serta keselamatan individu yang dirugikan akibat penyebaran data pribadi secara tidak sah.

2. Asas-asas dalam Hukum Pidana *Doxing*

Terdapat sejumlah asas-asas pelindungan data pribadi yang menjadi landasan UU PDP, asas-asas pelindungan data pribadi secara komprehensif, berikut uraiannya sebagaimana dimuat dalam Pasal 3 UU PDP:

a. Asas Perlindungan, Asas pelindungan adalah asas yang bermakna bahwa setiap pemrosesan data pribadi dilakukan dengan memberikan pelindungan kepada Subjek Data Pribadi atas data pribadinya agar data tersebut tidak disalahgunakan.
b. Asas Kepastian hukum, adalah asas yang bermakna bahwa setiap pemrosesan data pribadi dilakukan dengan landasan hukum untuk mewujudkan pelindungan data pribadi serta segala sesuatu yang mendukung penyelenggaraannya sehingga mendapatkan pengakuan hukum di dalam dan di luar pengadilan.
c. Asas Kepentingan umum, adalah asas yang bermakna bahwa dalam menegakkan pelindungan data pribadi, kepentingan umum atau masyarakat secara luas harus diperhatikan. Adapun yang dimaknai sebagai kepentingan umum tersebut, antara lain kepentingan penyelenggaraan negara dan pertahanan serta keamanan nasional.
d. Asas Kemanfaatan, adalah asas yang bermakna bahwa pengaturan pelindungan data pribadi harus bermanfaat bagi kepentingan nasional, khususnya dalam mewujudkan cita-cita kesejahteraan umum.

e. Asas Kehati-hatian, adalah asas yang bermakna bahwa para pihak yang terkait dengan pemrosesan dan pengawasan data pribadi harus memperhatikan segenap aspek yang berpotensi mendatangkan kerugian.

f. Asas Keseimbangan, adalah asas yang merupakan upaya pelindungan data pribadi untuk menyeimbangkan antara hak atas data pribadi di satu pihak dengan hak negara yang sah berdasarkan kepentingan umum.

g. Asas Akuntabilitas, adalah asas yang bermakna bahwa semua pihak yang terkait dengan pemrosesan dan pengawasan data pribadi bertindak secara bertanggung jawab sehingga mampu menjamin keseimbangan hak dan kewajiban para pihak yang terkait, termasuk halnya Subjek Data Pribadi.

h. Asas Kerahasiaan, adalah asas yang bermakna bahwa data pribadi terlindungi dari pihak yang tidak berhak dan/atau dari kegiatan pemrosesan data pribadi yang tidak sah.[22]

3. Unsur-unsur Tindak Pidana dalam Perspektif *Doxing*

Berdasarkan pasal 27 ayat 4 Undang-Undang Nomor 11 tahun 2008, *Jo* Undang-Undang Nomor 19 tahun 2016, adalah ilegal bagi seseorang untuk menyebarkan data pribadi seseorang bersama dengan konten yang mengandung ancaman. Menurut Pasal 27 Ayat 3 Undang-Undang ITE, *doxing* terdiri dari komponen berikut:

[22] Mengenal 8 Asas Pelindungan Data Pribadi dalam UU PDP. https://www.hukumonline.com/berita/a/asas-pelindungan-data-pribadi-lt6368bc61e4b97/. Diakses pada 08 Desember 2025.

1) Setiap orang
2) Melawan hukum
3) Menyerang kehormatan seseorang
4) Menuduhkan sesuatu untuk diketahui umum
5) Dalam bentuk elektronik dan atau dokumen elektronik
6) Dilakukan secara sistem elektronik

Dalam revisi terbaru Undang-Undang ITE, uraian pasal 27 telah dipersingkat untuk memudahkan pemidanaan bagi pelaku *doxing* yang sebelumnya merujuk kepada KUHP. Jika doxing mengandung kekerasan atau ancaman, seperti 9 ancaman secara fisik di dunia nyata, pelaku dapat dikenakan pasal 368 KUHP, yang ancamannya pidana.

Doxing juga dapat dikaitkan dengan Pasal 513 KUHP, yang menyatakan bahwa dilarang menggunakan barang yang bersifat informasi pribadi tanpa persetujuan orang tersebut. Pelaku doxing dapat dikenakan hukuman menurut ITE dan KUHP. [23] Pencurian dan penyebaran data pribadi juga melanggar hak korban, yaitu hak untuk mendapatkan privasi dan kebebasan berpendapat, yang disebutkan dalam pasal 28E ayat 2 dan 3 dan juga dimuat dalam pasal 28G ayat 1. UUD 1945. Beberapa hal penting yang perlu diperhatikan ketika terjadi tindakan doxing adalah sebagai berikut:

1) Ada atau tidaknya persetujuan (consent) untuk mengungkapkan data;
2) Muatan atau bentuk data pribadi yang diungkapkan;

[23] https://heylaw.id/blog/doxing-dan-penggerusan-privasi-online, diakses pada 07 Desember 2025.

3) Cara mendapatkannya;

4) Akibat atau jenis kerugian yang diderita oleh korban (target);dan

5) Alasan di balik tindakan doxing.

