

Tindak Pidana Penyebaran Data Pribadi Melalui Internet (*Doxing*)

Hayatinufus^{1*}, Rizky Awaludin², Amirotunnadia³

¹Hukum Tata Negara, UIN Sultan Maulana Hasanuddin Banten, Serang, Indonesia

²Hukum Tata Negara, UIN Sultan Maulana Hasanuddin Banten, Serang, Indonesia

³Hukum Tata Negara, UIN Sultan Maulana Hasanuddin Banten, Serang, Indonesia

ABSTRAK

Article Info

Article history:

Received June 17, 2024

Revised April 12, 2025

Accepted June 29, 2025

Keywords:

Tindak pidana

UU ITE

Doxing

Penelitian ini fokus pada analisis tentang bagaimana data pribadi tersebar melalui internet (*doxing*) sesuai dengan Undang-Undang No. 27 Tahun 2022 tentang Perlindungan Data Pribadi. Selain itu, penelitian ini juga mengeksplorasi upaya penegakan hukum terhadap pelaku *doxing* di Indonesia. Hasil temuan dari penelitian ini yaitu : 1. *Doxing* diatur dalam hukum Indonesia melalui Undang-Undang Informasi dan Transaksi

Elektronik (UU ITE) dan Undang-Undang Perlindungan Data Pribadi (UU PDP). UU ITE, yang merupakan perubahan dari Undang-Undang Nomor 11 Tahun 2008, dan lebih khusus lagi, UU PDP yang dikeluarkan pada tahun 2022, mengatur secara spesifik tentang praktik *doxing*; 2. Pasal 30 (1) bersama Pasal 46 ayat (1) dari Undang-Undang Informasi dan Transaksi Elektronik (UU ITE) menetapkan hukuman penjara hingga 6 tahun dan denda maksimal Rp 600 juta untuk akses ilegal terhadap sistem elektronik milik individu, tanpa memandang metode yang digunakan. Sementara itu, Pasal 30 ayat (2) bersama Pasal 46 ayat (2) UU ITE mengancam hukuman penjara hingga 7 tahun dan/atau denda, sementara Pasal 30 ayat (3) bersama Pasal 46 ayat (3) UU ITE mengancam hukuman penjara maksimal 8 tahun dan denda maksimal Rp 800 juta atas tindakan melanggar hukum seperti penetrasi, pelanggaran, atau peretasan terhadap sistem keamanan komputer.

This is an open access article under the [CC-BY 4.0](https://creativecommons.org/licenses/by/4.0/) license.



Corresponding Author:

Hayatinufus

Department of Informatic, Faculty of Saintek, Islamic State Sultan Maulana Hasanuddin University

Jl Syekh Nawawi Al Bantani Kota Serang Banten, Indonesia Email:

iman.wahyudi@mail.com

1. PENDAHULUAN

Kemajuan zaman yang terus berkembang secara modern telah signifikan memengaruhi cara individu berinteraksi dalam masyarakat. Perkembangan ilmu pengetahuan dan teknologi yang semakin maju telah mempercepat dan memperlancar komunikasi. Kehadiran internet di tengah masyarakat memberikan dampak baik dan buruk. Internet telah menjadi isu yang signifikan sejak dimanfaatkan dalam aktivitas perdagangan *online* yang dikenal sebagai *ecommerce*. Transaksi melalui internet dapat terjadi dengan mudah melalui perjanjian atau kontrak yang dilakukan secara *online*. Pemanfaatan teknologi informasi memfasilitasi penyebaran dan pencarian data yang penting untuk kegiatan sehari-hari. Namun, hal ini hanya dapat terjadi dengan adanya sistem telekomunikasi yang mendukung. Perkembangan teknologi komunikasi berbasis komputer telah mengalami kemajuan pesat, memberikan kemudahan bagi masyarakat dalam kehidupan sehari-hari.

