JICN: Jurnal Intelek dan Cendikiawan Nusantara
https://jicnusantara.com/index.php/jicn
Vol : 1 No: 2, April - Mei 2024
E-ISSN : 3046-4560

Analisis Yuridis Tindakan Kriminal Doxing Ditinjau Berdasarkan Undang Undang Nomor 27 Tahun 2022 Tentang Perlindungan Data Pribadi

Legal Analysis of Doxing Criminal Actions Reviewed Based on Law Number 27 of 2022 Concerning Personal Data Protection

Muhammad Kamarulzaman Satria[1*], Hudi Yusuf[2]
[1],Fakultas Hukum, Universitas Bung Karno, *Email :* kamaruzzaman.satria@gmail.com
[2]Fakultas Hukum, Universitas Bung Karno, *Email :* hoedydjoesoef@gmail.com

Article Info

Article history :
Received : 10-05-2024
Revised : 12-05-2024
Accepted : 14-05-2024
Published: 16-05-2024

Abstract

The digitalization era and the development of information technology have heightened the importance of personal data protection as a part of human rights. This study aims to analyze the implementation of Law Number 27 of 2022 on Personal Data Protection (PDP Law) in Indonesia, compare it with international regulations, and evaluate its effectiveness in safeguarding citizens' personal data. The methodology employed is normative juridical analysis, examining relevant legal documents and related literature to identify and understand the framework for personal data protection. The findings indicate that although the PDP Law provides a strong legal basis for personal data protection, challenges remain in terms of law enforcement, public awareness, and private sector compliance. This research proposes enhanced inter-agency cooperation and regulatory strengthening as subsequent steps to optimize personal data protection in Indonesia.

Keywords*: *Doxing, Personal data protection, Personal Data Protection Law

Abstrak

Era digitalisasi dan perkembangan teknologi informasi telah meningkatkan pentingnya perlindungan data pribadi sebagai bagian dari hak asasi manusia. Penelitian ini bertujuan untuk menganalisis implementasi Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi (UU PDP) di Indonesia, membandingkannya dengan regulasi internasional, dan mengevaluasi efektivitasnya dalam melindungi data pribadi warga. Metode yang digunakan adalah analisis yuridis normatif dengan mengkaji dokumen hukum yang relevan serta literatur terkait untuk mengidentifikasi dan memahami kerangka kerja perlindungan data pribadi. Hasil penelitian menunjukkan bahwa meskipun UU PDP telah memberikan dasar hukum yang kuat untuk perlindungan data pribadi, masih terdapat tantangan dalam hal penegakan hukum, kesadaran publik, dan kepatuhan sektor swasta. Penelitian ini mengusulkan peningkatan kerjasama antarlembaga dan penguatan regulasi sebagai langkah lanjutan untuk mengoptimalkan perlindungan data pribadi di Indonesia.

Kata Kunci: Doxing, Perlindungan data pribadi, UU Perlindungan Data Pribadi

PENDAHULUAN

Perkembangan industrialisasi digital yang ditandai dengan revolusi 4.0 telah mengangkat media internet sebagai panggung utama serta sumber utama informasi dalam era big data. Fenomena ini tidak hanya menciptakan suatu ruang untuk pertukaran informasi yang masif, tetapi juga mempengaruhi dinamika perilaku individu dengan mendorong ke arah konsumtif. Kemudahan akses dan penyebaran informasi melalui internet telah membentuk kebiasaan baru dalam pola interaksi manusia, di mana efektivitas dan efisiensi waktu menjadi faktor kunci dalam menentukan bagaimana informasi dikonsumsi dan disebarkan dalam masyarakat.

Berdasarkan perkembangan di era yang serba digital saat ini, terjadi perkembangan pada bidang teknologi informasi yang membawa sebuah perubahan yang sangat besar bagi masyarakat. Masyarakat bisa dengan mudahnya mengunggah sebuah informasi dan dikonsumsi oleh banyak orang. Namun, tidak serta merta informasi yang sifatnya pribadi tersebut bisa dikonsumsi oleh semua orang. Data pribadi adalah sebuah informasi yang sifatnya melekat pada diri dari setiap orang. Jika ditinjau berdasarkan pasal 1 ayat (1) Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi, "Data Pribadi adalah data tentang orang perseorangan yang teridentifikasi atau dapat diidentifikasi secara tersendiri atau dikombinasi dengan informasi lainnya baik secara langsung maupun tidak langsung melalui sistem elektronik atau nonelektronik." (Undang-Undang No. 27 Tahun 2022). Data pribadi tersebut sifatnya adalah sesuatu hal yang privasi dan sangat sensitif bagi seseorang (Kusnadi & Wijaya, 2021). Sedangkan menurut Suari & Sarjana (2023), data pribadi mencakup semua informasi tentang nama, alamat, riwayat kesehatan, informasi finansial, dan informasi yang sifatnya sensitif bagi orang tersebut. Dapat disimpulkan bahwa data pribadi adalah sebuah informasi yang mengidentifikasikan sebuah individu yang sifatnya sangat privasi dan sensitif baik menggunakan sistem elektronik atau nonelektronik.

