

Aspek Hukum Pertanggungjawaban Pelaku dan Upaya Pemulihan Hak Korban Atas Kejahatan Doxing

Shofiyyah Mardiyah Hasya^{1*}, Akmal Muhammad Abdullah²,
Raden Maulana Damarjati³

¹⁻³Fakultas Hukum Universitas Padjadjaran, Indonesia

Email: shofiyyah21001@mail.unpad.ac.id¹, akmal21006@mail.unpad.ac.id², raden21007@mail.unpad.ac.id³

Jl. Raya Bandung Sumedang KM.21, Hegarmanah, Kec. Jatinangor, Kabupaten Sumedang

Korespondensi penulis: shofiyyah21001@mail.unpad.ac.id*

Abstract. *The Indonesian Government has legalized Law Number 11 of 2008 concerning Electronic Information and Transactions (and its amendments) ("ITE Law") and Law Number 27 of 2022 concerning Personal Data Protection ("PDP Law"). These laws were established to protect privacy rights from cybercrimes such as doxing. Doxing is defined as the unlawful access and dissemination of information with bad faith towards the victims. This cybercrime can create significant losses for the victim due to their personal information being revealed. Despite doxing being regulated under the ITE Law and PDP Law, the enforcement of these rules and reparations for the victims are challenging. To uphold the constitutional rights of Indonesian citizens, this article addresses the regulation and implications of liability in doxing, as well as the restoration of rights for doxing victims. The research method used in this article is a normative juridical approach. Therefore, doxing is regulated as a prohibition on the misuse of personal data under the PDP Law. Furthermore, victims are entitled to receive reparations for such acts.*

Keywords: *Doxing, Liability, Personal Data.*

Abstrak. Dalam perkembangannya, hak privasi di Indonesia telah diupayakan dalam penegakannya melalui pembentukan Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (dan perubahannya) ("UU ITE") dan Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi ("UU PDP"). Peraturan perundang-undangan tersebut ditujukan untuk melindungi hak privasi setiap orang dari tindakan kejahatan siber seperti doxing. Doxing adalah tindakan mengakses dan menyebarkan informasi secara tanpa hak dengan itikad buruk kepada korban. Hal ini merupakan kejahatan siber yang dapat memberikan dampak kerugian besar kepada korban terkait terungkapnya data pribadi mereka. Meskipun tindakan doxing telah diatur secara implisit dalam UU ITE dan UU PDP, namun penegakannya serta pemulihan hak korbannya cenderung sulit. Berdasarkan hal tersebut, permasalahan utama dalam artikel ini adalah pengaturan serta bentuk pertanggungjawaban dalam tindakan doxing dan pemulihan hak terhadap korban doxing. Metode penelitian yang diaplikasikan dalam artikel ini adalah pendekatan yuridis normatif. Maka dari itu, doxing telah diatur sebagai larangan penggunaan data pribadi sebagai bentuk dari ketentuan pidana menurut UU PDP. Selain itu, korban juga berhak untuk mendapatkan ganti kerugian yang dialaminya dari tindakan tersebut.

Kata kunci : Data Pribadi, Doxing, Pertanggungjawaban.

1. LATAR BELAKANG

Sejatinya, Pasal 28G Ayat (1) Undang-Undang Dasar Negara Republik Indonesia tahun 1945 telah menegaskan bahwa setiap orang memiliki hak untuk memperoleh perlindungan diri pribadi termasuk atas kehormatan dan martabatnya. Hal ini mengimplikasikan bahwa hukum nasional telah menjamin hak privasi bagi setiap orang, tetapi dengan perkembangan teknologi yang pesat saat ini, pelindungan data pribadi perlu diperhatikan sebagai bagian yang tidak terpisahkan dalam perlindungan privasi seseorang (Rosadi, 2015). Secara umum, konsep pelindungan data pribadi didasarkan pada dua bentuk, yakni pengamanan data pribadi

berdasarkan fisiknya dan pembentukan dasar hukum untuk penjaminan privasi terhadap data pribadinya (Djafar, dkk, 2016). Dalam perkembangannya, Pemerintah Indonesia telah mengupayakan bentuk yang kedua. Hal ini dilakukan pada awalnya dengan pembentukan regulasi perihal informasi elektronik yang secara implisit mengatur terkait data pribadi dalam Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik sebagaimana diubah terakhir dalam Undang-Undang Nomor 1 Tahun 2024 (“UU ITE”). Dengan kata lain, pengaturan mengenai perlindungan data pribadi melalui UU ITE sejatinya masih belum komprehensif mengingat dalam muatannya hanya memuat sebagian kecil terkait perlindungan data pribadi.

Akan tetapi, dengan berkembangnya kebutuhan terkait pengaturan hukum dalam hal perlindungan data pribadi yang dapat menjamin hak privasi setiap warga negara, kemudian dibentuklah Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi (“UU PDP”). Hal ini dapat diartikan sebagai salah satu langkah untuk menjamin hak privasi terhadap data pribadi seseorang dalam rangka memberikan perlindungan terhadap data pribadi dan setiap rangkaian pemrosesan data pribadi. Dalam hal ini, data pribadi dapat dipahami sebagai hak dan kewajiban yang melekat pada diri seseorang mengenai data yang mencakup data pribadi yang bersifat rahasia (Karo, 2020). Merujuk pada Pasal 1 angka 6 jo. angka 7 UU PDP, setiap orang perseorangan ataupun korporasi adalah bagian dari Subjek Data Pribadi yang berhak mendapatkan perlindungan tersebut. Maka dari itu, setiap warga negara Indonesia termasuk sebagai Subjek Data Pribadi yang telah dilindungi.