Dengan kemajuan media sosial yang semakin canggih, orang dapat dengan mudah menyampaikan pikiran mereka tanpa mempertimbangkan dampak atau konsekuensi yang mungkin timbul. Hal ini dapat menyebabkan tindakan melanggar hukum di platform media sosial, seperti *doxing*, menjadi lebih mungkin terjadi. *Doxing* sering terjadi di Indonesia dan mengenai berbagai jenis korban, termasuk individu yang masih hidup atau yang sudah meninggal, pemimpin negara atau warga biasa, dan lain-lain. Ada banyak motif dan alasan di balik kejahatan *doxing* ini, mulai dari niat jahat individu hingga kesalahan sasaran oleh warganet yang awalnya ingin membantu orang lain di media sosial. *Doxing* merupakan tindakan mengungkapkan informasi pribadi seseorang dan membagikannya di ruang publik atau media sosial tanpa izin dari individu yang bersangkutan. Namun, penelitian mendalam mengenai *doxing* menunjukkan bahwa hal tersebut tidak hanya sebatas pengungkapan data pribadi di media sosial, melainkan juga dianggap sebagai ancaman kejahatan terkini yang dimungkinkan oleh teknologi digital.

Tindakan *doxing* sering membuat orang merasa tidak nyaman dalam menjelajah internet karena khawatir akan mengungkapkan informasi pribadi mereka di media sosial. Di Indonesia, ada peraturan yang berkaitan dengan perlindungan data pribadi. Salah satunya adalah Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi yang menyebutkan bahwa data pribadi adalah informasi tentang individu yang dapat diidentifikasi secara langsung atau tidak langsung, baik melalui sistem elektronik maupun non-elektronik. Menurut Peraturan Pemerintah Nomor 17 Tahun 2016 tentang Penyelenggaraan Sistem dan Transaksi Elektronik, data pribadi merujuk pada setiap informasi mengenai individu yang dapat diidentifikasi secara langsung atau tidak langsung, baik melalui sistem elektronik maupun non-elektronik. Data pribadi merupakan hak dan tanggung jawab individu terhadap informasi pribadi mereka, baik yang bersifat rahasia maupun sensitif, yang diberikan secara langsung atau tidak langsung melalui sistem elektronik ataupun konvensional (non-elektronik), untuk digunakan sesuai dengan kebutuhan oleh penyelenggara sistem elektronik.

Seperti yang diketahui belakangan ini, Indonesia sering kali menjadi target serangan siber oleh pelaku kejahatan digital yang mengakibatkan bocornya data pribadi dari beberapa platform di Indonesia. Masyarakat juga semakin resah dengan kebocoran data pribadi seperti nomor telepon seluler dan NIK yang terungkap di platform pinjaman online baru-baru ini. Banyak kasus

penyalahgunaan data pribadi seseorang, seperti Kartu Keluarga (KK) dan foto, terutama di kalangan debitur pinjaman online yang tidak memenuhi kewajibannya. Menanggapi hal ini, pemerintah menyatakan bahwa pengaturan mengenai perlindungan data pribadi saat ini diatur dalam beberapa perundang-undangan. Untuk meningkatkan efektivitas perlindungan terhadap data pribadi, disahkanlah Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi. UU tersebut bertujuan untuk memastikan perlindungan hak individu terhadap privasi mereka dan untuk meningkatkan kesadaran masyarakat tentang pentingnya perlindungan data pribadi serta memastikan pengakuan dan penghargaan terhadap hal tersebut.

Perlindungan data pribadi merupakan bagian dari hak asasi manusia yang terkait dengan perlindungan diri pribadi. Hal ini diatur dalam Pasal 28G UUD 1945 yang menyatakan bahwa “Setiap orang berhak atas perlindungan data diri pribadi, keluarga, kehormatan, martabat dan harta benda dibawah kekuasaannya, serta berhak atas rasa aman dan perlindungan dari ancaman ketakutan untuk berbuat atau tidak berbuat sesuatu yang merupakan hak asasi”. Perlindungan diri pribadi atau privasi ini diakui secara universal, yaitu diakui oleh banyak negara. Perlindungan data pribadi merupakan tindakan yang penting untuk mengurangi risiko kejahatan di dunia digital dan juga untuk mencegah penggunaan data pribadi secara tidak bertanggung jawab oleh pihak yang tidak diinginkan.