Atas dasar informasi yang sifatnya sensitif tersebut, muncul sebuah hak privasi. Hal privasi adalah segala sesuatu hal yang sifatnya mutlak serta dimiliki oleh manusia sebagai sebuah tuntutan untuk pemenuhan kebutuhan serta kepentingan diri dari data pribadi terhadap informasi yang berkaitan dengan dirinya sendiri serta pembatasan akses terhadap semua informasi pribadi. Bedasrkan *Black's Law Dictionary,* hak privasi adalah hak yang melekat pada diri seseorang untuk bisa mengontrol aktivitas yang sifatnya pribadi serta keputusan pribadi tanpa adanya campur tangan dari pihak lain (Black & Garner, 2009). Hak privasi tersebut sifatnya merupakan hak yang melekat pada diri individu untuk bisa mengatur penyebaran informasi pribadi dan pembatasan atas akses terhadap diri pribadi individu tersebut. Terdapat pula pengertian hak privasi menurut para ahli oleh Alan Westin yakni *"the claim of individuals, groups, or institutions to determine for themselves when, how, and to what extent information about them is communicated to others"*. Pengertian tersebut juga bisa memberikan pemahaman tentang hak privasi yakni informasi tersebut hanya diketahui oleh dirinya sendiri tanpa adanya tersebar kepada orang lain. Dengan kata lain, hal tersebut merupakan sebuah kekuasaan yang sifatnya terbesar atas individu untuk bisa menentukan kapan dan bagaimana semua informasi tentang dirinya tersebut dipublikasikan dan diketahui oleh orang lain.

Dalam Undang-Undang Dasar Negara Republik Indonesia Pasal 28G ayat (1), negara menjamin perlindungan diri pribadi setiap orang, yakni termasuk semua data diri. Bunyi dari pasal tersebut adalah "Setiap orang berhak atas perlindungan diri pribadi, keluarga, kehormatan, martabat, dan harta benda yang di bawah kekuasaannya, serta berhak atas rasa aman dan perlindungan dari ancaman ketakutan untuk berbuat atau tidak berbuat sesuatu yang merupakan hak asasi". Negara sendiri menjamin dari hak privasi setiap orang. Perwujudan tersebut adalah dengan adanya perlindungan dari data pribadi dalam kehidupan bermasyarakat. Perlindungan data pribadi tersebut menjadi sebuah kewajiban yang sifatnya fundamental dari pemerintah untuk bisa menghasilkan sebuah perlindungan hukum untuk bisa mewujudkan hak konstitusional dari setiap warga negara (Fikri & Rusdiana, 2023). Berdasarkan UUD 1945 Pasal 28G ayat (1) tersebut memaparkan bahwa tidak memperbolehkan siapapun untuk melakukan tindakan yang melibatkan perlindungan, keluarga, kehormatan, martabat, dan harta benda individu yang berada di bawah tanggung jawabnya, serta hak asasi manusia.

Perlindungan data pribadi tersebut berkaitan dengan perilaku *doxing*. Menurut Saly & Sulthanah (2023), *Doxing* adalah tindakan kriminal di internet yang melibatkan penargetan dan pengumpulan informasi pribadi tanpa izin, lalu menyebarkannya. Penyebaran informasi di internet harus mematuhi prinsip perlindungan Hak Asasi Manusia, sehingga penggunaannya memerlukan izin dari pemilik data. *Doxing* sering dilakukan dengan niat jahat untuk mengancam, mengintimidasi, dan dapat membahayakan kondisi fisik maupun mental seseorang. Tindakan ini melanggar privasi individu karena melibatkan pengumpulan dan penyebaran data pribadi tanpa izin. Perilaku *doxing* tak jarang banyak ditemui di media sosial dengan unggahan yang memuat informasi seseorang, bisa berupa gambar, video, atau narasi untuk menggiring suatu opini (Bagiartha, 2021). Kondisi tersebut berawal dari adanya gagasan kebebasan berpendapat. Namun, jika ditinjau lebih lanjut, kebebasan berpendapat apabila tidak berdasar pada etika yang berlaku di masyarakat akan menjadi akar dalam tindak perbuatan *doxing* tersebut.

Doxing adalah salah satu bentuk kejahatan yang sangat merusak privasi dan keamanan individu. Tindakan ini, yang melibatkan pengungkapan informasi pribadi seseorang tanpa izin, dapat membawa berbagai dampak negatif yang signifikan. Misalnya, korban dapat mengalami pelecehan, intimidasi, pencurian identitas, dan bahkan ancaman fisik. Dalam ranah kriminologi, doxing dikategorikan sebagai bentuk kekerasan digital yang bisa berakibat serius terhadap kesejahteraan psikologis dan fisik korban. Menurut penelitian Uweng et al (2023), doxing digolongkan sebagai tindak kriminal karena tujuannya yang sering kali untuk mempermalukan, mengancam, mengintimidasi, atau menghukum individu yang menjadi sasaran. Pelaku doxing, atau yang dikenal sebagai *doxer* (orang yang melakukan *doxing)*, biasanya melakukan tindakan ini untuk mencapai kepuasan atau keuntungan pribadi, yang pada akhirnya sangat merugikan korban. Doxing tidak hanya melanggar hak privasi seseorang tetapi juga menciptakan lingkungan yang penuh ketakutan dan ketidakamanan bagi korban.

Salah satu tindakan *doxing* yang pernah terjadi adalah kasus doxing Jurnalis Liputan6.com. Menurut Balqis & Monggilo (2023), Cakra selaku jurnalis dari Liputan6.com mengalami tiga jenis

doxing sekaligus dilihat dari aspek yang terdampak, yaitu deanonymizing doxing, targeting doxing, dan delegitimization doxing. Sedangkan jika dilihat dari motivasi pelaku, doxing yang dialami Cakra termasuk jenis silencing dan retribution. Dari kasus ini terlihat bahwa seseorang dapat mengalami lebih dari satu jenis doxing pada waktu yang sama. Jika membahas dampaknya, targeting doxing memiliki efek yang lebih serius bagi kehidupan nyata Cakra. Karena alamatnya telah tersebar, Cakra harus "mengungsi" ke safe house hingga situasi aman terkendali. Dalam menangani doxing terhadap jurnalisnya, Liputan6.com melakukan berbagai upaya baik di lingkup internal maupun eksternal. Secara internal, selain mengamankan Cakra dan keluarganya secara fisik, mereka juga meminta Cakra untuk segera mengamankan semua akun pribadinya, termasuk foto-foto anaknya. Mereka menanggung biaya makan selama di safe house, menawarkan bantuan psikologis, serta memantau kondisi Cakra dan keluarganya setiap jam.

Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi (UU PDP) menyediakan kerangka hukum yang jelas untuk melindungi data pribadi warga negara Indonesia dari penyalahgunaan, termasuk praktik doxing. Dalam UU PDP, pelanggaran terhadap privasi dan penyebaran data pribadi tanpa izin secara tegas diatur dan dilarang. Pasal 16 ayat (1) UU PDP menyebutkan bahwa pemrosesan data pribadi harus berdasarkan persetujuan dari pemilik data, kecuali ditentukan lain oleh peraturan perundang-undangan. Ini berarti bahwa setiap tindakan pengumpulan, penggunaan, atau penyebaran data pribadi harus mendapatkan persetujuan eksplisit dari individu yang bersangkutan. Dalam konteks doxing, pelaku yang menyebarkan informasi pribadi tanpa persetujuan jelas melanggar ketentuan ini.

Lebih lanjut, Pasal 65 UU PDP menjelaskan sanksi bagi pelanggaran terhadap aturan ini. Pasal 65 ayat (1) menyatakan bahwa setiap orang yang secara sengaja dan tanpa hak mengungkapkan data pribadi seseorang sehingga data tersebut diketahui oleh pihak ketiga yang tidak berhak dapat dipidana dengan pidana penjara paling lama lima tahun dan/atau pidana denda paling banyak Rp5.000.000.000,00 (lima miliar rupiah). Pasal 65 ayat (2) memperberat hukuman jika perbuatan tersebut menyebabkan kerugian bagi pemilik data, dengan ancaman pidana penjara paling lama tujuh tahun dan/atau pidana denda paling banyak Rp7.000.000.000,00 (tujuh miliar rupiah). Ketentuan ini menegaskan bahwa doxing, sebagai bentuk pengungkapan data pribadi tanpa izin, dikenai sanksi berat sesuai UU PDP.

UU PDP memberikan batasan yang jelas mengenai praktik doxing dengan mengatur pengumpulan, penggunaan, dan penyebaran data pribadi secara ketat. Berdasarkan UU PDP, doxing diartikan sebagai pengungkapan data pribadi seseorang tanpa izin yang sah dari pemilik data, yang termasuk tindakan ilegal. Pasal 16 ayat (1) mengharuskan setiap pemrosesan data pribadi harus didasarkan pada persetujuan eksplisit dari individu tersebut. Pengumpulan dan penyebaran informasi seperti nama, alamat, nomor telepon, atau data lainnya tanpa persetujuan jelas melanggar ketentuan ini. Hanya dalam keadaan tertentu, seperti untuk kepentingan umum atau penegakan hukum, data pribadi dapat diproses tanpa persetujuan, yang tidak mencakup tujuan doxing yang merugikan individu.

UU PDP juga memberikan sanksi yang tegas terhadap pelanggaran yang terkait dengan doxing. Pasal 65 ayat (1) menetapkan bahwa setiap orang yang mengungkapkan data pribadi tanpa hak dapat dipidana dengan penjara hingga lima tahun atau denda hingga lima miliar rupiah. Jika tindakan tersebut menyebabkan kerugian bagi pemilik data, hukuman dapat diperberat menjadi penjara hingga tujuh tahun atau denda hingga tujuh miliar rupiah, seperti yang diatur dalam pasal 65 ayat (2). Dengan adanya ketentuan ini, UU PDP memastikan bahwa tindakan doxing dianggap sebagai pelanggaran serius terhadap hak privasi individu dan memberikan perlindungan yang kuat bagi warga negara Indonesia dari penyalahgunaan data pribadi.

Mengingat bahwa doxing dapat mengancam privasi seseorang *(right to privacy)*, ditambah dengan pesatnya perkembangan teknologi informasi dan cepatnya penyebaran data di internet, data menjadi sangat rentan terhadap penyalahgunaan. Oleh karena itu, doxing merupakan isu Hak Asasi Manusia yang harus diatur dan dilindungi oleh negara. Tindakan doxing minim bahkan tidak ada kontak langsung antara pelaku dan korban, sehingga memerlukan perhatian serius. Dengan diberlakukannya UU PDP yang baru, penelitian tersebut membahas prinsip-prinsip perlindungan data pribadi dari tindakan doxing dengan merujuk pada UU ITE. Berdasarkan identifikasi yang telah dipaparkan sebelumnya, maka rumusan masalah pada penelitian ini adalah bagaimana doxing dikategorikan sebagai praktek tindak pidana berdasarkan Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi? Tujuan dari penelitian ini adalah untuk menganalisis tindak pidana doxing berdasarkan Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi.

METODE PENELITIAN

Penelitian ini mengusung metode analisis yuridis normatif, yang secara khusus menggali norma-norma hukum yang tercantum dalam peraturan perundang-undangan atau dokumen hukum lainnya. Tujuannya adalah untuk menyelidiki dan menginterpretasikan berbagai aspek hukum yang berkaitan dengan tindakan kriminal doxing. Dengan pendekatan ini, peneliti berupaya mendalami implikasi hukum dari praktik doxing, sambil mempertimbangkan aspek-aspek etis dan legal yang terlibat.

Metode analisis yuridis normatif memberikan ruang bagi peneliti untuk memperoleh pemahaman yang lebih dalam tentang kerangka hukum yang mengatur doxing. Dengan merujuk pada berbagai undang-undang dan literatur hukum, penelitian ini dapat menyoroti sudut pandang hukum yang relevan dalam memahami dan menangani fenomena doxing. Ini memungkinkan para peneliti untuk mengidentifikasi peraturan hukum yang dapat digunakan untuk melindungi individu dari praktik doxing yang merugikan, sambil juga memahami bagaimana hukum menanggapi doxing dalam berbagai konteks.

