Jurnal Darma Agung
Volume: 32, Nomor: 5, (2024), Oktober: 243 - 252
https://dx.doi.org.10.46930/ojsuda.v32i5.4794

P-ISSN:0852-7296
E-ISSN:2654-3915

TINJAUAN YURIDIS PERLINDUNGAN DATA PRIBADI DALAM TINDAKAN *DOXING* BERDASARKAN UNDANG UNDANG NOMOR 27 TAHUN 2022

Firman B. W. Panjaitan [1)], Krisna Sitorus [2)], Yanti Agustina [3)], Chirs Anggi Natalia B [4)]
Fakultas Hukum Universitas Prima Indonesia, Medan, Indonesia [1,2,3)]
Fakultas Hukum Universitas Kristen Indonesia, Jakarta, Indonesia [4)]
Corresponding Author:
firman.b.w.panjaitan@gmail.com [1)], *krisnasitorus20@gmail.com* [2)],
yantiagustina@unprimdn.ac.id [3)], *chris.angginatalia@uki.ac.id* [4)]

Abstrak

Perlindungan data pribadi sangat penting di era digital yang terus berkembang. Data pribadi mencakup informasi yang bisa mengenali individu, baik secara langsung maupun tidak langsung. Saat ini, penyalahgunaan data pribadi seperti doxing sering terjadi tanpa izin. Oleh karena itu, penelitian ini mengeksplorasi dampak hukum dari doxing berdasarkan Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi, serta langkah-langkah perlindungan yang sesuai dengan undang-undang yang berlaku. Penelitian ini memiliki pendekatan hukum normatif. Sesuai dengan Pasal 28 G ayat 1 Undang-Undang Dasar Negara Republik Indonesia Tahun 1945, setiap individu memiliki hak atas perlindungan diri, keluarga, kehormatan, martabat, serta harta benda yang berada dalam kekuasaannya. Selain itu, setiap individu berhak atas rasa aman serta perlindungan dari segala ancaman ketakutan untuk melakukan atau tidak melakukan sesuatu, yang merupakan hak asasi manusia yang terkait dengan privasi individu. Dampak hukum dari doxing sesuai dengan Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi adalah pelaku doxing dapat dikenai sanksi pidana sesuai dengan Pasal 67 ayat (1) dan (2), yang meliputi pidana penjara hingga lima tahun atau denda maksimal lima miliar rupiah. Untuk menghindari doxing, langkah-langkah perlindungan data pribadi yang dapat diambil termasuk menggunakan media sosial secara bijaksana dan menerapkan kata sandi yang kuat untuk setiap akun media sosial. Oleh karena itu, kesadaran bersama dan dukungan dalam menjaga keamanan data pribadi sangat penting.

Kata kunci: Perlindungan, Data Pribadi, Tindakan *Doxing*

Abstract

Protecting personal data is critical in today's swiftly advancing digital era. Personal data encompasses information that can directly or indirectly identify an individual. Unfortunately, there is frequent unauthorized exploitation of personal data, such as through doxing. This research investigates the legal implications of doxing under Law Number 27 of 2022 on Personal Data Protection and explores protective measures outlined in this legislation. The study employs a normative legal approach. Article 28G paragraph 1 of the 1945 Constitution of the Republic of Indonesia guarantees individuals the right to protect themselves, their families, honor, dignity, and property under their control. It also ensures the right to security and protection from all forms of intimidation to act or refrain from acting, thereby safeguarding personal privacy as a fundamental human right. According to Law Number 27 of 2022 on Personal Data Protection, the legal repercussions of doxing include criminal sanctions detailed in Article 67 paragraphs (1) and (2), which prescribe penalties of up to five years' imprisonment or fines up to five billion rupiahs. To prevent doxing, proactive measures involve prudent use of social media platforms and implementation of robust passwords for each account. Therefore, maintaining awareness and mutual support are crucial for upholding personal data security.