Pelindungan data pribadi termasuk hal yang harus diperhatikan dalam rangka menghindari ancaman kejahatan dunia maya, seperti penyerangan kepada aspek data pribadi seseorang (Dade dkk, 2024). Salah satu pelanggaran yang dapat terjadi dalam lingkup media digital adalah penyebaran data pribadi atau umumnya dikenal sebagai *doxing*. Pada dasarnya, *doxing* termasuk dalam tindakan *cybercrime* yang melibatkan aktivitas pengumpulan data pribadi seseorang yang kemudian disebar atau dipublikasikan tanpa persetujuan dari pemilik data pribadinya. Dalam penerapannya, *doxing* tidak hanya sebatas mengungkapkan data pribadi seseorang di ruang publik, tetapi juga disertai dengan berbagai ancaman untuk mengintimidasi korban (Dade dkk, 2024). Berdasarkan hal tersebut, *doxing* umumnya dilakukan dengan bentuk unggahan yang mengandung data pribadi seseorang baik berupa video, foto maupun narasi-narasi kontroversial yang dimaksudkan untuk menggiring opini negatif terhadap korban *doxing*.

Tindakan *doxing* merupakan salah satu konsekuensi dari pemanfaatan kemajuan teknologi yang tidak digunakan secara bijak. Semakin berkembangnya jenis kejahatan, maka sudah sepatutnya Pemerintah menciptakan regulasi yang dapat memberikan jaminan ruang aman dengan melindungi hak privasi individu, termasuk mengatur terkait dengan tindakan *doxing*. Selain ketentuan mengenai perlindungan data pribadi, Pasal 26 UU ITE juga mengatur pengaturan terkait tindakan *doxing* sebagai tindak pidana, yakni pada Pasal 32 Ayat (3) UU ITE jo. Pasal 48 Ayat (3) UU ITE. Selain itu, UU PDP juga mengatur secara lebih lengkap mengenai berbagai ketentuan terkait dengan perlindungan data pribadi, termasuk perlindungan terhadap kejahatan *doxing*, yakni dalam Pasal 67 Ayat (2) UU PDP. Dengan diundangkannya UU PDP, perlu ditegaskan bahwa hal ini tidak mencabut ketentuan yang berkenaan dengan perlindungan data pribadi dalam peraturan lain seperti UU ITE sepanjang tidak bertentangan dengan UU PDP.

Praktik *doxing* dapat mengakibatkan konsekuensi bagi korban, seperti menimbulkan rasa takut, kecemasan, rusaknya reputasi, pencurian identitas, dan lain sebagainya yang dapat merugikan korban. Selain itu, tindakan *doxing* dapat berpengaruh terhadap kehidupan nyata korban yang menimbulkan potensi terjadinya teror secara fisik. Sebagai contoh, ketika alamat lengkap dari korban tersebut diungkapkan, maka dapat memicu pihak tertentu untuk mendatangi, mengepung, ataupun tindakan lainnya yang mengancam keamanan korban. Hal ini memiliki implikasi terhadap timbulnya kerugian secara materiil dan immateriil (Widigdo dan Rosando, 2023). Maka dari itu, korban dari *doxing* seharusnya diberikan perlindungan yang pasti beserta dengan pemulihannya sebagai bentuk pemenuhan hak konstitusional.

Dalam penerapannya, kerugian yang diakibatkan dari tindakan *doxing* sejatinya sulit untuk diukur mengingat kerugian yang dirasakan korban dapat lebih signifikan daripada kerugian ekonomi karena tindakan tersebut telah merugikan kehidupan pribadi korban. Sebagai contoh, dampak dari tindakan *doxing* berupa materiil seperti tempat tinggal yang didatangi orang tidak dikenal hingga immateriil seperti mendapatkan ancaman melalui pesan langsung dan panggilan telepon dari nomor yang tidak diketahui yang berpotensi mempengaruhi keamanan jiwa maupun batin korban. Meskipun begitu, korban dari kejahatan tersebut sejatinya berhak untuk menerima pemulihan hak, seperti penerimaan ganti kerugian. Berdasarkan hal tersebut, pengaturan hukum yang memuat pemulihan terhadap hak-hak Subjek Data Pribadi dapat dikatakan sebagai hal yang sangat penting guna memberikan kepastian hukum bagi korban tindakan *doxing*. Akan tetapi, terdapat kekosongan hukum mengenai regulasi yang mengatur lebih lanjut terkait penilaian dan dasar pembuktian unsur

kerugian dalam pelanggaran data pribadi sehingga dapat menyebabkan timbulnya hambatan bagi penegakan hukum kejahatan *doxing*.

Salah satu kasus yang relevan dengan permasalahan yang penulis kaji dalam artikel ini terjadi pada tahun 2020 terhadap Denny Siregar sebagai seseorang yang aktif dalam sosial media *twitter* telah menjadi korban dari tindakan *doxing* (Baihaiqi, 2024). Hal ini diketahui ketika ia menemukan data pribadinya yang berupa nama, alamat, nomor telepon, hingga data perangkat yang digunakannya telah disebar oleh akun anonim @*Opposite6891*. Tindakan ini dilakukan dengan mendapatkan data pribadi milik Denny Siregar oleh Febriansyah (pelaku) sebagai salah satu pegawai dari GraPari Telkomsel Surabaya yang memperoleh data pelanggan dari perusahaan untuk diberikan dan disebar oleh akun tersebut. Meskipun pelaku telah dijerat dengan Pasal 48 Ayat (3) jo. Pasal 32 Ayat (3) UU ITE hingga divonis hukuman pidana 8 bulan penjara dan denda sebesar Rp2.000.000,00 (dua juta rupiah), pemulihan hak korban yang diderita oleh Denny Siregar perlu diperhatikan. Hal ini dikarenakan sebelum adanya putusan pidana tersebut, Denny Siregar telah mengajukan gugatan perbuatan melawan hukum kepada PT. Telekomunikasi Seluler (Tergugat I) dan Febriansyah (Tergugat II), beserta tergugat lainnya yang berkaitan dengan tuntutan ganti rugi kerugian moril yang dialami olehnya sebesar Rp1.000.000.000.000.- (1 triliun rupiah) hingga publikasi permohonan maaf secara publik atas peristiwa tersebut. Meskipun gugatannya telah dicabut, hal tersebut menunjukkan bahwa kerugian dari tindakan *doxing* yang dialami oleh korban merupakan hal yang sangat krusial. Berdasarkan hal tersebut, maka analisis terhadap pemulihan hak-hak korban dari tindakan *doxing* perlu dilakukan atas dasar kekosongan hukum yang ada terhadap peraturan yang secara khusus mengenai hal tersebut.