Yang dalam penjabarannya yaitu Perbuatan yang dilakukan secara sengaja pelaku harus memiliki unsur kesengajaan ketika menyebarkan informasi. Artinya, tindakan tersebut dilakukan dengan sadar, bukan karena kelalaian atau tanpa maksud. Distribusi (menyebarkan), transmisi (mengirimkan), atau membuat dapat diaksesnya informasi elektronik dan/atau dokumen elektronik komponen ini meliputi segala bentuk tindakan yang menyebabkan data pribadi korban tersebar atau dapat diakses publik. Contohnya: mem-posting identitas seseorang di media sosial, mengunggah alamat atau nomor telepon di forum, atau mengirimkan data pribadi ke pihak ketiga. Muatan penghinaan dan/atau pencemaran nama baik. *Doxing* pada prinsipnya dianggap sebagai pelanggaran UU ITE ketika informasi yang disebarkan mengandung unsur penghinaan atau pencemaran nama baik. Dengan kata lain, penyebaran data pribadi tersebut bertujuan untuk menjatuhkan reputasi, mempermalukan, atau merugikan subjeknya. Dilakukan melalui media elektronik seluruh tindakan harus dilakukan menggunakan sarana elektronik: internet, media sosial, aplikasi pesan, situs web, email, dan platform digital lainnya. Inilah yang membedakan *doxing* dari penghinaan/pencemaran secara luring.

C. Tinjauan Umum tentang Perlindungan Data Pribadi

1. Pengertian Data Pribadi dan Privasi Digital

Menurut Peraturan Pemerintah Nomor 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik, data pribadi didefinisikan sebagai segala jenis informasi yang berkaitan dengan individu, baik yang dapat diidentifikasi secara langsung maupun tidak langsung, baik secara mandiri maupun melalui penggabungan dengan informasi lain, yang dapat diakses melalui sistem elektronik maupun non-elektronik. Data perorangan tertentu adalah setiap informasi yang benar dan nyata serta melekat dan dapat diidentifikasi, baik langsung maupun tidak langsung, ada masing-masing individu yang pemanfaatannya sesuai ketentuan peraturan perundang-undangan.

Data pribadi dan kerahasiaan (privasi) adalah satu kesatuan yang tidak dapat dibelah menjadi dua bagian. Hal ini dikarenakan data pribadi saling berkaitan dengan privasi, apabila kita membicarakan tentang data pribadi yang dimiliki seseorang, secara tidak langsung kita juga membicarakan juga mengenai tentang privasi orang tersebut yang harus dilindungi serta dihormati.

Menurut Abu Bakar Munir, privasi dibagi menjadi 4 golongan, yaitu:

a. Privasi atas informasi, berkaitan dengan cara pengumpulan dan pengelolaan data pribadi seperti informasi kredit dan catatan kesehatan;

b. Privasi atas anggota badan, berkaitan dengan perlindungan secara fisik seseorang seperti prosedur pemeriksaan penggunaan obat bius, pengambilan data biometrik seperti sidik jari dan retina mata;
c. Privasi atas komunikasi, meliputi perlindungan atas komunikasi seseorang contohnya surat, telepon, email atau bentuk-bentuk komunikasi lainnya.[24]

Berdasarkan Pasal 6 Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi, data pribadi dibagi menjadi dua jenis, yaitu data pribadi bersifat umum dan data pribadi bersifat sensitif. Data umum mencakup informasi seperti nama, tempat dan tanggal lahir, nomor identitas, biometrik, hingga data lain yang dapat mengidentifikasi seseorang. Sementara itu, data sensitif mencakup informasi yang lebih privat dan memerlukan perlindungan ekstra, seperti data kesehatan, kondisi mental, kebiasaan pribadi, pandangan politik, data anak, hingga keuangan pribadi. Perlakuan hukum terhadap kedua jenis data ini berbeda, dengan data sensitif mendapat pengamanan yang lebih ketat karena potensi dampaknya yang lebih besar jika disalahgunakan. Serta salah satu bentuk data yang dilindungi adalah yang berbentuk informasi elektronik sebagai sekumpulan data elektronik, termasuk tetapi tidak terbatas pada tulisan, suara, gambar, peta, rancangan, foto, surat elektronik, atau sejenisnya, huruf, tanda,

[24] Tacino, Muhammad Jefri Maruli.*"Perlindungan terhadap hak Pribadi Seseorang di Media Sosial Menurut Undang-Undang Nomor 19 Tahun 2016 tentang Informasi dan Transaksi Elektronik".* (Jurnal Ilmiah Ilmu Hukum), (2020). Hal.179.

angka, kode akses, dan simbol. Informasi elektronik ini dapat terdapat dalam sistem elektronik atau berupa sebuah dokumen elektronik.

2. Hak dan Kewajiban dalam Perlindungan Data Pribadi

Pemerintah sebagai pembuat regulasi mengatur hak dan kewajiban pengendali data pribadi dalam UU No. 27 Tahun 2022 tentang perlindungan data pribadi.

a. Hak Pengendali Data Pribadi dalam UU No. 27 Tahun 2022

Menurut UU No. 27 Tahun 2022, pengendali data pribadi adalah setiap orang, badan publik, dan organisasi internasional yang bertindak sendiri-sendiri atau bersama-sama dalam menentukan tujuan dan melakukan kendali pemrosesan data pribadi. Pihak ini bertanggung jawab dalam melindungi data, memastikan penggunanya aman dan sesuai hukum, serta bertanggung jawab penuh atas setiap aktivitas pemrosesan data pribadi. Terdapat juga berbagai jenis-jenis data pribadi dalam UU No. 27 Tahun 2022 tersebut.