Keywords: Protection, Personal Data, Doxing

PENDAHULUAN

Data pribadi adalah hal yang sangat penting karena berkaitan erat dengan privasi tiap individu. Privasi ini dianggap sebagai hak pribadi yang dilindungi oleh Pasal 28G ayat 1 Undang-Undang Dasar Negara Republik Indonesia Tahun 1945. Selain itu, setiap orang berhak merasa aman dan terlindungi dari segala ancaman yang dapat menimbulkan ketakutan untuk bertindak atau tidak bertindak. Privasi, atau hak pribadi ini, dapat diartikan sebagai hak atas kebebasan pribadi. Hak privasi juga berkaitan

History:
Received : 25 Maret 2024
Revised : 10 Mei 2024
Accepted : 23 Juni 2024
Published : 27 Oktober 2024

Publisher: LPPM Universitas Darma Agung

dengan kebutuhan spiritual manusia, termasuk kebutuhan untuk dihormati dalam perasaan, pemikiran, dan hak untuk menikmati kehidupan, yang sering dikenal sebagai "the right to be let alone."

Berbagai sektor kehidupan telah mengadopsi sistem teknologi informasi, seperti e-commerce di sektor perdagangan atau bisnis, e-education di bidang pendidikan, e-health di bidang kesehatan, e-government di bidang pemerintahan, dan penerapan teknologi informasi dalam bidang-bidang lainnya. Penggunaan teknologi informasi memungkinkan pengumpulan dan transfer data pribadi dengan mudah dari satu entitas ke entitas lain tanpa pengetahuan subjek data pribadi, yang dapat mengancam hak konstitusional mereka.

Perkembangan tersebut ibarat pisau bermata dua; meskipun media interaksi berbasis internet membawa banyak manfaat, ada sisi negatifnya jika negara tidak mampu mengelola dan memanfaatkannya dengan baik. Fenomena pesatnya perkembangan teknologi informasi telah mencakup seluruh belahan dunia. Perlindungan data pada dasarnya bertujuan untuk menjaga hal-hal yang bersifat pribadi. Definisi ini sering disebut sebagai privasi informasi karena fokusnya pada informasi atau data pribadi.

Dari segi hukum, privasi adalah hak individu untuk mengontrol apakah informasi tentang dirinya dapat dibagikan untuk kepentingan publik. Masyarakat diharapkan untuk mematuhi ketentuan Pasal 28G ayat 1 UUD 1945 yang menyediakan landasan konstitusional mengenai hak privasi individu. Saat ini, data pribadi sering kali disalahgunakan, termasuk melalui praktik doxing.

Doxing adalah kejahatan berbasis internet yang bertujuan untuk menyebarluaskan informasi seseorang dengan maksud untuk merugikan atau menjatuhkan orang tersebut. Undang-undang juga mengatur beberapa jenis informasi publik yang dapat mengungkapkan privasi pribadi seseorang, sesuai dengan yang diatur dalam Pasal 17 huruf H Undang-Undang No 14 tahun 2008 tentang keterbukaan informasi publik. Komisi Nasional Hak Asasi Manusia (Komnas HAM) mengidentifikasi doxing sebagai bentuk pelanggaran Hak Asasi Manusia di dunia digital karena kemampuannya untuk menyebabkan kerugian dan merendahkan martabat individu.

Doxing pada umumnya dilakukan dengan tujuan spesifik, seperti untuk mengintimidasi atau meneror seseorang. Teknologi modern memudahkan pelaku untuk mengumpulkan dan menyebarkan informasi pribadi secara luas, karena akses internet yang mudah diperoleh oleh banyak orang. Doxing sering kali terjadi di Indonesia sebagai kejahatan yang cukup umum, walaupun banyak orang masih kurang menyadari konsekuensinya. Hal ini menunjukkan bahwa doxing dapat mengancam privasi dan keamanan individu yang terlibat dalam kegiatan publik atau berbicara tentang isu-isu sensitif. Oleh karena itu, penting untuk memperlakukan perlindungan data pribadi sebagai bagian dari langkah-langkah preventif untuk mengurangi dampak kejahatan doxing. Doxing memiliki dampak serius, seperti menyebabkan rasa malu, diskriminasi, cyberstalking dan fisik stalking, pencurian identitas, penipuan keuangan, merusak reputasi, meningkatkan kecemasan, dan mengurangi harga diri. Contoh nyata dari kejahatan cyber yang berbahaya adalah doxing, yang bisa berujung pada cyberbullying dan penyebaran data pribadi secara luas di internet. Dengan latar belakang ini, penulis tertarik untuk melakukan penelitian dengan judul: "Tinjauan Yuridis Perlindungan Data Pribadi dalam Tindakan Doxing berdasarkan Undang-Undang Nomor 27 Tahun 2022."