2. KAJIAN TEORITIS

Doxing merupakan tindakan mengakses dan menyebarkan informasi secara tanpa hak dengan niatan buruk dalam rangka mengancam, mengintimidasi, dan mempermalukan korban melalui sistem elektronik (Kamarulzaman dan Yusuf, 2024). Terdapat tiga jenis tindakan *doxing* sebagai salah satu bentuk dari kejahatan siber. Pertama, *doxing deanonymizing* yang berarti tindakannya dilakukan dengan tujuan mengungkap jenis informasi secara terperinci untuk melakukan pemprofilan terhadap identitas anonim atau *pseudonim* seseorang dengan identitas aslinya. Kedua, *doxing targeting* yang dilakukan dengan cara pengungkapan informasi pribadi seseorang yang dapat dianalisis untuk menunjukkan keberadaan seseorang secara fisik, misalkan alamat rumah dan tempat kerja seseorang. Ketiga, *doxing delegitimizing* yang dilakukan untuk mengungkap suatu informasi tertentu yang dapat digunakan untuk

merendahkan atau menghancurkan kredibilitas, serta martabat seseorang. Maka dari itu, tindakan *doxing* yang sedang marak terjadi di dunia siber Indonesia telah menjadi suatu isu penting dalam era digital saat ini (David M. Douglas, 2016).

Seseorang yang menjadi korban *doxing* umumnya akan merasakan ketakutan, kecemasan, rusaknya reputasi, serta hal-hal lain akibat data pribadi miliknya terungkap. Sekalipun *doxing* termasuk ke dalam kejahatan siber, artinya terjadi melalui dunia digital, tetapi kerugian yang ditimbulkan dapat dirasakan hingga dunia fisik. Sebagai contoh, alamat rumah seseorang yang diungkap dapat mengakibatkan korban merasa tidak aman, sebab sewaktu-waktu sangat mungkin akan mendapatkan teror secara fisik. Hal ini berdampak pula pada psikis korban yang akan mengalami paranoid terhadap lingkungannya (Uweng, dkk, 2023). Maka dari itu, korban *doxing* tidak dapat dipahami sebatas sebagai orang yang informasi pribadinya diungkap sehingga dapat diakses oleh orang lain semata, sebab terdapat dampak lain yang akan ditimbulkan akibat terungkapnya data pribadi milik korban.

Permasalahan *doxing* memiliki kaitan erat dengan hak privasi individu karena adanya kerentanan terhadap pelanggaran data pribadi. Permasalahan tersebut telah menjadi suatu isu internasional hingga dibentuknya hukum *General Data Protection Regulation 2016* (“**GDPR**”) oleh Uni Eropa. Meskipun keberlakuan GDPR diperuntukkan untuk negara-negara Uni Eropa, tetapi muatannya banyak diadopsi oleh berbagai negara termasuk Indonesia. UU PDP banyak mengadopsi ketentuan-ketentuan di dalam GDPR, seperti mengenai dasar pemrosesan data pribadi, hak Subjek Data Pribadi, dan juga pengaturan yang berkaitan dengan tindakan *doxing*. Keberadaan UU PDP di Indonesia menjadi salah satu terobosan baru bagi tatanan sistem hukum nasional karena diharapkan menjadi payung hukum yang kuat untuk memberi perlindungan data pribadi.

Lebih lanjut, tindakan *doxing* merupakan salah satu bentuk kejahatan sehingga dapat dikenakan sanksi pidana terhadapnya. Hal ini dikarenakan tindakan tersebut dapat mengakibatkan seseorang merasa tidak nyaman serta menimbulkan rasa terintimidasi akibat terungkap data pribadi miliknya. Atas dasar hal tersebut, penanganan kasus *doxing* tidak cukup hanya dengan menjatuhkan sanksi pidana terhadap pelaku, tetapi juga harus memperhatikan aspek pemulihan hak korban yang dirugikan (Dade, dkk, 2024). Di Indonesia, tindakan *doxing* telah diatur dalam UU PDP mengenai larangan tindakannya, hingga ketentuan pidananya. Namun, dalam praktiknya efektivitas mengenai penegakan hukum dalam kasus *doxing* masih kurang optimal (Nugraha & Saputra, 2024). Hal ini dikarenakan kerangka hukum yang berlaku saat ini belum mengatur secara eksplisit mengenai tindakan *doxing* serta hak-hak bagi korban dari tindakan tersebut untuk pemulihannya.

Pada dasarnya, dalam kasus kejahatan *doxing* terdapat sejumlah hak korban sebagai Subjek Data Pribadi yang telah dilanggar sehingga dibutuhkan adanya pemulihan hak terhadap korban yang dirugikan atas kejahatan tersebut. Pemulihan hak korban merupakan hal yang sangat diperlukan mengingat tindakan *doxing* akan mempengaruhi reputasi nama baik dari Subjek Data Pribadi karena mendapatkan penghinaan, rasa malu, hingga pelecehan yang menyerang martabat korban sehingga sulit untuk dipulihkan (Syailendra, Moody Rizqi, dkk, 2024). Lebih lanjut, pemberian hak-hak pemulihan bagi korban dapat dilakukan untuk menciptakan ruang lingkup terhadap tindakan *doxing* itu sendiri sehingga dapat menjadi tolak ukur untuk melaksanakan kategorisasi tindakan *doxing* dalam penegakannya melalui UU PDP. Tolak ukur ini dapat dikaji berdasarkan unsur-unsurnya, seperti identifikasi Subjek Data Pribadi yang jelas, persetujuan Subjek Data Pribadi, dan niat pelaku dalam tindakannya (Yusuf, 2024). Sebagai contoh, tolak ukur pertama untuk mengkategorisasikan *doxing* sebagai pelanggaran ketentuan pidana dalam UU PDP adalah legalitasnya dalam proses pengumpulan data.