UU No. 27 Tahun 2022 telah mengatur hak-hak pengendali data pribadi dalam mengolah dan memproses data pribadi subjek data pribadi. Berikut hak pengendali data pribadi dalam UU No.27 Tahun 2022:

a) Menentukan tujuan dan kendali pemrosesan data pribadi berdasarkan Pasal 1 angka 4.
b) Menetapkan dasar hukum pemrosesan data pribadi sesuai Pasal 20 seperti persetujuan sah dari subjek data pribadi,

pemenuhan kewajiban perjanjian atau hukum, perlindungan kepentingan vital subjek data, kepentingan umum atau pelayanan publik, serta kepentingan sah lainnya dengan keseimbangan terhadap hak subjek data.

c) Menolak permintaan akses atau perubahan data jika membahayakan keamanan, melanggar hukum, atau bertentangan dengan kepentingan nasional yang tertuang pada Pasal 33.

d) Menetapkan kebijakan internal dan sistem keamanan untuk melindungi data pribadi yang sesuai Pasal 35-39.

e) Mengalihkan data pribadi antar-pengendali di dalam maupun luar negeri sepanjang memenuhi ketentuan perlindungan data yang tertuang pada Pasal 55-56.

b. Hak Pengendali Data Pribadi dalam UU No. 27 Tahun 2022 Kewajiban Pengendali Data Pribadi dalam UU No. 27 Tahun 2022

Kewajiban pengendalian UU Perlindungan Data Pribadi (PDP) memuat kewajiban yang terperinci yang tertulis dari 20 pasal yaitu Pasal 20-49. Berikut kewajiban pengendali data pribadi berdasarkan UU No. 27 Tahun 2022:

1) Dasar dan Prinsip Pemrosesan

Pasal 20, pengendali data pribadi wajib memiliki dasar pemrosesan data pribadi.

Pasal 27, pengendali data pribadi wajib melakukan pemrosesan data pribadi secara terbatas dan spesifik, sah secara hukum, dan transparan.

Pasal 28, pengendali data pribadi wajib melakukan pemrosesan data pribadi sesuai dengan tujuan pemrosesan data pribadi.

Pasal 29, pengendali data pribadi wajib melakukan pemrosesan data pribadi sesuai dengan tujuan pemrosesan data pribadi.

2) Pemenuhan Hak Subjek Data

Pasal 30, pengendali data pribadi wajib memperbarui dan/ atau memperbaiki kesalahan dan / atau ketidakakuratan data pribadi paling lambat 3 x 24 (tiga kali dua puluh empat) jam terhitung sejak pengendali data pribadi menerima permintaan pembaruan dan /atau perbaikan data pribadi.

Pasal 32, pengendali data pribadi wajib memberikan akses kepada subjek data pribadi terhadap data pribadi yang diproses beserta rekam jejak pemrosesan data pribadi sesuai dengan jangka waktu penyimpanan data pribadi.

Pasal 34, pengendali data pribadi wajib melakukan penilaian dampak perlindungan data pribadi dalam hal pemrosesan data pribadi memiliki potensi risiko tinggi terhadap subjek data pribadi.

3) Perlindungan dan Keamanan Data

Pasal 35, pengendali data pribadi wajib melindungi dan memastikan keamanan data pribadi yang diprosesnya dengan menyusun langkah teknis dan operasional perlindungan data.

Pasal 36-39, pengendali data pribadi wajib menjaga kerahasiaan, mencegah akses atau pemrosesan yang tidak sah.

Pasal 40, pengendali data pribadi wajib menghentikan pemrosesan data pribadi dalam hal subjek data pribadi menarik kembali persetujuan pemrosesan data pribadi.

Pasal 41, pengendali data pribadi wajib melakukan penundaan dan pembatasan pemrosesan data pribadi baik sebagian maupun seluruhnya paling lambat 3 x 24 (tiga kali dua puluh empat) jam terhitung sejak pengendali data pribadi menerima permintaan penundaan dan pembatasan pemrosesan data pribadi.

4) Penghapusan dan Kegagalan Pelindungan

Pasal 44-45, pengendali data pribadi wajib menghapus/memusnahkan data setelah masa retensi berakhir atau atas permintaan subjek data pribadi.

Pasal 46, dalam hal terjadi kegagalan pelindungan data pribadi, pengendali data pribadi wajib menyampaikan pemberitahuan secara tertulis paling lambat 3 x 24 (tiga kali

dua puluh empat) jam kepada subjek data pribadi dan lembaga.

5) Akuntabilitas dan Tanggung Jawab

Pasal 47, pengendali data pribadi wajib bertanggung jawab atas pemrosesan data pribadi dan menunjukkan pertanggungjawaban dalam pemenuhan kewajiban pelaksanaan prinsip pelindungan data pribadi

Pasal 48, pengendali data pribadi berbentuk badan hukum yang melakukan penggabungan, pemisahan, pengambilalihan, peleburan, atau pembubaran badan hukum wajib menyampaikan pemberitahuan pengalihan data pribadi kepada subjek data pribadi.