METODE PENELITIAN

A. Jenis Penelitian

Metode penelitian yang digunakan oleh penulis untuk menjawab permasalahan yang dihadapi adalah pendekatan penelitian yuridis normatif. Pendekatan ini difokuskan pada penerapan kaidah-kaidah atau norma-norma yang terdapat dalam

hukum positif. Dalam konsep ini, hukum dipandang sebagai suatu sistem normatif yang eksis secara mandiri, tertutup, dan terlepas dari realitas kehidupan masyarakat.

Penelitian ini sepenuhnya mengacu pada peraturan-peraturan tertulis, sehingga sangat bergantung pada sumber data sekunder yang diperoleh dari perpustakaan. Dalam konteks penelitian hukum normatif, aspek-aspek hukum tertulis dianalisis dari berbagai perspektif seperti teori, filosofi, perbandingan, struktur/komposisi, konsistensi, penjelasan umum dan penjelasan pada setiap pasal, formalitas, kekuatan mengikat suatu undang-undang, serta bahasa yang digunakan dalam konteks hukum. Penelitian hukum normatif memiliki cakupan yang luas dengan objek yang terfokus pada doktrin, asas, dan prinsip-prinsip hukum.

B. Sumber Bahan Hukum

Data yang digunakan dalam penelitian ini berasal dari sumber data sekunder. Data sekunder merujuk kepada informasi yang diperoleh melalui studi kepustakaan, dan memiliki validitas hukum yang bersumber dari bahan hukum primer, bahan hukum sekunder, dan bahan hukum tersier.

Data sekunder meliputi bahan-bahan sebagai berikut:

1. Bahan hukum primer: Bahan hukum primer, yaitu bahan-bahan hukum yang mempunyai otoritas. Adapun bahan hukum primer yang digunakan dalam penelitian terdiri dari:
   a. Undang-Undang Dasar 1945;
   b. Undang-Undang Nomor 27 Tahun 2022 tentang perlindungan data pribadi
   c. UU Nomor 11 Tahun 2008 jo. UU Nomor 19 Tahun 2016 UU Tentang Informasi dan Transaksi Elektronik (UU ITE);
2. Bahan Hukum Sekunder: Bahan hukum sekunder, yaitu bahan hukum yang menjelaskan bahan hukum primer. Adapun bahan hukum sekunder yang digunakan dalam penelitian ini terdiri dari:
   a. Buku-buku teks;
   b. Jurnal hukum;
   c. Skripsi, tesis dan disertasi
3. Bahan Hukum Tersier: Bahan hukum tersier, yaitu bahan hukum yang memberi petunjuk atau penjelasan terhadap bahan hukum primer dan bahan hukum sekunder. Adapun bahan hukum tersier yang digunakan dalam penelitian ini terdiri dari:
   a. Kamus hukum
   b. Ensiklopedia Indonesia
   c. Kamus Besar Bahasa Indonesia

C. Teknik pengumpulan data

Pengumpulan data dalam penulisan jurnal ini dilakukan melalui metode studi kepustakaan. Studi kepustakaan adalah pendekatan pengumpulan data yang memanfaatkan sumber-sumber tertulis, dengan menerapkan teknik analisis konten.

D. Analisis Data

Teknik analisis data dalam penulisan jurnal ini menggunakan pendekatan analisis kualitatif. Penelitian kualitatif mengacu pada interpretasi norma hukum yang terdapat dalam peraturan perundang-undangan dan putusan pengadilan, serta norma-norma yang berlaku dan berkembang dalam masyarakat secara umum.

HASIL DAN PEMBAHASAN

1. Akibat hukum atas tindakan doxing menurut Undang-Undang Nomor 27 Tahun 2022 Tentang Perlindungan Data Pribadi

Perkembangan teknologi saat ini berpengaruh besar terhadap cara berpikir masyarakat, terlihat dari kemudahan mereka dalam mengakses informasi melalui telepon seluler. Penggunaan teknologi saat ini memiliki dampak positif dan negatif yang signifikan. Fenomena ini telah menarik perhatian dalam konteks hukum, etika, dan keamanan informasi di era kemajuan teknologi saat ini. Masalah keamanan data pribadi menjadi semakin penting untuk diperhatikan.