Berdasarkan Pasal 20 Ayat (1) jo. Ayat (2) UU PDP, pengumpulan data harus dilakukan dengan sah menurut hukum dan juga atas dasar persetujuan secara eksplisit dari seseorang yang datanya diproses. Selain itu, niat pelaku juga dapat mendukung pengklasifikasian tindakan *doxing*. Dalam melakukan tindakan tersebut, pelaku harus memiliki niat meskipun tidak terbatas pada menyakiti, memermalukan, atau merugikan individu yang data pribadinya disebar. Jika mengacu kepada dua tolak ukur tersebut, maka tolak ukur terakhir adalah untuk menghitung dampak kerugian yang dialami korban untuk menindak pelaku tersebut dan juga menentukan hak-hak korban yang dapat dipulihkan melalui ganti kerugian atau cara-cara lainnya berdasarkan peraturan perundang-undangan.

Penelitian mengenai *doxing* dan perlindungan data pribadi telah banyak ditulis oleh penulis-penulis terdahulu sehingga penting untuk menentukan daya pembeda dari penelitian kali ini. Sebagai perbandingan, artikel dalam jurnal yang ditulis oleh Intan Saripa Uweng dan kawan-kawan, serta terbit pada tahun 2023 berjudul “Perlindungan Hukum Pidana Terhadap *Doxing* Menurut Undang-undang Informasi dan Transaksi Elektronik”, membahas mengenai perlindungan hukum bagi korban tindak pidana *doxing*. Namun, dalam tulisan tersebut tidak diuraikan mengenai pemulihan hak korban, melainkan sebatas sanksi pidana bagi pelaku *doxing*. Selain itu, kajian yang dibuat menggunakan UU ITE sebagai dasar hukumnya, sementara dalam tulisan ini akan lebih berfokus pada hak-hak korban *doxing* berdasarkan UU PDP serta aturan lain yang terkait. Dengan demikian, melalui artikel ini penulis akan menganalisis dan membahas dua pokok permasalahan, yaitu pertanggungjawaban pelaku

doxing ditinjau berdasarkan Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi dan upaya pemulihan hak-hak korban yang mengalami kejahatan *doxing*.

3. METODE PENELITIAN

Penulis mengaplikasikan metode penelitian dengan pendekatan yuridis normatif melalui kegiatan pengkajian terhadap regulasi yang berlaku dan relevan dengan pembahasan artikel ini. Penulis mengumpulkan dan menggunakan bahan hukum primer maupun sekunder. Dalam hal ini, bahan hukum primer yang digunakan mencakup peraturan perundang-undangan, sedangkan bahan hukum sekunder yang dijadikan acuan meliputi rujukan tertulis lainnya, seperti buku, jurnal, maupun rujukan elektronik lainnya yang sesuai dan berkaitan dengan permasalahan mengenai pertanggungjawaban pelaku maupun upaya pemulihan korban dari kejahatan *doxing*. Lebih jelasnya, dalam membahas artikel ini penulis menggunakan pendekatan yuridis normatif dengan menganalisis UU PDP dikaitkan dengan isu mengenai pertanggungjawaban pelaku *doxing*. Selain itu, untuk membahas upaya pemulihan hak korban dari kejahatan *doxing* penulis juga menerapkan pendekatan yuridis normatif dengan menganalisis ketentuan dalam UU PDP maupun UU ITE.

4. HASIL DAN PEMBAHASAN

1. Pertanggungjawaban Pelaku Doxing ditinjau berdasarkan Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi

Secara umum, terdapat tiga ketentuan dalam UU PDP yang relevan untuk mengkaji pengaturan tindakan *doxing*, yakni jenis data pribadi, hak Subjek Data Pribadi, dan ketentuan pidana. Pertama, jenis data pribadi. Mengacu pada Pasal 4 UU PDP, sejatinya data pribadi mencakup 2 (dua) jenis sesuai dengan sifatnya, yakni data spesifik dan data umum. Sebagai contoh, data spesifik adalah data yang berupa informasi kesehatan, data biometrik, dan/atau data lainnya yang disebutkan dalam Pasal 4 Ayat (2) UU PDP. Berbeda dengan hal tersebut, data umum adalah data yang secara sifatnya dapat diketahui secara umum seperti nama lengkap, jenis kelamin dan/atau data lainnya yang dapat digunakan untuk mengenali atau mengidentifikasi seseorang sebagaimana diuraikan dalam Pasal 4 Ayat (3) UU PDP. Perbedaan kedua jenis data tersebut dibuat atas dasar adanya dampak yang lebih besar jika suatu data yang bersifat spesifik milik seseorang tersebar. Hal ini dikarenakan pemrosesan terhadap data pribadi seseorang yang bersifat spesifik memiliki potensi risiko tinggi sehingga pelaksanaannya perlu dilakukan terlebih dahulu terkait penilaian dampak pelindungan data pribadi tersebut.

Kedua, berkenaan dengan sejumlah hak dari Subjek Data Pribadi. Pemilik data pribadi yang dimaksud dalam UU PDP adalah setiap orang yang terikat dengan data pribadinya atau disebut sebagai ‘Subjek Data Pribadi’. Adapun hak Subjek Data Pribadi yang berkaitan dengan *doxing*, yaitu hak untuk menggugat dan memperoleh ganti rugi atas terjadinya pelanggaran pemrosesan data pribadi milik dirinya sebagaimana diuraikan dalam Pasal 12 Ayat (1) UU PDP. Selain itu, dalam hal terjadinya tindak pidana, maka Subjek Data Pribadi berhak memperoleh pembayaran ganti rugi sebagaimana diatur dalam Pasal 69 UU PDP. Oleh karena itu, hak Subjek Data Pribadi telah dijamin dalam UU PDP dan jika mengalami kerugian atas tindakan *doxing* dari orang lain, maka ia berhak untuk mendapatkan ganti rugi dari peristiwa tersebut.