Pasal 49, pengendali data pribadi dan / atau prosesor data pribadi wajib melaksanakan perintah lembaga dalam rangka penyelenggaraan pelindungan data pribadi sesuai dengan undang-undang ini.

Pasal 53-54, pengendali data pribadi wajib menunjuk pejabat/petugas pelindungan data pribadi *(data protection officer)* bila memenuhi kriteria tertentu.

3. Sanksi terhadap Pelanggaran Data Pribadi

Adapun UU PDP berisikan aturan seperti pelindungan hak fundamental warga negara, memperkuat kewenangan pemerintah dalam pemantauan pihak yang memproses data, payung hukum pelindungan data pribadi, keseimbangan hak subjek data pribadi dengan kewajiban

pengendali data, mendorong reformasi praktik pemrosesan data di seluruh pengendali data pribadi, memberikan perlindungan kepada kelompok rentan khususnya anak dan penyandang disabilitas, serta kesempatan untuk meningkatkan standar industri.

Di samping itu, adanya UU PDP akan mengedepankan perspektif pelindungan data pribadi dalam setiap pengembangan teknologi baru, sehingga akan mendorong inovasi yang beretika dan menghormati hak asasi manusia. Sebagai upaya mengantisipasi kemajuan teknologi dan budaya digital, adanya UU PDP juga diharapkan mendorong kebiasaan baru pada masyarakat untuk lebih menerapkan pelindungan data pribadi. Dengan begitu, menurut Menteri Johnny, regulasi tersebut akan mendorong tumbuhnya ekosistem digital dalam memperbanyak talenta baru dalam bidang perlindungan data pribadi, baik di instansi pemerintahan, swasta ataupun publik.

Sanksi Hukum dan Lembaga PDP, secara garis besar dalam UU PDP tersebut, antara lain, diatur mengenai Lembaga Pelindungan Data Pribadi (PDP). Selain itu, juga diatur mengenai sanksi atau hukuman untuk pelanggaran UU PDP. Sanksi berlaku bagi penyelenggara sistem elektronik (PSE), baik pemerintah (publik) maupun swasta (privat), perseorangan, serta korporasi. Disebutkan, UU PDP mengamanatkan pembentukan Lembaga PDP berada di bawah presiden dan bertanggung jawab kepada presiden. Mengenai Lembaga PDP diatur dalam Pasal 58 dan 60 UU PDP.

Lembaga PDP memiliki sejumlah fungsi dan tugas, di antaranya, merumuskan dan menetapkan kebijakan serta strategi PDP, pengawasan penyelenggaraan PDP, penegakan hukum administratif terhadap pelanggaran UU PDP, dan memfasilitasi penyelesaian sengketa di luar pengadilan *(out of court)* terkait pelindungan data pribadi di ranah digital.

Dalam draf UU PDP, terdapat dua jenis sanksi bagi pelanggar data pribadi. Jenis pertama, bagi pengendali atau pemroses data pribadi jika melanggar ketentuan UU PDP. Di antaranya, tidak memproses data pribadi sesuai tujuannya dan tidak mencegah akses data tidak sah. Sanksi hukum terdiri dari empat jenis, yaitu pertama, sanksi administratif dalam Pasal 57 UU PDP berupa peringatan tertulis; kedua, penghentian sementara kegiatan pemrosesan data pribadi; ketiga, penghapusan atau pemusnahan data pribadi; dan/atau keempat, denda administratif/paling tinggi dua persen dari pendapatan tahunan atau penerimaan tahunan terhadap variabel pelanggaran.

Jenis kedua, bagi orang perseorangan atau korporasi yang melakukan perbuatan terlarang. Di antaranya, mengumpulkan data pribadi yang bukan miliknya untuk menguntungkan diri sendiri atau orang lain mengungkapkan data pribadi yang bukan miliknya dan memalsukan data pribadi untuk keuntungan yang mengakibatkan kerugian bagi orang lain dapat dikenakan Pasal 67 sampai dengan 73 UU PDP.

Adapun ketentuan pidana diatur dalam UU sebagai berikut pertama pidana denda maksimal Rp4 miliar hingga Rp6 miliar, dan kedua, pidana penjara maksimal 4 tahun hingga 6 tahun.

Selain sanksi yang sudah disebutkan di atas, Pasal 69 mengatur pidana tambahan berupa perampasan keuntungan dan/atau harta kekayaan yang diperoleh atau hasil dari tindak pidana dan pembayaran ganti kerugian. Jika tindak pidana dilakukan oleh korporasi, menurut Pasal 70 UU PDP, dapat dikenakan hukuman denda sebesar 10 kali lipat dari yang pidana asli beserta penjatuhan pidana tambahan tertentu lainnya.[25]

Untuk pelanggaran UU PDP memalsukan data pribadi dapat dipidana 6 tahun dan atau denda sebesar Rp60 miliar. Jika menjual atau membeli data pribadi akan dipidana 5 tahun atau denda sebesar Rp50 miliar. Korporasi yang kedapatan melanggar undang-undang ini dapat dikenakan pidana tambahan berupa perampasan keuntungan dan/atau harta kekayaan/pembekuan seluruh atau sebagian usaha korporasi sampai dengan pembubaran korporasi.