Dengan demikian, pendekatan analisis yuridis normatif membuka jalan bagi pemahaman yang lebih komprehensif tentang masalah doxing dari perspektif hukum. Penelitian semacam ini tidak hanya membantu menggali regulasi yang ada, tetapi juga memberikan landasan untuk

pengembangan kebijakan yang lebih efektif dalam menanggulangi praktik doxing yang merugikan masyarakat.

HASIL DAN PEMBAHASAN

Doxing, yang mengacu pada tindakan pengumpulan dan penyebaran informasi pribadi seseorang secara online tanpa persetujuan mereka, membawa dampak signifikan dalam konteks hukum. Praktik ini biasanya bertujuan untuk merugikan, mempermalukan, atau bahkan membahayakan individu yang ditargetkan. Dari perspektif hukum, *doxing* melanggar berbagai prinsip perlindungan data pribadi yang diakui secara internasional dan juga oleh peraturan lokal di banyak negara, termasuk Indonesia.

Di Indonesia, sebelum adanya UU Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi (PDP), praktik *doxing* belum secara eksplisit diatur dalam kerangka hukum yang spesifik. Namun, dengan disahkannya UU PDP, ada dasar hukum yang jelas yang melarang pengumpulan dan penyebaran data pribadi tanpa izin. UU PDP menetapkan bahwa setiap orang memiliki hak untuk melindungi data pribadinya dari penggunaan yang tidak sah, dan pelanggaran atas hak ini dapat dikenai sanksi berupa denda atau bahkan hukuman penjara.

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.

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.

Prinsip Pengolahan Data Pribadi

Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi (UU PDP) di Indonesia mendetailkan prinsip-prinsip penting yang harus diikuti dalam pengolahan data pribadi, yang mencakup legalitas, proporsionalitas, dan transparansi. Pertama, prinsip legalitas menggarisbawahi bahwa segala pengolahan data pribadi harus memiliki dasar hukum yang jelas dan sah. Ini menghindarkan dari pengolahan data sembarangan dan tanpa dasar yang jelas, memastikan bahwa hanya data yang benar-benar perlu dan sesuai dengan peraturan yang berlaku yang diproses.

Kedua, prinsip proporsionalitas menekankan bahwa pengolahan data harus seimbang dengan tujuan pengolahan tersebut. Artinya, data yang dikumpulkan harus proporsional, tidak berlebihan, dan terbatas hanya pada apa yang diperlukan untuk mencapai tujuan spesifik. Ini meminimalkan risiko penyalahgunaan data dan mengurangi potensi kerugian yang bisa ditimbulkan kepada subjek data.

Ketiga, prinsip transparansi mengharuskan bahwa semua proses pengolahan data harus dilakukan secara terbuka dan jujur. Subjek data harus diberitahu tentang bagaimana data mereka dikumpulkan, diproses, dan digunakan. Hal ini mencakup memberikan informasi yang jelas tentang siapa yang bertanggung jawab atas pengolahan data, tujuan pengolahan data, dan hak-hak subjek data terkait penggunaan data mereka, termasuk hak untuk mengakses, memperbaiki, dan menghapus data tersebut.

Penerapan prinsip-prinsip ini sangat krusial dalam mencegah praktik-praktik seperti doxing, yang melibatkan penggunaan data pribadi tanpa izin untuk tujuan yang merugikan, seperti pemerasan, pelecehan, atau pencemaran nama baik. Tanpa adanya dasar hukum yang kuat, proporsionalitas dalam pengumpulan dan penggunaan data, serta transparansi dalam proses pengolahan data, tindakan seperti doxing dengan jelas melanggar UU PDP dan merupakan tindakan ilegal yang bisa dikenakan sanksi berat menurut hukum yang berlaku.

Aturan Pada *Doxing*

Doxing, yang melibatkan penyebaran informasi pribadi tanpa persetujuan, dapat menimbulkan pelanggaran serius terhadap privasi individu dan sering kali bertentangan dengan norma-norma hukum yang ada yang dirancang untuk melindungi data pribadi. Secara hukum, *doxing* dapat dikategorikan sebagai pelanggaran terhadap undang-undang perlindungan data pribadi yang ada. Di Indonesia, misalnya, Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi (UU PDP) menyediakan kerangka kerja hukum yang jelas terhadap penanganan data pribadi. UU ini secara eksplisit mengharuskan pengolahan data pribadi untuk mendapatkan persetujuan dari pemilik data sebelum data tersebut diproses atau disebarkan. Melanggar prinsip ini, seperti yang terjadi dalam kebanyakan kasus *doxing*, bisa menimbulkan sanksi hukum yang berat, termasuk denda dan hukuman penjara bagi pelaku.

Namun, 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.

Selanjutnya, walaupun undang-undang seperti UU PDP menyediakan dasar yang kuat untuk melawan *doxing*, masih terdapat ruang untuk penyempurnaan. Misalnya, diperlukan kejelasan lebih lanjut mengenai definisi "persetujuan" dalam konteks online dan bagaimana persetujuan tersebut dapat secara sah dikumpulkan dan diverifikasi. Ini memastikan bahwa hukum

dapat efektif mengatasi manipulasi informasi dan penyebaran data ilegal dalam lingkungan digital yang kompleks.

Pada konteks internasional, perbedaan antara yurisdiksi dalam hal definisi dan penanganan *doxing* bisa menimbulkan tantangan tambahan. Sebuah pendekatan yang lebih harmonis dan kerjasama lintas negara mungkin diperlukan untuk efektif menangani *doxing* yang melibatkan pihak-pihak dari berbagai negara.