Pemerintah telah mengambil langkah untuk melarang dan mengatur praktik doxing karena dampak negatifnya terhadap privasi individu dan ikeamanan informasi. Di Indonesia, pelanggaran doxing dapat dikenai sanksi berupa denda, hukuman penjara, atau keduanya, tergantung pada Undang-Undang yang mengaturnya. Beberapa undang-undang yang relevan termasuk Undang-Undang No 19 Tahun 2016 tentang Perubahan atas Undang-Undang No 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik, Undang-Undang No 27 Tahun 2022 tentang Perlindungan Data Pribadi, dan Undang-Undang No 23 Tahun 2013 tentang Administrasi Kependudukan.

a. Undang-Undang Nomor 19 Tahun 2016
   1) Pasal 26 Ayat (1) Undang-Undang No. 19 Tahun 2016 Tentang Informasi dan Transaksi Elektronik (UU ITE), Pasal 26 Ayat (1) UU ITE menyatakan: "Kecuali ditentukan oleh undang-undang, penggunaan informasi melalui media elektronik mengenai informasi pribadi seseorang harus atas persetujuan yang bersangkutan." Isi pasal ini dimaksudkan untuk melindungi hak individu terhadap penggunaan informasi pribadi yang tidak sah.
   2) Pasal 27 Ayat (4) Undang-Undang No. 19 Tahun 2016 Tentang Informasi dan Transaksi Elektronik (UU ITE), Pasal 27 Ayat (4) Pasal ini menyatakan bahwa "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, dipidana dengan pidana penjara paling lama 4 (empat) tahun dan/atau denda paling banyak Rp750.000.000,- (tujuh ratus lima puluh juta rupiah)".
   3) Pasal 45 Ayat (1) Undang-Undang No. 19 Tahun 2016 Tentang Informasi dan Transaksi Elektronik (UU ITE), Pasal 45 Ayat (1) Undang-Undang No. 19 Tahun 2016 Tentang Informasi dan Transaksi Elektronik (UU ITE) 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 Rp.1.000.000.000,00 (satu miliar rupiah)". Pasal ini mengatur tentang pidana bagi pelaku yang melakukan tindakan penghinaan, pencemaran nama baik, atau perbuatan teror online yang melanggar Pasal 27 Ayat (1), Ayat (2), Ayat (3), atau Ayat (4) UU ITE. Pasal 45 Ayat (1) UU ITE bertujuan untuk memberikan sanksi pidana bagi pelaku yang melakukan tindakan yang merugikan individu atau kelompok melalui media elektronik.

b. Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi (UU PDP);
   1) Pasal 1 Ayat (1) Ke-1 Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi (UU PDP), menyatakan bahwa "Data Pribadi merupakan 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".Data pribadi yang dapat diidentifikasi sendiri atau digabungkan dengan informasi lain, baik secara langsung

atau tidak langsung melalui sistem elektronik atau non-elektronik, mencakup informasi seperti nama, alamat, nomor. ponsel, email, foto dan hal-hal lain yang dapat mengungkap identitas seseorang.

2) Pasal 4 Ayat (2) Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi (UU PDP), Isi pasal ini mengatur tentang kewajiban pengolah data yang bertanggung jawab untuk menjaga kerahasiaan data pribadi yang ditanganinya sesuai dengan kriteria yang ditentukan dalam peraturan perundang-undangan. Data Pribadi yang bersifat spesifik sebagaimana dimaksud pada ayat (l) huruf a meliputi data dan informasi kesehatan; data biometrik; data genetika; catatan kejahatan; data anak;data keterangan pribadi; dan/ atau data lainnya sesuai dengan ketentuan peraturan perundang-undangan.
3) Pasal 65 Ayat (1) & (2) Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi (UU PDP) mengatur tentang larangan dalam penggunaan data pribadi. Pasal ini menyatakan:
   a. Pasal 65 Ayat (1): "Setiap Orang dilarang membuat Data Pribadi palsu atau memalsukan Data Pribadi dengan maksud untuk menguntungkan diri sendiri atau orang lain yang dapat mengakibatkan kerugian bagi orang lain."
   b. Pasal 65 Ayat (2): "Setiap Orang yang dengan sengaja dan melawan hukum mengungkapkan Data Pribadi yang bukan miliknya dipidana dengan pidana penjara paling lama 7 (tujuh) tahun dan/atau denda paling banyak Rp 5.000.000.000,00 (lima miliar rupiah)." Tujuan dari pasal ini adalah untuk melindungi data pribadi dari pemalsuan dan pengungkapan yang tidak sah, dan untuk memberikan hukuman pidana atas pelanggaran larangan ini. Hal ini merupakan bagian dari upaya melindungi hak konstitusional atas data dan mencegah penyalahgunaan data pribadi yang dapat merugikan orang lain.
4) Pasal 67 Ayat (1) & (2) Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi (UU PDP) mengatur tentang larangan dalam penggunaan data pribadi. Pasal ini menyatakan:
   a. Pasal 67 Ayat (1): "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 bagi orang lain."
   b. Pasal 67 Ayat (2): "Setiap orang yang dengan sengaja dan melawan hukum menggunakan Data Pribadi yang bukan miliknya dipidana dengan pidana penjara paling lama 7 (tujuh) tahun dan/atau denda paling banyak Rp 5.000.000.000,00 (lima miliar rupiah)."
5) Pasal 69 Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi (UU PDP), menyatakan bahwa “Selain dijatuhi pidana sebagaimana dimaksud dalam Pasal 67 dan Pasal 68 juga dapat dijatuhi pidana tambahan berupa perampasan keuntungan dan/ atau harta kekayaan yang diperoleh atau hasil dari tindak pidana dan pembayaran ganti kerugian”.