D. Pengaturan *Doxing* dalam Sistem Hukum Positif Indonesia

1. Peraturan Undang-Undangan tentang *Doxing*

Pemerintah Indonesia telah mengatur masalah ini dalam Undang-Undang Nomor 19 Tahun 2016 tentang Perubahan atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi

[25] *Mengenal Sanksi Pelanggar Data Pribadi*. https://www.komdigi.go.id/berita/artikel/detail/mengenal-sanksi-pelanggar-data-pribadi. Diakses tanggal 07 Desember 2025.

Elektronik (UU ITE). Undang-Undang ITE mengatur berbagai tindakan yang berkaitan dengan penyalahgunaan teknologi informasi, termasuk di dalamnya adalah tindakan *doxing*. Dalam pasal-pasal yang relevan, disebutkan bahwa pengungkapan data pribadi tanpa izin merupakan pelanggaran yang dapat dikenakan sanksi pidana. Hal ini bertujuan untuk memberikan perlindungan terhadap individu yang menjadi korban penyebaran data pribadi yang dapat membahayakan privasi dan keselamatan mereka.

Selain Undang-Undang ITE, Indonesia juga telah memiliki Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi (UU PDP). UU PDP ini mengatur lebih lanjut tentang hak-hak individu terkait dengan perlindungan data pribadi mereka. Salah satu fokus utama dari UU PDP adalah memberikan kontrol kepada individu atas data pribadi mereka serta memberikan sanksi bagi mereka yang melakukan penyalahgunaan atau pelanggaran terhadap data pribadi. *Doxing* jelas melanggar ketentuan yang ada dalam UU PDP, karena tindakan ini secara langsung berkaitan dengan pengungkapan data pribadi tanpa izin yang dapat menimbulkan kerugian bagi korban. Tindak pidana *doxing* ini semakin menonjol dalam era digital, di mana informasi pribadi mudah diakses dan disebarluaskan. Oleh karena itu, sangat penting bagi masyarakat untuk memahami risiko dari tindak pidana ini serta menjaga privasi dan data pribadi mereka dengan bijak. Dalam upaya mencegah dan menangani doxing, diperlukan kerjasama antara pihak pemerintah, penyedia platform digital, serta masyarakat.

Pemerintah perlu terus memperbarui regulasi yang ada agar dapat menanggulangi ancaman kejahatan siber, sementara masyarakat juga harus meningkatkan kesadaran akan pentingnya perlindungan data pribadi dalam kehidupan digital mereka.

2. Ketiadaan Pengaturan Khusus tentang *Doxing*

Salah satu faktor penghambat dalam upaya penegakan hukum terhadap korban doxing di Indonesia adalah minimnya pengaturan hukum yang secara khusus mengatur kejahatan *doxing.* Meskipun tindakan *doxing* dapat dikategorikan sebagai tindak pidana siber dan telah diatur dalam Undang-Undang Nomor 19 Tahun 2016 tentang Perubahan atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE), Pasal 26 ayat (1), yang menyebutkan bahwa setiap orang berhak atas perlindungan data pribadi dalam sistem elektronik, namun ketentuan tersebut masih bersifat umum dan belum secara spesifik mengatur mengenai doxing sebagai bentuk kejahatan yang berdiri sendiri. Hal ini menyebabkan ruang lingkup penegakan hukumnya menjadi terbatas dan interpretasi hukumnya kerap menimbulkan perdebatan.

Ketidakpastian dalam proses penanganan kasus kejahatan doxing juga menjadi hambatan serius. Proses penyelidikan dan pembuktian seringkali terhambat oleh keterbatasan dalam pelacakan identitas pelaku yang umumnya menggunakan akun anonim atau media yang sulit diakses oleh aparat penegak hukum. Dalam banyak kasus, sulitnya menemukan bukti digital yang valid dan dapat dipertanggungjawabkan

secara hukum menjadi tantangan utama bagi kepolisian dan kejaksaan. Kondisi ini berdampak pada rendahnya angka penyelesaian kasus *doxing* di Indonesia, sehingga korban sering kali tidak mendapatkan keadilan yang memadai. Meskipun Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi telah memberikan landasan hukum yang lebih kuat, implementasi UU ini masih menghadapi berbagai kendala. Dalam Pasal 65 ayat (2) disebutkan bahwa setiap orang yang dengan sengaja dan melawan hukum mengungkapkan data pribadi yang bukan miliknya dapat dipidana penjara paling lama lima tahun dan/atau denda maksimal Rp 5 miliar.