Regulasi *doxing* memerlukan pendekatan yang komprehensif yang tidak hanya mengandalkan sanksi hukum tetapi juga penguatan mekanisme pengawasan dan kerjasama antar lembaga, baik di tingkat nasional maupun internasional. Penyempurnaan terus-menerus dari undang-undang yang ada dan adaptasi terhadap evolusi teknologi digital adalah kunci untuk menjaga keefektifan hukum dalam melindungi individu dari praktik *doxing* yang merugikan

Tolak Ukur Doxing

Penentuan tolok ukur doxing dalam konteks hukum mengharuskan pemahaman yang mendalam mengenai aspek-aspek yang membentuk tindakan ini sebagai pelangaran hukum. Doxing, yang didefinisikan sebagai penyebaran informasi pribadi tanpa persetujuan, memerlukan kriteria tertentu untuk dapat dikategorikan dalam ranah hukum sebagai tindak pidana atau pelanggaran privasi. Tolok ukur ini umumnya meliputi unsur-unsur seperti identifikasi subjek data yang jelas, persetujuan subjek data, dan niat pelaku dalam penyebaran data tersebut.

Menurut Wijaya (2022), tolok ukur pertama dalam menentukan doxing adalah legalitas pengumpulan data. Data harus dikumpulkan dengan cara yang sah menurut hukum yang berlaku dan dengan persetujuan yang eksplisit dari individu yang bersangkutan. Tanpa persetujuan yang jelas dan sah, pengumpulan dan penyebaran data sudah dapat dianggap sebagai tindakan doxing. Kedua, niat pelaku juga penting dalam penentuan tindakan sebagai doxing. Apabila niatnya adalah untuk menyakiti, mempermalukan, atau merugikan individu yang data pribadinya disebarkan, maka ini menegaskan tindakan tersebut sebagai doxing yang berpotensi dikenai sanksi hukum.

Tolok ukur lainnya adalah dampak yang ditimbulkan dari tindakan doxing. Menurut Setiawan (2021), dampak ini bisa berupa gangguan psikologis, kerugian ekonomi, atau kerusakan reputasi yang dialami oleh korban. Evaluasi dampak ini penting untuk menentukan tingkat keparahan dan jenis sanksi yang mungkin diberikan kepada pelaku.

Secara hukum, penentuan tolok ukur doxing di Indonesia masih menghadapi beberapa tantangan. Meskipun Undang-Undang Perlindungan Data Pribadi telah menyediakan kerangka kerja, masih terdapat kebutuhan untuk regulasi yang lebih spesifik yang mendefinisikan dan mengatur aspek-aspek seperti persetujuan eksplisit, metode pengumpulan data yang sah, dan kriteria niat pelaku.

Konflik *Doxing*

Pada banyak sistem hukum, terdapat area-area di mana ketiadaan atau kekurangan aturan hukum yang jelas dapat menyebabkan konflik dan ketidakpastian, terutama di era digital yang cepat

berkembang ini. Konflik hukum sering terjadi ketika teknologi baru melebihi perkembangan kerangka hukum yang ada, menciptakan apa yang sering disebut sebagai "celah hukum.". Salah satu contoh yang signifikan dari area dimana kurangnya regulasi sering kali menimbulkan konflik adalah penggunaan data pribadi dan privasi di internet. Contohnya, fenomena *doxing*, yang menunjukkan bagaimana kekurangan aturan dapat menyebabkan pelanggaran privasi yang serius. Meskipun banyak negara telah mengembangkan undang-undang perlindungan data pribadi, seringkali peraturan ini tidak cukup terperinci untuk mengatasi semua aspek atau teknik *doxing* yang spesifik. Akibatnya, korban *doxing* mungkin kesulitan untuk mencari keadilan karena ketidakjelasan tentang bagaimana hukum berlaku terhadap kasus-kasus spesifik mereka.

Di Indonesia, pengesahan UU Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi adalah langkah penting dalam mengatasi celah hukum ini. Namun, seperti banyak undang-undang baru, implementasi penuhnya memerlukan waktu, dan ada periode di mana ketidakjelasan hukum masih bisa terjadi. Dalam periode transisi ini, bisa muncul konflik ketika pelaku usaha, misalnya, belum sepenuhnya memahami kewajiban mereka di bawah undang-undang baru, atau ketika ada ketidakjelasan tentang bagaimana aturan tersebut diterapkan dalam kasus praktis.

Lebih jauh lagi, dalam konteks global, kekurangan aturan seragam mengenai privasi dan perlindungan data di berbagai yurisdiksi menciptakan tantangan tambahan, terutama untuk perusahaan yang beroperasi secara internasional. Perbedaan dalam regulasi dapat menyebabkan konflik hukum antarnegara yang memerlukan navigasi hukum yang kompleks dan sering kali mahal.

Solusi Permasalahan

Pada menerapkan regulasi yang kompleks seperti Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi (UU PDP) di Indonesia, sering kali muncul kebutuhan untuk mengembangkan peraturan pelaksana atau UU turunan yang lebih spesifik untuk memastikan efektivitas penerapan undang-undang tersebut. Peraturan pelaksana ini bertujuan untuk memberikan detail teknis dan prosedural yang tidak dicakup secara rinci dalam undang-undang induk, membantu mengatasi ambiguasi, dan menyediakan kerangka kerja yang jelas untuk semua pihak yang terlibat dalam pengolahan data pribadi.

Kebutuhan peraturan pelaksana untuk UU PDP mengungkapkan beberapa aspek penting. Pertama, peraturan pelaksana diperlukan untuk mendefinisikan lebih lanjut standar dan prosedur teknis seperti keamanan data, kriteria persetujuan, dan mekanisme pengaduan yang efektif untuk pelanggaran data. Kedua, dalam konteks yang serba digital dan terkoneksi ini, peraturan tersebut juga harus mencakup pedoman tentang transfer data lintas batas, yang sangat penting mengingat banyaknya operasi bisnis yang melampaui yurisdiksi nasional.