Doxing, yaitu tindakan menyebarkan informasi pribadi seseorang melalui internet atau media sosial tanpa izin dari individu yang bersangkutan, dilakukan oleh individu yang tidak bertanggung jawab dan bertujuan negatif. Data pribadi seseorang merupakan bagian dari privasi yang harus dihormati dan tidak boleh dibagikan secara sembarangan. Hal ini diatur dalam Undang-Undang Nomor 19 Tahun 2016, Pasal 26 ayat (1), yang menegaskan bahwa penggunaan informasi apapun yang menyangkut data pribadi seseorang melalui media elektronik harus mendapatkan izin dari individu yang bersangkutan.

2. METODE

Penelitian ini menggunakan metode deskriptif, serta menerapkan pendekatan hukum yuridis normatif yang sesuai dengan permasalahan yang diajukan. Menggali berbagai sumber seperti literatur, undang-undang, dan dokumen tekstual lainnya merupakan elemen penting dalam analisis hukum normatif. Dengan memperdalam teori, konsep, prinsip-prinsip hukum, dan peraturan perundang-undangan yang relevan, penelitian hukum normatif mengandalkan bahan hukum primer sebagai landasan.

3. HASIL DAN DISKUSI

3.1. Pengaturan Tentang Penyebaran Data Pribadi (*Doxing*)

Kemajuan teknologi baru-baru ini yang dirasakan oleh sebagian besar masyarakat Indonesia telah meningkatkan kesadaran akan pentingnya melindungi kerahasiaan data pribadi dari berbagai potensi pelanggaran atau penyalahgunaan oleh pihak lain. Data merupakan elemen krusial yang memuat informasi pribadi yang sering digunakan dalam berbagai aktivitas di platform digital. Data ini seringkali diperlukan untuk mengakses layanan di platform digital yang mungkin tidak mampu menjamin keamanan data pribadi

pengguna mereka. Situasi ini meningkatkan risiko penyalahgunaan data pribadi yang sulit untuk dipertanggungjawabkan.

Penyelenggara sistem elektronik merujuk kepada individu, entitas pemerintah, badan usaha, dan masyarakat yang menyediakan, mengelola, dan/atau mengoperasikan sistem elektronik baik secara mandiri maupun kolaboratif untuk kepentingan diri sendiri atau orang lain. Kewajiban penyelenggara sistem elektronik terkait dengan perlindungan data pribadi diatur dalam Peraturan Menteri Komunikasi dan Informatika Nomor 20 Tahun 2016 tentang Perlindungan Data Pribadi Pengguna Internet. Pengguna sistem elektronik merujuk kepada individu, entitas pemerintah, badan usaha, dan masyarakat yang menggunakan barang, jasa, fasilitas, atau informasi yang disediakan oleh penyelenggara sistem elektronik.

Informasi pribadi seseorang melalui beberapa tahap, termasuk pengumpulan, penyimpanan, pemrosesan, dan transfer data dari satu sektor ke sektor lainnya. Semakin besar volume data yang terkumpul, semakin besar juga risiko penyalahgunaan data tersebut. Warga negara memiliki hak untuk mendapatkan perlindungan hukum dari pemerintah, terutama dalam konteks perlindungan data pribadi yang merupakan hak asasi individu. Konstitusi Indonesia mengakui hak tersebut, yang tercermin dalam Pasal 28 G: “Setiap orang berhak atas perlindungan diri pribadi, keluarga kehormatan, dan harta benda yang dibawah kekuasaannya, serta berhak dari rasa aman dan perlindungan dari ancaman ketakutan untuk berbuat atau tidak berbuat sesuatu yang merupakan hak asasi”. Pasal tersebut menegaskan bahwa negara menjamin hak dan perlindungan terhadap privasi individu warga negaranya.

Menurut Undang-Undang No. 27 Tahun 2022 tentang Perlindungan Data Pribadi

Sebelum pengesahan Undang-Undang Nomor 27 Tahun 2022, pengaturan mengenai perlindungan data pribadi masih terbatas dan belum menyeluruh. Salah satu undangundang yang mencakup aspek tersebut adalah Undang-Undang Nomor 11 Tahun 2008 yang telah diamendemen dengan Undang-Undang Nomor 19 Tahun 2016. Meskipun undangundang tersebut telah mengatur perlindungan data pribadi, namun masih belum mencakup secara lengkap dan menyeluruh.