Namun dalam praktiknya, belum semua aparat penegak hukum memahami teknis pelaksanaan UU tersebut dengan baik, mengingat regulasi ini masih relatif baru dan sosialisasinya belum merata di seluruh wilayah Indonesia. Kurangnya kolaborasi antara pemerintah, aparat penegak hukum, dan masyarakat juga menjadi faktor penghambat dalam memberikan perlindungan yang optimal bagi korban doxing. Tanpa adanya sinergi yang baik, upaya pencegahan, edukasi, serta pelaporan kasus doxing menjadi tidak efektif. Masyarakat sering kali tidak mengetahui hak-hak mereka terkait data pribadi dan bagaimana melindungi diri dari serangan doxing, sedangkan aparat hukum terkadang belum mendapatkan pelatihan yang memadai dalam penanganan kejahatan siber yang kompleks ini. Diperlukan upaya kolaboratif yang berkelanjutan antara seluruh pemangku kepentingan untuk memperkuat perlindungan hukum bagi

korban doxing di Indonesia. Perlu adanya perbaikan regulasi yang lebih spesifik mengenai kejahatan doxing, peningkatan kapasitas aparat penegak hukum, serta penyuluhan hukum kepada masyarakat agar mereka lebih sadar akan pentingnya menjaga data pribadi. Menegaskan bahwa penguatan penerapan Undang-Undang Nomor 27 Tahun 2022 dan revisi kebijakan terkait UU ITE adalah langkah penting dalam menciptakan keadilan dan rasa aman bagi setiap warga negara dalam era digital.

E. Urgensi Pengaturan *Doxing* dalam Hukum Pidana Indonesia

1. Secara Filosofis

Secara filosofis, upaya pengaturan hak privasi atas data diri merupakan manifestasi dari pengakuan dan Perlindungan hak-hak dasar manusia. Oleh karena itu, penyusunan Rancangan Undang-Undang Perlindungan Data Pribadi memiliki landasan filosofis yang kuat dan dapat dipertanggungjawabkan. Secara khusus, UU PDP mengharuskan pengolahan data pribadi dilakukan berdasarkan prinsip legalitas, proporsionalitas, dan transparansi. Ini berarti bahwa data pribadi tidak boleh diproses tanpa dasar hukum yang kuat, harus sebanding dengan tujuan pengolahan, dan dilakukan secara terbuka serta jujur. Dengan demikian, *doxing* yang melibatkan penggunaan data pribadi tanpa izin dan sering kali untuk tujuan yang merugikan tidak memenuhi kriteria ini dan jelas merupakan tindakan ilegal. Landasan filosofis adalah Pancasila yang merupakan *recthsidee* (cita hukum) atau konstruksi pikir (ide) untuk mengarahkan hukum kepada apa yang dicita-citakan. (Rosadi Sinta,Op., Cit, hlm.11) Rudolf Stammler mengatakan bahwa

rechtsidee berfungsi sebagai *leitsern* (bintang pemandu) bagi terwujudnya cita-cita sebuah masyarakat. Dari situlah disusun konsep dan politik hukum sebuah negara. Cita hukum merupakan sesuatu yang bersifat normatif dan konstitutif, normatif berarti memiliki fungsi sebagai prasyarat transendental yang mendasari bermartabatnya hukum positif. Selain itu,cita hukum juga merupakan landasan moral hukum sekaligus tolak ukur sistem hukum positif. Konstitutif berarti *rechtsidee* berfungsi sebagai arah bagi hukum untuk mencapai tujuan. Gustav Radbruch menyatakan bahwa *rechtsidee* memberikan makna bagi hukum sebagai dasar yang bersifat konstitutif bagi hukum positif. *Rechtsidee* merupakan tolok ukur yang bersifat regulatif untuk menguji keadilan hukum positif. Cita hukum akan berpengaruh dan berfungsi sebagai asas umum yang memberikan pedoman *(guiding principle),* norma kritik (kaidah evaluasi) dan faktor yang memotivasi dalam penyelenggaraan hukum dalam hal Pembentukan, penemuan, penerapan, dan perilaku hukum. Sila kedua Pancasila yang berbunyi, Kemanusiaan yang adil dan beradab, merupakan landasan filosofis Perlindungan data pribadi. Perlindungan yang dimaksud akan menciptakan keadilan, juga membentuk peradaban manusia yang menghormati dan menghargai data pribadi. Secara yuridis, nilai-nilai Pancasila harus diderivasikan ke dalam seluruh peraturan perundang-undangan sebagai konsekuensi dari kedudukan Pancasila yang terkandung dalam Pembukaan Undang-Undang Dasar Negara Republik Indonesia Tahun 1945 Pancasila terkandung dalam Pembukaan

Undang-Undang Dasar Negara Republik Indonesia Tahun 1945 sebagai konstitusi negara Indonesia. UndangUndang Dasar Negara Republik Indonesia Tahun 1945 merupakan dasar hukum bagi pembentukan hukum positifyang mengandung empat ide pokok. Cita Perlindungan mengandung makna bahwa hukum menjamin Perlindungan untuk segenap bangsa Indonesia. Hal ini selaras dengan prinsip keadilan kumulatif yang dikemukakan oleh Jeremy Bentham. la mengemukakan bahwa fungsi utama dari hukum adalah memberikan penghidupan, mendorong persamaan, dan memelihara keamanan bagi semua orang. Sementara itu, cita keadilan sosial mencerminkan hukum yang menjamin keadilan dalam bermasyarakat. Keadilan sosial yang mengutamakan perlakuan adil kepada seluruh rakyat Indonesia tanpa memandang ras, golongan, dan agama. Aristoteles dan Thomas Aquinas memandang keadilan semacam itu sebagai keadilan distributif. Keadilan distributif merupakan pembagian barang dan kehormatan kepada masing-masing anggota masyarakat sesuai dengan kedudukannya dalam masyarakat. Selanjutnya, cita kemanfaatan adalah cita hukum mengenai kegunaan hukum dalam bernegara. Sunaryati Hartono memandang para pendiri bangsa Indonesia menganut falsafah hukum bahwa rakyat memiliki hak asasi manusia, baik sebagai kelompok maupun perorangan. Perlindungan data pribadi merupakan perwujudan dari Perlindungan hak asasi manusia sebagaimana paham yang dianut oleh bangsa Indonesia. Negara hukum yang demokratis merupakan cita-cita para pendiri bangsa *(the founding fathers)* dengan