Ketiga, yaitu ketentuan pidana. Sejatinya tindak pidana *doxing* diatur dalam Pasal 67 Ayat (1) jo. Ayat (2) UU PDP. Pada pokoknya, pasal ini mengatur terkait ketentuan pidana yang diberlakukan terhadap setiap aktivitas yang berkaitan dengan data pribadi seseorang. Dalam hal ini, tindakan *doxing* dilakukan dengan cara mengumpulkan suatu informasi atau data pribadi seseorang dan disebarkannya data tersebut melalui internet (Kamarulzaman & Yusuf, 2024). Hal ini selaras dengan larangan penggunaan data pribadi dalam Pasal 65 Ayat (1) jo. Ayat (2) UU PDP, yakni “mengumpulkan” data pribadi bukan miliknya secara melawan hukum dan “mengungkapkan” data pribadi tersebut. Adanya pengaturan ini merupakan bentuk perlindungan hak Subjek Data Pribadi dalam rangka menghindari pelanggaran terhadap data pribadi yang dapat merugikannya. Pengaturan ketentuan pidana yang diatur dalam UU PDP pada dasarnya diterapkan dalam rangka melindungi privasi individu sehingga hanya dapat dikenakan bagi pelaku pengungkapan data pribadi orang perseorangan. Penyalahgunaan data pribadi untuk kegiatan di luar dari tujuan data tersebut diberikan dapat diselesaikan melalui hukum administrasi negara maupun secara perdata, dan pidana (Munir, 2017).

Dalam hal terjadi tindakan *doxing* yang melibatkan kesalahan pihak lain di luar orang perseorangan, UU PDP juga memberikan ketentuan terkait pertanggungjawaban yang dapat dijatuhkan kepada Pengendali dan/atau Prosesor Data Pribadi. Tindakan pengumpulan dan pengungkapan data pribadi merupakan dua diantara beberapa bentuk kegiatan pemrosesan data pribadi sehingga dalam melakukan pemrosesan tersebut wajib mengacu pada dasar pemrosesan data pribadi yang ditentukan pada Pasal 20 Ayat (2) UU PDP. Dalam tindakan *doxing* tentunya pengungkapan data pribadi dilakukan tidak disertai dengan adanya dasar pemrosesan data pribadi sehingga perbuatan tersebut diklasifikasikan sebagai perbuatan yang ilegal.

Pada umumnya, data pribadi digunakan sebagai syarat untuk dapat mengakses layanan media digital. Hal ini menimbulkan kerentanan akan keamanan data pribadi pengguna jika Pengendali dan Prosesor Data Pribadi tidak melakukan kewajibannya untuk melakukan upaya-upaya perlindungan (Dade dkk, 2024). Pemrosesan data pribadi yang dilakukan oleh Pengendali Data Pribadi dapat dialihkan kepada pihak lain, yaitu Prosesor Data Pribadi dengan mekanisme penunjukkan. Merujuk pada Pasal 51 Ayat (6) UU PDP, tindakan yang dilakukan Prosesor Data Pribadi akan menjadi tanggung jawab dari Pengendali Data Pribadi sepanjang tindakannya tidak bertentangan dengan perintah dari Pengendali Data Pribadi.

Merujuk pada Pasal 57 UU PDP, apabila Pengendali Data Pribadi melakukan pelanggaran atas kewajiban-kewajibannya, maka terdapat sejumlah sanksi administratif yang dapat diberikan. Selain itu, Pengendali Data Pribadi berbentuk korporasi juga dapat dijatuhkan sanksi pidana beserta dengan pidana tambahan yang diatur dalam Pasal 70 Ayat (4) UU PDP. Maka dari itu, berdasarkan UU PDP, setiap orang perorangan maupun korporasi dapat dibebankan pertanggungjawaban dari sanksi administratif, gugatan perdata, hingga hukuman pidana. Relevan dengan hal tersebut, perlu diperhatikan bahwa tidak terdapat ketentuan yang menegaskan adanya penerapan secara terpisah ataupun pengenaan sanksi yang didahulukan dalam hal terjadinya pelanggaran data pribadi (Subhan & Muttaqihlm 2024).

Apabila dipahami lebih lanjut, terdapat persamaan maupun perbedaan antara tindakan doxing yang dapat dikenakan terhadap pelaku individu maupun korporasi sebagai Pengendali dan/atau Prosesor Data Pribadi. Dalam lingkup persamaan, baik individu maupun korporasi tersebut dapat dikenakan pertanggungjawaban baik secara administratif, perdata dan/atau pidana disesuaikan dengan ketentuan yang dilanggarnya. Perbedaan dalam hal pertanggungjawabannya jika pelaku tersebut adalah korporasi, maka terdapat pidana tambahan yang dapat dikenakan terhadapnya berupa perampasan kekayaan untuk pemberian ganti kerugian kepada korban. Berbeda dengan keadaan apabila pelakunya adalah individu maka tidak dapat dikenakan pidana tambahan tersebut.

2. Upaya Pemulihan Hak-Hak Korban yang Mengalami Kejahatan Doxing

Terdapat sejumlah ketentuan mengenai upaya yang dapat ditempuh oleh korban untuk memulihkan hak-haknya sebagaimana diatur dalam UU PDP. Salah satu bentuk pemulihan yang dapat diperoleh Subjek Data Pribadi adalah penerimaan ganti kerugian sebagaimana diamanatkan dalam Pasal 12 Ayat (1) UU PDP. Ketentuan tersebut menegaskan bahwa dalam hal terjadinya pelanggaran pemrosesan data pribadi, maka Subjek Data Pribadi berhak memperoleh ganti kerugian dengan mengajukan gugatan. Dalam hal ini, perlu dicatat bahwa penerapan ketentuan tersebut belum dapat diterapkan secara efektif selama belum disahkannya

Peraturan Pemerintah (“PP”) yang mengatur mengenai pemenuhan ganti kerugian sebagai peraturan turunan dari UU PDP (Rosadi, 2023).

Selain itu, salah satu dampak yang dapat terjadi kepada korban *doxing* adalah ancaman langsung terhadap kediamannya. Dalam hal ini, korban dapat meminta perlindungan dari Lembaga Perlindungan Saksi dan Korban (“LPSK”) yang dapat memberikan ‘rumah aman’ sementara serta bantuan rehabilitasi psikososial sebagaimana diatur dalam Pasal 1 angka 8 dan Pasal 12A Undang-Undang Nomor 31 Tahun 2014 tentang Perubahan atas Undang-Undang Nomor 13 Tahun 2006 tentang Perlindungan Saksi dan Korban. Perlindungan tersebut dapat membantu korban untuk bisa memulihkan keadaannya secara fisik maupun psikis atas hasil dari tindakan *doxing* yang menimpanya.