Meskipun Undang-Undang tersebut melarang tindakan-tindakan yang berkaitan dengan data pribadi, namun masalah utamanya adalah bahwa Undang-Undang tersebut tidak memberikan definisi yang jelas tentang apa yang dimaksud dengan data pribadi. Karena itu, penggunaan Undang-Undang ini dalam kasus perselisihan atau tindak pidana dapat menyulitkan pihak yang mengajukan gugatan atau melaporkan kejadian, karena sulit untuk membuktikan hal tersebut. Oleh karena itu, diperlukan undang-undang yang secara komprehensif mengatur tentang perlindungan data pribadi. Di Indonesia, telah disahkan Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi yang mengatur secara lebih lengkap mengenai hal ini.

Negara Kesatuan Republik Indonesia, sesuai dengan prinsip-prinsip Pancasila dan Undang-Undang Dasar Negara Republik Indonesia Tahun 1945, memiliki tanggung jawab untuk memberikan perlindungan dan pengakuan terhadap penetapan status pribadi dan hukum setiap peristiwa kependudukan dan peristiwa penting yang dialami oleh warga yang

berada di dalam maupun di luar wilayah negara ini. Informasi yang terkait dengan masalah kependudukan sangat penting untuk organisasi dan administrasi yang efisien. Sesuai dengan Undang-Undang Nomor 24 tahun 2013 tentang Administrasi Kependudukan, kegiatan administrasi kependudukan mencakup proses pengaturan dan penataan dokumen serta data kependudukan melalui pendaftaran penduduk, pencatatan sipil, manajemen informasi administrasi kependudukan, dan penggunaan hasilnya untuk pelayanan publik serta pembangunan sektor lainnya.

Pendaftaran penduduk merupakan tanggung jawab pemerintah daerah, dimulai dari tingkat desa atau kelurahan sebagai pusat kegiatan pendaftaran penduduk, sehingga setiap warga dapat didaftarkan secara administratif. Sistem administrasi kependudukan yang ada akan menghasilkan data kependudukan yang akurat, termasuk data jumlah penduduk, kondisi ekonomi, tingkat pendidikan, dan lain-lain. Data yang akurat tersebut penting untuk mendukung pelaksanaan kebijakan atau program pemerintah lainnya. Dokumen kependudukan adalah dokumen resmi yang dikeluarkan oleh instansi pemerintah yang memiliki kekuatan hukum sebagai bukti otentik yang berasal dari proses pendaftaran penduduk dan pencatatan sipil.

Meskipun Undang-Undang Informasi dan Transaksi Elektronik (ITE) belum secara spesifik mengatur perlindungan data pribadi, namun secara tidak langsung undang-undang ini memunculkan pemahaman baru tentang pentingnya melindungi data atau informasi elektronik, baik yang bersifat umum maupun pribadi. Perlindungan data pribadi dalam konteks sistem elektronik melibatkan upaya untuk mencegah penggunaan tanpa izin, perlindungan oleh penyelenggara sistem elektronik, dan perlindungan dari akses ilegal dan intervensi. Terkait dengan perlindungan dari penggunaan tanpa izin, Pasal 26 dari Undang-Undang Nomor 11 tahun 2008 tentang Informasi dan Transaksi Elektronik mensyaratkan bahwa penggunaan data pribadi dalam konteks media elektronik harus memperoleh izin dari pemilik data yang bersangkutan. Pelanggaran terhadap ketentuan ini dapat mengakibatkan tuntutan atas kerugian yang ditimbulkan.

Dengan tegas, undang-undang ITE menyatakan bahwa penyadapan (*interception*) merupakan tindakan yang dilarang, kecuali dilakukan oleh pihak yang memiliki wewenang dalam konteks upaya hukum. Berdasarkan undang-undang ITE ini, setiap orang dilarang untuk membuka informasi milik individu lain dengan cara apapun, bahkan jika informasi tersebut bersifat rahasia, kecuali dalam situasi di mana data tersebut terbuka secara publik.