menjadikan keadilan sebagai tujuan dari negara hukum". Dengan terciptanya negara hukum yang demokratis, peningkatan kesejahteraan umum dan kecerdasan bangsa juga menjadi tujuan negara kesejahteraan *(welvartstaat)*. Dengan lain kata, penyusun Undang-Undang Dasar Negara Republik Indonesia Tahun 1945 bukan hanya mengharapkan negara hukum dalam arti sempit. Penyusun juga tidak hanya mengharapkan negara yang berdasar undang-undang atau kehidupan bernegara yang berdasarkan kepada supremasi hukum semata. Harapan utamanya adalah kehidupan berbangsa dan bernegara yang membawa keadilan sosial bagi seluruh rakyat Indonesia. Tidak hanya adil bagi Indonesia sebagai satu kesatuan politik, tetapi juga bagi tiap warga negara tanpa memandang perbedaan asal-usul etnologis atau rasial, strata status sosial seseorang, maupun agama yang dianut.

2. Secara Sosiologis

Perumusan aturan mengenai pelindungan data pribadi dapat dipahami secara sosiologis. Hal tersebut karena kebutuhan untuk melindungi hak-hak individual dalam masyarakat yang berhubungan dengan pengumpulan, pemrosesan, pengelolaan, dan penyebarluasan data pribadi. Pelindungan privasi mengenai data diri pribadi yang memadai akan menumbuhkan kepercayaan masyarakat untuk menyediakan data pribadi guna berbagai kepentingan yang lebih besar tanpa disalahgunakan atau dilanggar hakhak pribadinya. Dengan demikian, pengaturan ini akan menciptakan keseimbangan antara hak-hak individu dan masyarakat yang diwakili kepentingannya oleh

negara. Dalam hal praktik *doxing* menyoroti perlunya kesadaran yang lebih besar tentang risiko dan konsekuensi hukum dari kegiatan ini, baik bagi pelaku maupun bagi korban. Untuk mengatasi dan mencegah *doxing,* penting bagi pemerintah untuk melakukan edukasi kepada publik tentang pentingnya melindungi privasi *online* dan juga untuk memperkuat implementasi peraturan yang melindungi data pribadi.

Penerapan efektif UU PDP dan kerjasama antar lembaga, termasuk lembaga penegak hukum dan penyedia layanan internet, adalah kunci untuk menangani masalah doxing dengan cara yang efektif dan menghormati hak privasi setiap individu.[26] Pengaturan tentang pelindungan data pribadi akan memberikan kontribusi yang besar terhadap terciptanya ketertiban dan kemajuan dalam masyarakat informasi. Secara sosiologis terkesan bahwa masyarakat Indonesia belum atau kurang menghargai privasi karena nilai-nilai tersebut bukan berasal dari bangsa Indonesia. Padahal masyarakat juga menghargai privasi dengan tidak mengganggu atau mengusik kehidupan setiap individu sebagai anggota masyarakat. Bahkan tindakan-tindakan seperti itu disadari sebagai tindakan yang kurang pantas dan bertentangan dengan nilainilai luhur berbangsa dan hal ini juga tercermin dari hasil survei yang menunjukkan bahwa bernegara. terdapat kesadaran data pribadi dan harapan masyarakat terhadap pelindungan privasi menyangkut data pribadi. Kurangnya kesadaran

[26] Fikri, M. & Rusdiana, S. (2023). Ruang Lingkup Perlindungan Data Pribadi:Kajian Hukum Positif Indonesia. Ganesha Law Review, 5(1), 39-57.

masyarakat terhadap pelindungan privasi menyebabkan adanya ruang atas sejumlah pelanggaran dan penyalahgunaan data pribadi. Potensi pelanggaran hak privasi terhadap data pribadi ini tidak hanya di dunia maya atau *online,* tetapi juga dapat terjadi di dunia nyata atau *offline*. Beberapa contoh potensi pelanggaran yang dapat terjadi secara *online*, yaitu pengumpulan data pribadi secara massal *(digital dossier),* pemasaran langsung *(directselling),* media sosial, pelaksanaan program KTP-el, pelaksanaan program *e-health*, hingga kegiatan komputasi awan *(cloud computing)*.[27]