Dalam hal ini, terdapat 3 (tiga) mekanisme penuntutan ganti kerugian yang sejatinya dapat diajukan oleh Subjek Data Pribadi, yakni secara administratif, perdata dan pidana (Rosadi, 2023). Segala bentuk sanksi administratif dapat dijatuhkan oleh lembaga yang seharusnya dibentuk paling lambat dua tahun pasca pengesahan UU PDP. Selain itu, penuntutan ganti kerugian secara perdata dapat dilakukan diluar pengadilan dan/atau pengadilan sedangkan tuntutan ganti rugi secara pidana hanya dapat diajukan melalui mekanisme pengadilan saja.

Dalam lingkup penyelesaian secara perdata, Subjek Data Pribadi berhak memperoleh ganti kerugian dengan mengajukan gugatan Perbuatan Melawan Hukum (“PMH”) sesuai Pasal 1365 KUHPperdata. Sejatinya, PMH memiliki 4 (empat) unsur yang wajib untuk dipenuhi, yakni perbuatan melawan hukum, kesalahan, kerugian, dan kausalitas antara perbuatan dengan kerugian yang timbul (Sari, 2020). Dalam lingkup PMH, pelanggaran terhadap Pasal 65 dan Pasal 66 UU PDP dapat dijadikan sebagai dasar gugatan untuk meminta ganti rugi kepada Pelaku melalui pengadilan. Berdasarkan Pasal 64 Ayat (1) UU PDP, selain melalui pengadilan, gugatan ganti rugi secara perdata juga dapat dimintakan melalui mekanisme arbitrase maupun alternatif penyelesaian sengketa sebagai pilihan bagi Subjek Data Pribadi untuk memulihkan hak-haknya yang telah dirugikan.

Selanjutnya, mekanisme secara pidana untuk pemulihan korban berupa penerimaan ganti kerugian. Pembayaran ganti kerugian menjadi bagian salah satu bentuk pidana tambahan yang dapat dijatuhkan oleh hakim melalui putusannya kepada Pelaku tindak pidana. Merujuk pada Pasal 69 UU PDP ditegaskan bahwa Pelaku juga dapat dikenakan pidana tambahan melalui perampasan keuntungan atas tindak pidana tersebut dan pembayaran ganti kerugian bagi Subjek Data Pribadi selaku korban. Selanjutnya, dalam Pasal 70 Ayat (4) UU PDP diatur bahwa terhadap tindak pidana pelanggaran data pribadi oleh korporasi, selain dijatuhi pidana

pokok, terdapat pidana tambahan dalam bentuk pengenaan pembayaran ganti kerugian kepada subjek data yang dirugikan sebagai upaya pemulihan hak korban.

Perlu diperhatikan bahwa meskipun UU PDP telah memberikan hak bagi Subjek Data Pribadi untuk mengajukan tuntutan ganti kerugian dalam hal terjadinya pelanggaran data pribadi, tetapi sampai saat ini belum terdapat regulasi yang merinci terkait penilaian besaran ganti rugi yang dapat diperoleh subjek data. Hal ini berkaitan dengan PP turunan dari UU PDP yang mengatur lebih lanjut terkait hal tersebut dan mengenai hak Subjek Data Pribadi dalam memperoleh ganti kerugian belum disahkan hingga saat ini. Oleh karena itu, selama belum disahkan PP tersebut maka penilaian besaran ganti kerugian sepenuhnya bergantung pada penilaian dari hakim yang memutus perkara tersebut.

Sekalipun pemulihan dalam bentuk ganti kerugian dapat diperoleh Subjek Data Pribadi yang telah dirugikan akibat *doxing*, tetapi hal tersebut tidak langsung menyelesaikan permasalahan mengenai data pribadi yang telah diungkap. Kemajuan teknologi saat ini berdampak pada lalu lintas informasi dan data yang kian cepat tanpa terbatas oleh ruang dan waktu. Berdasarkan hal tersebut, maka disamping adanya pemulihan berupa pembayaran ganti kerugian terhadap korban, diperlukan juga bentuk pemulihan lain sebagai upaya menghentikan penyebaran data pribadi yang telah diungkap akibat tindakan *doxing*. Berdasarkan Pasal 8 UU PDP, bentuk pemulihan tersebut dapat dikaitkan dengan hak Subjek Data Pribadi untuk menghapus dan/atau memusnahkan data pribadi miliknya. Terkait hal ini, Pasal 43 Ayat (1) huruf b UU PDP juga memberikan kewajiban bagi Pengendali Data Pribadi untuk menghapus data pribadi yang persetujuan pemrosesannya telah ditarik oleh Subjek Data Pribadi. Hak ini merupakan bentuk penerapan *right to be forgotten* (“**RTBF**”) dalam GDPR yang dapat dimaknai sebagai hak untuk mengajukan penghapusan data pribadi miliknya.

Pada dasarnya, RTBF adalah hak yang dimiliki oleh individu agar tidak bisa dilacak oleh pihak ketiga sebagai bentuk perlindungan terhadap data pribadinya, termasuk juga sebagai bentuk penegakkan hak atas privasi seorang individu (Yudiana, dkk 2022). Hak ini dapat diterapkan untuk membantu setiap individu yang terdampak dari tindakan *doxing* dan juga melindungi data-data pribadinya yang secara melawan hukum disebarkan melalui internet. Secara umum, dalam menerapkan hak ini, Subjek Data Pribadi dapat mengajukan permohonan kepada Pengendali Data Pribadi untuk menghapus suatu data pribadinya yang dianggap merugikannya. Secara historis, konsep RTBF pertama kali diajukan sebagai hak mendasar dalam perlindungan data pribadi di Uni Eropa yang memberikan kesempatan bagi Subjek Data Pribadi untuk menghapus data pribadi miliknya di internet (Hutapea, 2021). Munculnya konsep hak tersebut diawali pada tahun 2014 ketika Court of Justice European Union (CJEU)

menjatuhkan putusan terkait kasus Costeja. Dalam kasus tersebut, majelis hakim mengabulkan tuntutan Costeja sebagai pemohon untuk menghapus seluruh tautan yang memuat data pribadinya.