3.2. Penegakan Hukum Terhadap Pelaku Penyebaran Data Pribadi Seseorang Melalui Internet (*Doxing*) di Indonesia

Penegakan hukum adalah proses yang bertujuan untuk menerapkan norma-norma hukum secara konkret sebagai panduan perilaku dalam berinteraksi atau menjalani hubungan hukum dalam kehidupan sosial dan negara. Soerjono Soekanto menggambarkan penegakan hukum sebagai upaya untuk mengatur hubungan antara nilai-nilai yang terwujud dalam aturan yang mapan dengan perilaku yang diterapkan sebagai langkah terakhir dalam mengimplementasikan nilai-nilai tersebut, dengan tujuan untuk menciptakan, memelihara, dan menjaga kedamaian dalam kehidupan bermasyarakat. Sistem penegakan hukum ini

melibatkan koordinasi antara nilai-nilai yang terdapat dalam aturan dengan perilaku manusia, di mana aturan-aturan tersebut kemudian menjadi pedoman atau standar bagi perilaku yang dianggap pantas atau tepat. Perilaku atau tindakan tersebut bertujuan untuk memelihara dan mempertahankan kedamaian yang telah terbentuk dalam masyarakat.

Sistem penegakan hukum yang efektif melibatkan koordinasi antara nilai-nilai, aturan, dan perilaku manusia dalam kehidupan sehari-hari. Manusia pada dasarnya memiliki pandangan tertentu tentang apa yang benar dan salah, dan dalam pandangan tersebut terkandung nilai-nilai yang perlu diaplikasikan secara konkret dalam kaidah-kaidah hukum yang mengatur perintah, larangan, atau hal yang diizinkan. Kaidah-kaidah ini menjadi standar atau pedoman bagi perilaku manusia yang dianggap sesuai atau patut. Perilaku dan tindakan manusia bertujuan untuk menciptakan, memelihara, dan menjaga perdamaian dalam masyarakat.

Pemahaman tentang penegakan hukum dapat dilihat dari dua sudut pandang: secara objektif, yang mencakup makna luas dan makna sempit. Dalam konteks luas, penegakan hukum mencakup nilai-nilai keadilan yang tercermin dalam aturan hukum formal dan juga nilai-nilai keadilan yang hidup dalam masyarakat. Sedangkan dalam konteks sempit, penegakan hukum hanya mengacu pada penerapan aturan hukum formal yang tertulis. Oleh karena itu, terjemahan frasa "*Law enforcement*" ke dalam bahasa Indonesia lebih cocok menggunakan istilah "penegakan hukum" dalam arti luas, sementara dalam arti sempit istilah yang lebih tepat adalah "penegakan peraturan".

Perkembangan internet dan media sosial telah memunculkan berbagai bentuk kejahatan baru yang dikenal sebagai *cybercrime*. Contohnya termasuk penipuan *online*, *carding*, *cracking*, dan *doxing*, yang mendorong kebutuhan untuk adanya regulasi yang lebih ketat seperti Undang-Undang Informasi dan Transaksi Elektronik (UU ITE). *Doxing*, misalnya, diatur dalam Pasal 27 ayat 4 UU No. 11 tahun 2008 Jo UU No. 19 tahun 2016, yang melarang individu untuk menyebarkan data pribadi seseorang dengan tambahan muatan ancaman. *Doxing* umumnya menimpa individu-individu yang berpengaruh seperti wartawan, politikus, artis, dan kelompok-kelompok berpengaruh, dan kadang-kadang dilakukan oleh masyarakat umum untuk tujuan intimidasi terhadap korban. Data yang dikumpulkan kemudian dipublikasikan secara bertahap dengan informasi yang memicu orang lain untuk melakukan intimidasi terhadap korban *doxing* tersebut. UU ITE menetapkan tindak pidana dalam bidang *cybercrime* dan menetapkan sifat kejahatan serta penyerangan terhadap berbagai kepentingan hukum melalui rumusan-rumusan tindak pidana tertentu.

UU No. 39 Tahun 1999 Tentang Hak Asasi Manusia, dalam Pasal 29 ayat (1) menyatakan bahwa "Setiap orang berhak atas perlindungan data pribadi" maka dalam pernyataan tersebut, dapat ditarik kesimpulan mengenai perlindungan atas penyebaran data pribadi merupakan hak (*privacy rights*) yang dimiliki setiap orang yang harus dilindungi oleh Negara, dimana dalam *privacy rights* setiap orang memiliki hak untuk menutup atau merahasiakan hal-hal yang sifatnya pribadi".