3. Alasan Yuridis

Secara yuridis tentang pelindungan data pribadi bersumber kepada Pada Pasal 28G dan Pasal 28H Undang-Undang Dasar Negara Republik Indonesia Tahun 1945. Dengan demikian pelindungan data pribadi merupakan salah satu bentuk perwujudan amanat konstitusi yang harus diatur dalam bentuk undang-undang. Pasal 28G Undang-Undang Dasar Negara Republik Indonesia Tahun 1945 menyatakan bahwa,

> *"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 merupakan hak asasi."*

Berikutnya, pada Pasal 28H ayat (4) Undang-Undang Dasar Negara Republik Indonesia Tahun 1945 menyatakan bahwa,

> *"Setiap orang berhak mempunyai hak milik pribadi dan hak milik tersebut tidak boleh diambil alih secara sewenang-wenang oleh siapa pun."*

[27] Nabila,Annisa.Marlinaa.Leviza,Jelly. 2025. *Kebijakan Hukum Pidana terhadap Perlindungan Pengguna Media Sosial dari Pelaku Doxing sebagai Upaya Perlindungan Hak Privasi Individu.*Jurnal Ilmu Hukum, Humaniora dan Politik. Vol.6 No.1. Hal.16.

Pasal-pasal ini menjadi pertimbangan bagi perlunya pembentukan peraturan perundang-undangan yang melindungi data pribadi. Putusan Mahkamah Konstitusi Nomor 006/PUU-I/2003 semakin mempertegas bahwa pengaturan pelindungan data pribadi harus dalam bentuk Undang-undang. Dalam putusan Mahkamah Konstitusi tersebut disebutkan bahwa ketentuan yang menyangkut HAM harus dalam bentuk Undang-Undang.[28] Penegakan hukum terhadap doxing menimbulkan tantangan tersendiri, terutama terkait dengan identifikasi pelaku dan pembuktian bahwa *doxing* memang terjadi. Banyak kasus *doxing* terjadi secara anonim atau melalui platform *online* yang memungkinkan pelaku untuk menyembunyikan identitas mereka. Ini mempersulit proses penegakan hukum dan sering kali memerlukan kerjasama antara agen penegak hukum dan penyedia layanan internet pemanfaatan ilmu pengetahuan dan teknologi harus dilakukan untuk mewujudkan bangsa yang berdayasaing sebagaimana telah ditentukan dalam Undang-Undang Nomor 17 Tahun 2007 tentang Rencana Pembangunan Jangka Panjang Nasional 2005-2025.

4. Kebutuhan Pembentukan Norma Khusus

Permasalahan kebocoran informasi individu di internet kian kerap bermunculan dan semakin kompleks bentuknya. Tidak hanya terjadi pada pengguna biasa, tetapi juga melibatkan berbagai industri global

[28] Adi Nugraha and Saputra, *"Penerapan Hukum Terhadap Tindak Pidana Doxing Di Indonesia"*, 2024, Hlm. 12.

raksasa yang menjadi target empuk para pelaku kejahatan siber. Kasus-kasus kebocoran data serupa juga terjadi di Indonesia, di mana banyak akun maupun informasi pribadi pengguna internet bocor dan beredar bebas melalui media sosial, forum gelap, hingga platform e-commerce. Kondisi ini menunjukkan bahwa ekosistem digital Indonesia masih menghadapi kerentanan serius terhadap pelanggaran privasi dan penyalahgunaan data pribadi.

Penguatan hukum terkait kebocoran informasi individu di Indonesia masih jauh tertinggal dibandingkan dengan negara-negara lain yang lebih progresif dalam membangun payung hukum perlindungan data pribadi. Kelemahan penegakan hukum, ketidakjelasan mekanisme pertanggungjawaban, hingga ketiadaan sanksi tegas yang bersifat *deterrent* menyebabkan pelaku tidak mendapatkan efek jera. Akibatnya, insiden kebocoran data berpotensi terus berulang tanpa ada penanganan yang sistematis dan komprehensif.

Dalam konteks inilah, kebutuhan pembentukan norma hukum khusus menjadi sangat mendesak. Norma khusus diperlukan untuk mengisi kekosongan regulasi yang belum secara rinci mengatur tata kelola data, standar keamanan informasi, kewajiban pengendali data, hingga mekanisme pemulihan bagi korban. Norma khusus juga berfungsi memberikan kepastian hukum yang lebih kuat, baik bagi masyarakat sebagai pemilik data, maupun bagi pelaku usaha sebagai pengelola data. Dengan adanya pengaturan yang jelas, tegas, dan terstruktur, negara dapat membangun sistem perlindungan data pribadi yang lebih kokoh

dan mampu mengimbangi perkembangan teknologi digital yang begitu cepat.

Tanpa pembentukan norma khusus, Indonesia akan terus berada pada posisi rentan di mana kebocoran data tidak hanya merugikan individu secara ekonomi dan psikologis, tetapi juga dapat mengancam stabilitas nasional, menurunkan kepercayaan publik, serta menghambat iklim investasi di sektor digital. Oleh karena itu, pembentukan norma hukum khusus bukan lagi sekadar pilihan, tetapi suatu keharusan untuk memastikan perlindungan hak privasi setiap warga negara secara efektif dan berkelanjutan.[29]

[29] Nabila,Annisa.Marlinaa.Leviza,Jelly, *Op.cit.* hal.18