Pada dasarnya, penghapusan data pribadi dapat dilakukan apabila Subjek Data Pribadi mencabut persetujuan pemrosesan datanya, terdapat permohonan dari Subjek Data Pribadi, dan pemrosesan data dilakukan secara ilegal. Selain berdasarkan permohonan Subjek Data Pribadi, RTBF dapat diterapkan melalui penjatuhan sanksi administratif. Berdasarkan Pasal 57 Ayat (2) UU PDP, salah satu bentuk sanksi administratif yang dapat diterapkan kepada Pengendali dan/atau Prosesor Data Pribadi akibat pelanggaran terhadap kewajibannya adalah penghapusan atau pemusnahan data pribadi. Lebih lanjut, Pasal 60 huruf c UU PDP memberikan mandat kepada Pemerintah untuk membentuk lembaga yang memiliki kewenangan dalam memberikan sanksi administratif ketika terjadi pelanggaran terkait perlindungan data pribadi oleh Pengendali maupun Prosesor Data Pribadi. Selama lembaga tersebut belum dibentuk oleh Pemerintah maka penjatuhan sanksi administratif tidak dapat dilaksanakan. Hal ini dapat menjadi hambatan dalam pemulihan hak korban tindakan *doxing* apabila hingga ketentuan dalam UU PDP berlaku sepenuhnya masih belum terdapat lembaga untuk menjalankan kewenangan tersebut.

Secara garis besar, implementasi dari RTBF dapat dikatakan sebagai suatu jalan keluar bagi Subjek Data Pribadi yang menginginkan data pribadinya untuk dihapuskan guna menghindari timbulnya kerugian serta melindungi keselamatan maupun reputasinya. Konsep tersebut memberikan dampak positif terhadap hak privasi di tengah masifnya pemanfaatan teknologi saat ini mengingat Subjek Data Pribadi memiliki peran untuk mengontrol penyebaran data pribadi miliknya di dunia maya (Yudiana, 2022). Tentunya agar konsep demikian dapat berjalan secara efektif, diperlukan adanya kesadaran masyarakat akan pentingnya melindungi privasinya sendiri. Dalam rangka memperoleh hak untuk dilupakan, Subjek Data Pribadi harus mengajukan permohonan kepada Pengendali Data Pribadi secara elektronik ataupun non-elektronik agar data pribadi miliknya dihapuskan sebagaimana diuraikan dalam Pasal 14 UU PDP. Namun, hingga kini masih belum terdapat peraturan turunan dari UU PDP, termasuk pengaturan secara spesifik mengenai pelaksanaan RTBF sebagai bentuk pemulihan hak bagi korban atas tindakan *doxing*.

Ketiadaan lembaga yang dimaksudkan dalam UU PDP guna menegakkan RTBF pun dapat menjadi salah satu hambatan. Hal ini menimbulkan kesulitan bagi korban *doxing* untuk menuntut agar data pribadi miliknya yang telah diakses dan diungkap oleh pelaku dapat dihapuskan. Meskipun begitu, disamping penerapan RTBF melalui lembaga tersebut, sejatinya

Subjek Data Pribadi dapat mengajukan permohonan penghapusan data pribadi melalui pengadilan sebagaimana diuraikan dalam Pasal 26 ayat (3) UU ITE. Berdasarkan ketentuan tersebut, terdapat kewajiban bagi Penyelenggara Sistem Elektronik untuk menghapus informasi elektronik berdasarkan permintaan pihak yang bersangkutan dengan penetapan pengadilan. Dengan demikian, implementasi dari RTBF sebagai bentuk pemulihan hak korban korban yang mengalami kejahatan *Doxing* dapat diterapkan melalui lembaga yang dibentuk berdasarkan UU PDP maupun penetapan pengadilan.

5. KESIMPULAN DAN SARAN

Dalam UU PDP diatur mengenai pertanggungjawaban dari pelaku *doxing* yang dapat dikenakan sanksi pidana sebagaimana diatur dalam Pasal 65 ayat (1) jo. ayat (2) UU PDP. Di samping tanggung jawab secara pidana, terhadap pelaku *doxing* juga dapat dimintakan sanksi administratif dan perdata. Pengendali Data Pribadi berbentuk korporasi juga dapat dijatuhkan sanksi pidana beserta dengan pidana tambahan yang diatur dalam Pasal 70 Ayat (4) UU PDP. Akan tetapi, penyelesaian kasus *doxing* tidak terbatas pada penjatuhan sanksi terhadap pelaku, tetapi perlu diperhatikan pula aspek pemulihan hak korban yang dirugikan. Salah satu bentuk pemulihan yang dapat diperoleh Subjek Data Pribadi adalah penerimaan ganti kerugian sebagaimana diamanatkan dalam Pasal 12 Ayat (1) UU PDP melalui pengajuan gugatan. Namun, ketentuan tersebut belum dapat diterapkan secara efektif dikarenakan belum disahkannya PP yang mengatur perihal pemenuhan ganti kerugian sebagai peraturan turunan dari UU PDP. Terdapat 3 (tiga) mekanisme penuntutan ganti kerugian yang dapat diajukan oleh Subjek Data Pribadi, yakni secara administratif, perdata dan pidana. Di samping pemulihan dalam bentuk ganti rugi, Subjek Data Pribadi juga memiliki hak untuk dilupakan atau RTBF agar data milik korban dimusnahkan sehingga tidak dapat dilacak oleh pihak ketiga. Di samping itu, *doxing* juga dapat menimbulkan dampak ancaman secara fisik, seperti adanya ancaman terhadap kediaman korban. Dalam hal ini, korban dapat meminta perlindungan dari LPSK yang dapat memberikan ‘rumah aman’ sementara serta bantuan pemulihan psikososial.