Perlindungan atas penyebaran data pribadi diatur dalam UU No. 19 Tahun 2016 atas Perubahan atas Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi Dan

Transaksi Elektronik, yang tercantum dalam Pasal 26 ayat (1) dan (2) yang menyatakan bahwa: 1) Kecuali ditentukan lain oleh peraturan perundang-undangan, penggunaan setiap informasi melalui media elektronik yang menyangkut data pribadi seseorang harus dilakukan atas persetujuan Orang yang bersangkutan. 2) Setiap Orang yang melanggar haknya sebagaimana dimaksud pada ayat (1) dapat mengajukan gugatan atas kerugian yang ditimbulkan berdasarkan Undang-Undang ini.

Ketentuan yang diatur tersebut memberikan hak kepada pemilik data pribadi untuk menjaga kerahasiaan informasi mereka. Jika data pribadi telah tersebar dan disalahgunakan oleh pihak lain, pemilik data pribadi berhak mengajukan gugatan ke pengadilan. Gugatan tersebut diajukan dalam bentuk gugatan perdata sesuai dengan peraturan perundang-undangan yang berlaku. Pasal tersebut memberikan perlindungan umum terhadap data pribadi seseorang, sehingga dalam setiap transaksi elektronik yang melibatkan data pribadi, penting untuk menjaga dan melindungi kerahasiaan data tersebut. Dengan pengaturan ini, setiap individu memiliki hak untuk menyimpan, merawat, dan menjaga kerahasiaan data mereka, dan setiap penggunaan data pribadi harus sesuai dengan persetujuan dari pemiliknya dan harus dijaga kerahasiaannya.

Seperti yang diuraikan sebelumnya bahwa Indonesia sendiri telah mengatur *doxing* atau penyebaran data pribadi di dalam Undang-Undang Informasi dan Transaksi Elektronik Nomor 11 Tahun 2008 Pasal 27 yang menyatakan bahwa:

1. Setiap Orang dengan sengaja dan tanpa hak mendistribusikan dan/atau mentransmisikan dan/atau membuat dapat diaksesnya Informasi Elektronik dan/atau Dokumen Elektronik yang memiliki muatan yang melanggar
2. Setiap Orang dengan sengaja dan tanpa hak mendistribusikan dan/atau mentransmisikan dan/atau membuat dapat diaksesnya Informasi Elektronik dan/atau Dokumen Elektronik yang memiliki muatan perjudian.
3. Setiap Orang dengan sengaja dan tanpa hak mendistribusikan dan/atau mentransmisikan dan/atau membuat dapat diaksesnya Informasi Elektronik dan/atau Dokumen Elektronik yang memiliki muatan penghinaan dan/atau pencemaran nama baik.
4. Setiap Orang dengan sengaja dan tanpa hak mendistribusikan dan/atau mentransmisikan dan/atau membuat dapat diaksesnya Informasi Elektronik dan/atau Dokumen Elektronik yang memiliki muatan pemerasan dan/atau pengancaman.”

Beberapa elemen dalam Pasal 27 yang dilihat sebagai tindakan *doxing* yang melanggar hukum adalah sebagai berikut:

1. Setiap orang
2. Melawan hukum
3. Mendistribusikan dokumen elektronik
4. Berisi muatan ancaman

Pasal 27 menghadirkan penjelasan yang tidak jelas, sehingga direvisi karena bisa menjadi ambigu dan dapat dimanfaatkan korban untuk menjerat pelaku yang tidak sengaja melakukan doxing. Revisi pada Pasal 27 ini bertujuan untuk mengklarifikasi makna dari

setiap unsurnya, yakni: Pasal 27 ayat 3 UU No.19 Tahun 2016

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

Dengan revisi UU ITE ini, makna Pasal 27 telah lebih jelas sehingga mempermudah proses penegakan hukum terhadap pelaku *doxing*, yang sebelumnya diatur oleh KUHP. Hukuman yang lebih berat dapat diberikan jika *doxing* mengandung unsur kekerasan atau ancaman, misalnya ancaman fisik di dunia nyata yang dapat dikenai pasal 368 KUHP dengan ancaman hukuman penjara maksimal 9 tahun. *Doxing* juga dapat dihukum jika melibatkan kekerasan atau ancaman, baik dalam bentuk penyebaran data pribadi atau ancaman kekerasan fisik, sesuai dengan Pasal 45 Ayat (1) UU ITE yang menyatakan bahwa: “Setiap Orang yang memenuhi unsur sebagaimana dimaksud dalam Pasal 27 ayat (1), ayat (2), ayat (3), atau ayat (4) dipidana dengan pidana penjara paling lama 6 (enam) tahun dan/atau denda paling banyak Rp1.000.000.000,00 (satu miliar rupiah).”