Selain itu, mengingat perkembangan teknologi yang cepat, terdapat kemungkinan bahwa beberapa ketentuan dalam UU PDP mungkin perlu disesuaikan atau diperbarui untuk memenuhi tantangan baru yang muncul. Misalnya, perkembangan terbaru dalam kecerdasan buatan dan pembelajaran mesin mungkin memerlukan pemikiran ulang tentang bagaimana data pribadi

diproses dan perlindungan privasi yang diperlukan. Dalam hal ini, mungkin diperlukan amandemen terhadap beberapa pasal dalam UU PDP untuk memastikan bahwa undang-undang tersebut tetap relevan dan efektif dalam melindungi hak privasi warga.

Pada pengembangan UU turunan dari Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi (UU PDP) di Indonesia, diperlukan pertimbangan mendetail mengenai siapa yang terlibat, bentuk regulasi yang akan diimplementasikan, proses penerapannya, serta batasan yang harus diperhatikan untuk mencegah penyalahgunaan. Pertama, UU turunan ini harus mengidentifikasi secara jelas subjek yang terlibat, termasuk pengontrol data, pemroses data, subjek data, dan penyedia layanan teknologi dan platform online. Ini penting untuk menetapkan tanggung jawab masing-masing pihak dalam proses pengolahan data.

Kedua, regulasi dalam UU turunan ini harus meliputi ketentuan mengenai persetujuan yang harus jelas dan tak ambigu, prosedur untuk pelaporan dan respons terhadap pelanggaran, serta mekanisme audit dan pemantauan yang efektif. Sanksi yang jelas dan tegas juga harus ditetapkan untuk mencegah pelanggaran dan memberikan efek jera bagi pelaku.

Ketiga, implementasi dari UU turunan ini memerlukan kerja sama erat antar lembaga, termasuk otoritas perlindungan data dan penegak hukum, serta pelaksanaan program pendidikan dan pelatihan untuk meningkatkan kesadaran pengontrol data dan pemroses data tentang pentingnya perlindungan data pribadi. Partisipasi masyarakat sipil dalam pengawasan dan evaluasi juga vital untuk memastikan transparansi dan akuntabilitas.

Akhirnya, UU turunan harus memiliki batasan yang jelas untuk menghindari pengumpulan data yang berlebihan dan tidak relevan, serta menjamin bahwa akses ke data pribadi dibatasi hanya untuk tujuan yang sah dan telah disetujui oleh subjek data. Transparansi dari pengontrol dan pemroses data dalam semua aktivitas pengolahan data juga harus dipastikan. Dengan langkah-langkah ini, Indonesia dapat memperkuat perlindungan privasi warganya dalam menghadapi tantangan era digital, sambil mendukung inovasi dan pertumbuhan yang bertanggung jawab.

Implementasi Perlindungan Data Pribadi (PDP) di Berbagai Negara

Implementasi perlindungan data pribadi (PDP) di berbagai negara menunjukkan variasi yang signifikan tergantung pada kerangka hukum dan kebijakan masing-masing negara. Di Eropa, misalnya, General Data Protection Regulation (GDPR) merupakan standar emas dalam perlindungan data pribadi, memberikan individu kontrol yang kuat atas data mereka dengan persyaratan ketat terhadap transparansi dan akuntabilitas untuk organisasi yang memproses data (Setiawan, 2020). GDPR menekankan pada hak untuk dilupakan, yang memungkinkan individu meminta penghapusan data mereka dari database perusahaan, serta membutuhkan persetujuan yang jelas dan tegas dari individu sebelum data mereka diproses.

Di Amerika Serikat, pendekatan terhadap perlindungan data pribadi lebih terfragmentasi, dengan regulasi yang berbeda di setiap negara bagian daripada kerangka hukum federal yang menyeluruh (Prasetyo, 2019). California, misalnya, telah mengimplementasikan California Consumer Privacy Act (CCPA), yang memberi penduduk negara tersebut hak yang signifikan atas

data mereka, mirip dengan GDPR. Namun, di negara bagian lain, perlindungan data bisa jauh lebih lemah.

Di Asia Tenggara, Singapura mendapat pengakuan sebagai salah satu negara dengan regulasi perlindungan data pribadi (PDP) yang paling maju, khususnya melalui Personal Data Protection Act (PDPA) yang diimplementasikan. PDPA Singapura menawarkan kerangka kerja komprehensif yang menjamin perlindungan data pribadi warganya dengan mengatur pengumpulan, penggunaan, dan pengungkapan data pribadi secara ketat. Singapura juga memberikan wewenang kepada otoritas perlindungan data untuk melakukan pemeriksaan dan mengenakan denda yang berat bagi pelanggaran, menunjukkan komitmen kuat negara tersebut dalam menjaga privasi data warganya (Suhariyanto, 2021).

Sementara itu, Jepang, yang juga diakui memiliki sistem perlindungan data yang kuat, telah mengadaptasi beberapa elemen dari pendekatan GDPR. Hukum perlindungan data di Jepang, yang diperbaharui dalam Act on the Protection of Personal Information (APPI), mengharuskan persetujuan eksplisit untuk pengumpulan data pribadi dan menetapkan aturan ketat mengenai transfer data lintas batas. APPI juga mendukung prinsip minimasi data dan akuntabilitas, memastikan bahwa data pribadi hanya digunakan untuk tujuan yang jelas dan sah serta dengan transparansi penuh kepada subjek data.