Berdasarkan kesimpulan tersebut penulis mengharapkan bahwa pemerintah harus segera dibuat peraturan turunan dari UU PDP yang mengatur secara jelas mengenai mekanisme pemberian *right to be forgotten* berdasarkan permohonan Subjek Data Pribadi. Lebih lanjut, Pemerintah juga harus segera membentuk lembaga sebagaimana diamanatkan dalam UU PDP agar terdapat kepastian hukum mengenai lembaga yang berwenang dalam menjatuhkan sanksi administratif kepada Pengendali dan Prosesor Data Pribadi, termasuk penjatuhan sanksi untuk

melakukan penghapusan atau pemusnahan data pribadi sebagai bentuk pemenuhan *right to be forgotten* bagi korban.

DAFTAR REFERENSI

Buku

- Djafar, W., et al. (2016). *Perlindungan data pribadi di Indonesia: Usulan pelebagaan kebijakan dari perspektif hak asasi manusia*. Jakarta: Lembaga Studi dan Advokasi Masyarakat (ELSAM).
- Karo, R. (2020). *Pengaturan perlindungan data pribadi di Indonesia: Perspektif teori keadilan bermanfaat*. Bandung: Nusa Media.
- Munir, N. (2017). *Pengantar hukum siber Indonesia* (Edisi ketiga). Depok: Rajagrafindo Persada.
- Rosadi, S. D. (2015). *Aspek data privasi menurut hukum internasional, regional, dan nasional*. Bandung: Refika Aditama.
- Rosadi, S. D. (2023). *Pembahasan UU Perlindungan Data Pribadi (UU RI No. Tahun 2022)*. Jakarta Timur: Sinar Grafika.

Jurnal

- Dade, L. L., et al. (2024). Kajian yuridis tentang tindak pidana penyebaran data pribadi melalui internet (doxing) di Indonesia. *Lex Privatum*, 13(3). <https://ejournal.unsrat.ac.id/v3/index.php/lexprivatum/article/view/54687>
- Douglas, D. M. (2016). Doxing: A conceptual analysis. *Ethics and Information Technology*, 18(3). <https://doi.org/10.1007/s10676-016-9406-0>
- Hutapea, S. A. (2021). Right to be forgotten sebagai bentuk rehabilitasi bagi korban pelanggaran data pribadi. *Jurnal Jurisprudencia*, 4(1). <https://jurisprudencia.bunghatta.ac.id/index.php/jurisprudencia/article/view/3>
- Kamarulzaman, M. S., & Yusuf, H. (2024). Analisis yuridis tindakan kriminal doxing ditinjau berdasarkan Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi. *Jurnal Intelek dan Cendekiawan Nusantara*, 1(2). <https://jicnusantara.com/index.php/jicn/article/view/266>
- Ngantung, F. M. (2024). Perlindungan hukum terhadap korban doxing perusahaan pinjaman online legal. *Lex Privatum*, 13(5). <https://ejournal.unsrat.ac.id/v3/index.php/lexprivatum/article/view/57131>
- Nugraha, Y. A., & Saputra, T. (2024). Penerapan hukum terhadap tindak pidana doxing di Indonesia. *Jurnal Hukum Pelita*, 5(1). <https://jurnal.pelitabangsa.ac.id/index.php/JH/article/download/2670/1952>
- Rizqi, S. M., et al. (2024). Studi kasus sebuah ancaman terhadap privasi kasus doxing di Indonesia dalam perspektif hukum dan etika. *Multilingual: Journal of Universal Studies*, 4(4). <https://ejournal.penerbitjurnal.com/index.php/multilingual/article/view/941>

- Sari, I. (2020). Perbuatan melawan hukum (PMH) dalam hukum pidana dan hukum perdata. *Jurnal Ilmiah Hukum Dirgantara*, 11(1). <https://journal.universitassuryadarma.ac.id/index.php/jihd/article/view/651>
- Subhan, M., & Muttaqihlm, N. I. N. (2024). Perlindungan hukum bagi korban penyebaran data pribadi oleh penyedia jasa pinjaman online ilegal dalam perspektif viktimologi. *Delicti: Jurnal Hukum Pidana dan Kriminologi*, 2(1). <http://delicti.fhuk.unand.ac.id/index.php/jdc/article/view/35>
- Uweng, I. S., et al. (2023). Perlindungan hukum pidana terhadap doxing menurut Undang-Undang Informasi dan Transaksi Elektronik. *Pattimura Law Study Review*, 1(1). <https://ojs3.unpatti.ac.id/index.php/palarev/article/view/10897>
- Widigdo, Z., & Rosando, A. F. (2023). Perlindungan negara terhadap privasi data pribadi dalam layanan SIM card di era digital. *Bureaucracy Journal: Indonesia Journal of Law and Social-Political Governance*, 3(1). <https://bureaucracy.gapenas-publisher.org/index.php/home/article/view/210>
- Yudiana, T. C., et al. (2022). The urgency of doxing on social media regulation and the implementation of right to be forgotten on related content for the optimization of data privacy protection in Indonesia. *Padjadjaran Journal of Law*, 9(1). <https://jurnal.unpad.ac.id/pjih/article/view/37793>

Dokumen Lain

- Baihaiqi, A. (2024). Pembobol data pribadi Denny Siregar divonis 8 bulan penjara. Retrieved from <https://news.detik.com/berita-jawa-timur/d-5479358/pembobol-data-pribadi-denny-siregar-divonis-8-bulan-penjara>

Dokumen Hukum

- Undang-Undang Dasar Negara Republik Indonesia 1945.
- Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi.
- Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik.
- Undang-Undang Nomor 31 Tahun 2014 tentang Perubahan atas Undang-Undang Nomor 13 Tahun 2006 tentang Perlindungan Saksi dan Korban.
- Undang-Undang Nomor 19 Tahun 2016 tentang Perubahan atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik.
- Undang-Undang Nomor 1 Tahun 2024 tentang Perubahan Kedua atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik.
- Peraturan Pemerintah Nomor 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik.
- Putusan Pengadilan Negeri Jakarta Selatan Nomor 958/Pdt.G/2020/Pn Jkt.S.