Undang-Undang terbaru yang mengatur tentang kejahatan *doxing* atau penyebaran data pribadi adalah Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi. *Doxing* atau penyebaran data pribadi diatur dalam Pasal 65 UU yang menyatakan : “Setiap Orang dilarang secara melawan hukum memperoleh atau mengumpulkan Data Pribadi yang bukan miliknya dengan maksud untuk menguntungkan diri sendiri atau orang lain yang dapat mengakibatkan kerugian Subjek Data Pribadi. Setiap Orang dilarang secara melawan hukum mengungkapkan Data Pribadi yang bukan miliknya. Setiap orang dilarang secara hukum menggunakan data pribadi yang bukan miliknya.” Selain itu, tindakan penggunaan data pribadi tanpa izin pemiliknya juga diatur dalam Pasal 513 KUHP sebagai pelanggaran hukum. Selain Pasal 513 KUHP, Undang-Undang Perlindungan Data Pribadi (PDP) juga memiliki ketentuan yang relevan terhadap *doxing*. Menurut UU PDP, pelaku *doxing* bisa dikenakan hukuman pidana penjara maksimal 5 tahun atau denda maksimal lima miliar rupiah jika terlibat dalam pengumpulan dan penyebaran data pribadi, dan pidana penjara hingga 4 tahun dan denda hingga empat miliar rupiah jika hanya terlibat dalam penyebaran data pribadi hasil pengumpulan tersebut.

Pasal 67 menjelaskan peraturan hukuman bagi pelaku *doxing* yang dikenal sebagai mereka yang menghimpun informasi pribadi individu dan menyingkapkan informasi tersebut tanpa izin: “Setiap Orang yang dengan sengaja dan melawan hukum memperoleh atau mengumpulkan Data Pribadi yang bukan miliknya dengan maksud untuk menguntungkan diri sendiri atau orang lain yang dapat mengakibatkan kerugian Subjek Data Pribadi sebagaimana dimaksud dalam Pasal 65 ayat (1) dipidana dengan pidana penjara paling lama 5 (lima) tahun dan/atau pidana denda paling banyak Rp5.000.000.000,00 (lima miliar rupiah). (2) Setiap Orang yang dengan sengaja dan melawan hukum mengungkapkan Data Pribadi yang bukan miliknya sebagaimana dimaksud dalam Pasal 65 ayat (2) dipidana dengan pidana penjara paling lama 4 (empat) tahun dan/atau pidana denda paling banyak

Rp4.000.000.000,00 (empat miliar rupiah). (3) Setiap Orang yang dengan sengaja dan melawan hukum menggunakan Data Pribadi yang bukan miliknya sebagaimana dimaksud dalam Pasal 65 ayat (3) dipidana dengan pidana penjara paling lama 5 (lima) tahun dan/atau pidana denda paling banyak Rp.5.000.000.000,00 (lima miliar rupiah)”

4. KESIMPULAN

1. Doxing adalah kejahatan yang menggunakan teknologi untuk mengungkapkan informasi pribadi seseorang tanpa melakukan kontak fisik. Tujuan utamanya bervariasi, seperti untuk tujuan hiburan, untuk membongkar individu, dan sebagainya. Oleh karena itu, penegakan hukum terhadap kasus doxing dan penyebaran data pribadi harus dilakukan secara tuntas, agar korban mendapat keadilan dan pelaku mendapat hukuman yang pantas. Praktik doxing diatur dalam Undang-Undang Informasi dan Transaksi Elektronik (UU ITE) dan Undang-Undang Perlindungan Data Pribadi (UU PDP), khususnya dalam Undang-Undang Nomor 19 Tahun 2016 tentang Perubahan atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi Dan Transaksi Elektronik, serta secara lebih rinci dalam Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi.
2. Di Indonesia, regulasi terkait dengan kejahatan cyber, termasuk doxing, tertuang dalam Undang-Undang (UU) Nomor 19 Tahun 2016 Tentang Perubahan Atas UU Nomor 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik (UU ITE). UU ITE menetapkan larangan-larangan dan sanksi-sanksinya. Selain itu, doxing juga diatur dalam Undang-Undang Nomor 27 Tahun 2022 Tentang Perlindungan Data Pribadi (UU PDP).