Perbandingan Perlindungan Data Pribadi (PDP) di Negara lain Dengan di Indonesia

Perbandingan implementasi perlindungan data pribadi (PDP) antara Indonesia dengan negara lain menunjukkan kontras yang mencolok dalam hal ketatnya regulasi, cakupan hukum, dan mekanisme penegakan. Indonesia baru-baru ini mengambil langkah penting dalam perlindungan data pribadi dengan pengesahan Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi (UU PDP). UU ini mengikuti model global yang umum, dengan menekankan pada hak individu untuk mengontrol data mereka serta menetapkan kewajiban bagi pemroses data untuk melindungi data tersebut (Suhariyanto, 2021).

Dibandingkan dengan Eropa, di mana General Data Protection Regulation (GDPR) telah menjadi standar emas dalam PDP, UU PDP Indonesia memiliki beberapa kesamaan seperti persyaratan untuk konsen eksplisit, hak atas penghapusan data, dan kewajiban untuk transparansi dalam pengolahan data. Namun, GDPR jauh lebih ketat dalam hal denda dan sanksi untuk pelanggaran, yang menunjukkan pendekatan yang lebih agresif terhadap pelanggaran privasi data (Setiawan, 2020).

Di sisi lain, jika dibandingkan dengan Amerika Serikat, dimana tidak ada undang-undang perlindungan data pribadi federal dan peraturan berbeda-beda tergantung negara bagian, Indonesia memiliki kerangka kerja yang lebih seragam dan kohesif. California, dengan California Consumer Privacy Act (CCPA)nya, mungkin yang paling mendekati GDPR dalam hal pemberian hak kepada konsumen dan transparansi, namun masih jauh lebih lembut dibandingkan dengan regulasi di Indonesia dari segi cakupan dan ketatnya sanksi (Prasetyo, 2019).

Dalam konteks Asia, Singapura dan Jepang memiliki undang-undang PDP yang sangat maju. Singapura dengan Personal Data Protection Act (PDPA)nya, menawarkan pendekatan yang seimbang antara perlindungan privasi dan fleksibilitas untuk bisnis, sebuah aspek yang masih dalam tahap penyesuaian di Indonesia. Jepang, yang PDPA-nya mendapatkan pengakuan kesetaraan dari Uni Eropa, menunjukkan standar tinggi yang bisa menjadi model untuk Indonesia dalam aspek kepatuhan internasional dan kerjasama lintas negara (Nugroho, 2020).

Secara keseluruhan, meskipun UU PDP Indonesia merupakan langkah maju, masih terdapat ruang untuk peningkatan, khususnya dalam hal penegakan hukum dan konsistensi penerapan. Perbandingan ini menunjukkan bahwa sementara Indonesia telah membuat kemajuan signifikan, masih terdapat pelajaran yang bisa dipetik dari praktik baik internasional dalam rangka mengoptimalkan perlindungan data pribadi di dalam negeri.

Solusi Model dan Prinsip yang Dapat Di Adopsi

Implementasi perlindungan data pribadi (PDP) yang efektif di Indonesia bisa mendapatkan inspirasi dari praktek terbaik yang sudah diterapkan di berbagai negara lain. Beberapa solusi yang telah terbukti efektif di luar negeri ini bisa disesuaikan dengan konteks hukum dan sosial Indonesia untuk meningkatkan keamanan dan privasi data warga.

1. Adopsi Prinsip-prinsip GDPR: Seperti di Eropa, Indonesia bisa mengadopsi prinsip-prinsip umum dari General Data Protection Regulation (GDPR) yang mencakup transparansi, pembatasan tujuan, dan minimisasi data. Prinsip-prinsip ini mendorong perusahaan untuk hanya mengumpulkan data yang esensial untuk tujuan yang jelas dan terdefinisi serta menginformasikan kepada pengguna tentang penggunaan data mereka secara jelas dan transparan (Setiawan, 2020). Prinsip "hak untuk dilupakan" juga dapat diimplementasikan, memberikan warga Indonesia hak untuk meminta penghapusan data pribadi mereka dari sistem.
2. Model CCPA untuk Keterlibatan Konsumen: Mengadopsi elemen dari California Consumer Privacy Act (CCPA) bisa memberikan individu di Indonesia kontrol yang lebih besar atas data pribadi mereka. Misalnya, memberikan warga hak untuk mengetahui informasi apa yang dikumpulkan tentang mereka, meminta penghapusan data tersebut, dan menolak penjualan informasi mereka kepada pihak ketiga (Prasetyo, 2019).
3. Regulasi Data Sektor Spesifik: Mirip dengan pendekatan di Amerika Serikat yang menggunakan regulasi sektor-spesifik seperti HIPAA untuk data kesehatan, Indonesia bisa mengembangkan regulasi yang menargetkan sektor-sektor tertentu seperti kesehatan, keuangan, dan pendidikan. Hal ini akan memastikan bahwa data yang sangat sensitif ini dikelola dengan standar yang lebih tinggi dan ketat.
4. Peningkatan Kapasitas Penegak Hukum: Mengikuti model Singapura dan Jepang, Indonesia bisa memperkuat kapasitas penegak hukum dan lembaga perlindungan data untuk melakukan audit secara berkala, menyelidiki pelanggaran, dan menerapkan sanksi

bagi pelanggar (Suhariyanto, 2021). Hal ini termasuk pelatihan khusus untuk penegak hukum tentang teknologi terbaru dan metode pengolahan data.

5. Kerja Sama Internasional: Dengan meningkatnya transfer data lintas batas, Indonesia dapat menbenefit dari kerja sama internasional yang lebih kuat, mengikuti model dari negara-negara dengan regulasi data yang matang. Kerja sama ini dapat meliputi pertukaran informasi tentang pelanggaran dan ancaman keamanan serta koordinasi dalam penegakan hukum lintas negara.