UU ITE memberlakukan sanksi pidana, seperti yang diuraikan berikut ini:

- Pasal 30 ayat (1) jo. Pasal 46 ayat (1) UU ITE mengancam hukuman penjara maksimal 6 tahun dan denda maksimal Rp 600 juta bagi mereka yang melakukan akses ilegal terhadap sistem elektronik milik orang lain.
- Pasal 30 ayat (2) jo. Pasal 46 ayat (2) UU ITE mengancam hukuman penjara maksimal 7 tahun dan/atau denda maksimal Rp 700 juta bagi mereka yang melakukan akses ilegal terhadap komputer dan/atau sistem elektronik dengan maksud memperoleh informasi dan/atau dokumen elektronik.
- Pasal 30 ayat (3) jo. Pasal 46 ayat (3) UU ITE mengancam hukuman penjara maksimal 8 tahun dan denda maksimal Rp 800 juta bagi mereka yang melakukan tindakan melawan hukum seperti penerobosan, melampaui batas, atau penjeblolan terhadap sistem pengamanan komputer.

Ancaman hukuman yang lebih berat, berupa penjara maksimal 10 tahun dan/atau denda hingga Rp 800 juta, diberlakukan untuk intersepsi atau penyadapan sistem elektronik orang lain, sebagaimana diatur dalam Pasal 31 ayat (1) jo. Pasal 47 UU ITE. Pasal 32 ayat (1) jo. Pasal 48 ayat (1) mengancam hukuman penjara maksimal 8 tahun dan denda hingga Rp 2 miliar atas perbuatan melawan hukum seperti mengubah, menambah, atau merusak informasi elektronik orang lain. Sementara Pasal 32 ayat (2) jo. Pasal 48 ayat (2) mengancam hukuman penjara maksimal 9 tahun

dan denda hingga Rp 3 miliar bagi siapa pun yang tanpa hak memindahkan atau mentransfer informasi elektronik kepada sistem elektronik yang tidak berhak. Pasal 32 ayat (3) jo. Pasal 48 ayat (3) UU ITE menetapkan hukuman penjara maksimal 10 tahun dan denda hingga Rp 5 miliar bagi mereka yang membuka akses informasi elektronik yang seharusnya bersifat rahasia.

Dalam UU PDP, larangan termasuk memperoleh atau mengumpulkan data pribadi yang bukan miliknya, dengan maksud menguntungkan diri sendiri atau orang lain, yang dapat mengakibatkan kerugian bagi subjek data pribadi.

DAFTAR PUSTAKA

- [1] Abdul Halim Barkatullah, *Perlindungan Hukum Bagi Konsumen Dalam Transaksi Ecommerce Lintas Negara di Indonesia*, FH UII Press, Yogyakarta, 2009.
- [2] Agus Rahardjo, *Cybercrime Pemahaman dan Upaya Pencegahan Kejahatan Berteknologi*, PT.Citra Aditya Bakti, Bandung, 2003
- [3] Barda Nawawi Arief, *Masalah Penegakan Hukum dan Kebijakan Hukum Pidana dalam Penanggulangan Kejahatan*, Kencana Prenada Media Group, Jakarta, 2007.
- [4] Budi Agus Riswandi, *Hukum dan Internet di Indonesia*, UII Press, Yogyakarta, 2003.
- [5] Eka N.A.M Sihombing dan Cynthia Hadita, *Penelitian Hukum*, Setara Pers, Malang, 2022.
- [6] Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi.
- [7] Undang-Undang Nomor 19 Tahun 2016 tentang Informasi dan Transaksi Elektronik
- [8] Undang-Undang Nomor 39 Tahun 1999 tentang Hak Asasi Manusia
- [9] Undang-Undang No 23 Tahun 2006 jo UU No. 24 Tahun 2013 tentang Administrasi Kependudukan.
- [10] Undang-undang Nomor 14 Tahun 2008 tentang Keterbukaan Informasi Publik