Implementasi solusi-solusi ini memerlukan analisis yang mendalam terhadap kebutuhan unik Indonesia dalam konteks sosial dan hukumnya serta adaptasi kebijakan yang sudah terbukti sukses di negara lain. Kesuksesan implementasi ini juga bergantung pada dukungan dari semua pemangku kepentingan, termasuk pemerintah, industri, dan masyarakat sipil.

KESIMPULAN

Kesimpulan dari penelitian ini menegaskan bahwa Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi (UU PDP) di Indonesia telah menetapkan dasar hukum yang kuat untuk perlindungan data pribadi, mencerminkan tren global dan menanggapi kebutuhan mendesak akan privasi di era digital. Dengan mengadopsi norma-norma internasional dan menyesuaikan dengan konteks lokal, Indonesia telah mengambil langkah signifikan untuk memperkuat hak atas privasi warganya.

Penelitian ini juga menyoroti bahwa meskipun UU PDP memberikan kerangka kerja, masih ada tantangan dalam implementasi dan penegakan hukum, mirip dengan tantangan yang dihadapi oleh negara lain yang telah lama menerapkan regulasi serupa. Perbedaan dalam kekuatan dan efektivitas penegakan antar negara menunjukkan bahwa ada ruang untuk peningkatan di Indonesia, terutama dalam hal kejelasan regulasi, peningkatan kapasitas penegak hukum, dan pendidikan publik mengenai hak-hak data pribadi.

Dari penelitian ini, menjadi jelas bahwa untuk mencapai penerapan UU PDP yang efektif, perlu adanya upaya yang berkelanjutan dan koordinasi antar berbagai stakeholder, termasuk pemerintah, sektor swasta, dan masyarakat sipil. Penelitian ini mengusulkan perlunya penelitian lanjutan yang dapat mengeksplorasi dampak implementasi UU PDP pada berbagai sektor industri di Indonesia, menilai efektivitas mekanisme pengaduan dan penyelesaian kasus pelanggaran data, serta mengembangkan strategi untuk meningkatkan kesadaran publik tentang pentingnya melindungi data pribadi.

Selain itu, penelitian lanjutan bisa mengkaji lebih dalam mengenai pengaruh budaya dan nilai sosial terhadap persepsi dan perilaku masyarakat Indonesia dalam melindungi data pribadi mereka, sehingga dapat memberikan wawasan yang lebih komprehensif mengenai cara terbaik untuk menyosialisasikan dan menerapkan regulasi perlindungan data pribadi di Indonesia.

UCAPAN TERIMA KASIH

Dapat digunakan untuk menyebutkan sumber dana penelitian yang hasilnya dilaporkan pada jurnal ini dan memberikan penghargaan kepada beberapa institusi.

DAFTAR PUSTAKA

Bagiartha, I., P. (2021). Perilaku Doxing dan Pengaturannya dalam Positivisme Hukum indonesia. *Widya Kerta Jurnal Hukum Agama Hindu, 4*(2), 90-104.

Balqis, D., R. & Monggilo, Z., M., Z. (2023). Doxing Sebagai Ancaman Baru Jurnalis Online: Menelisik Kasus Doxing Jurnalis Liputan6.com. *Komunikasi: Jurnal Komunikasi, 14*(2), 133-144

Black, B. A., & Garner, B. A. Ed. (2009). *Black's Law Dictionary* (9th ed.). Minnesota: West Publishing Co

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

Garner, B. A. Ed. (2009). *Black's Law Dictionary (9th.ed.)*. Minesota: West Publishing Co

Hartanti, M. (2022). Perlindungan Hukum terhadap Korban Doxing Menurut UU Perlindungan Data Pribadi. *Jurnal Hukum Cyber*, vol. 5, no. 2

Indonesia. 2022. Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi. peraturan.bpk.go.id

Kusnadi, S., A. & Wijaya, A., U. (2021). Perlindungan Hukum Data Pribadi Sebagai Hak Privasi. *JA: Jurnal Al-Wasath, 2*(1), 19-32.

Saly, J. N. & Sulthanah, L. T. (2023). Pelindungan Data Pribadi dalam Tindakan Doxing Berdasarkan Undang-Undang Nomor 27 Tahun 2022. *Jurnal Kewaranegaraan,* 7(2), 1708-1713

Setiawan, J. (2020). Perlindungan Privasi di Indonesia: Analisis dan Prospek. Jakarta: Yayasan Pustaka Obor Indonesia

Suari, K., R., A. & Sarjana, I., M. (2023). Menjaga Privasi di Era Digital:Perlindungan Data Pribadi di Indonesia. *Jurnal Analisis Hukum, 6*(1), 132-146.

Suhariyanto, R. (2021). "Kerangka Perlindungan Data Pribadi Singapura: Sebuah Analisis Komparatif." Jurnal Hukum Teknologi dan Informasi.

Uweng, I., S. Wadjo, H., Z., & Saimima, J., M. (2023). Perlindungan Hukum Pidana Terhadap Doxing Menurut Undang-Undang Informasi Dan Transaksi Elektronik. *Pattimura Law Study Review, 1*(1), 168-179.

Prasetyo, B. (2019). "Perlindungan Data Pribadi di Amerika Serikat: Tantangan dan Peluang." Jurnal Privasi dan Keamanan Siber.

Saly, J., N. & Sulthanah, L., T. (2023). Pelindungan Data Pribadi dalam Tindakan Doxing Berdasarkan Undang-Undang Nomor 27 Tahun 2022. *Jurnal Kewaranegaraan, 7*(2), 1708-1713.

Wijaya, C. (2022). Implementasi Undang-Undang Perlindungan Data Pribadi di Indonesia: Tantangan dan Harapan. *Majalah Ilmu Hukum Indonesia*, *18* (1).