Korban doxing dapat mengajukan gugatan perdata terhadap pelaku untuk mendapatkan kompensasi atas kerugian yang disebabkan. Doxing, yang melibatkan penggunaan informasi pribadi seseorang tanpa izin melalui media elektronik, dapat mengakibatkan pertanggungjawaban hukum berdasarkan Pasal 26 ayat 2 PMH dan Pasal 1365 KUHPerdata, yang menuntut penggantian kerugian baik materiil (terhadap harta benda) maupun immateriil (seperti rasa takut atau trauma).

Selain itu, Peraturan Menteri Kominfo No. 20 Tahun 2016 juga mengatur bahwa penggunaan data pribadi tanpa hak dapat dikenai sanksi administratif sesuai dengan ketentuan yang berlaku, termasuk dalam Pasal 36 yang menjelaskan jenis-jenis pelanggaran dan sanksi administratif yang dapat diterapkan. Sanksi administratif yang dapat diberlakukan sesuai dengan Peraturan Menteri Kominfo No. 20 Tahun 2016 termasuk:

a. Peringatan lisan;
b. Peringatan tertulis;
c. Penghentian sementara kegiatan; dan/atau
d. Pengumuman di situs dalam jaringan (website online).

Undang-Undang yang dibuat oleh pemerintah bertujuan menjadi landasan hukum yang komprehensif bagi masyarakat Indonesia dalam melindungi hak privasi dari tindakan doxing. Undang-undang ini menjamin hak privasi individu dengan mengatur bahwa penggunaan data pribadi hanya boleh dilakukan dengan persetujuan dari pemiliknya. Setiap individu memiliki hak atas perlindungan terhadap data pribadinya, yang merupakan bagian dari hak privasi yang seharusnya dijaga dan dilindungi dengan baik. Dalam menegakkan hukum terhadap pelaku doxing, undang-undang memberikan sanksi yang tegas dan efektif. Hal ini bertujuan untuk mencegah terjadinya tindakan doxing yang dapat menimbulkan kerugian bagi seluruh lapisan masyarakat Indonesia.

2. Upaya Yang Dapat Dilakukan Untuk Melindungi Data Pribadi Dari Tindakan Doxing Berdasarkan Undang - Undang Nomor 27 Tahun 2022 Tentang Perlindungan Data Pribadi

Aktivitas masyarakat yang semakin bergantung pada platform ini meningkatkan kerentanan terhadap keamanan data pribadi, baik dalam penyimpanan, penggunaan, maupun transfer data kepada pihak lain yang mendukung aktivitas atau pekerjaan mereka. Berikut ini beberapa pengertian data yang relevan:

a. Data adalah informasi yang belum memiliki makna bagi penerimanya dan memerlukan pengolahan lebih lanjut. Data dapat berupa keadaan, gambar, suara, huruf, angka, atau simbol lain yang digunakan sebagai bahan untuk melihat lingkungan, obyek, kejadian, atau konsep tertentu. (Data Protection Act Inggris 2018)
b. Menurut Webster New World Dictionary, data adalah "things known or assumed," yang berarti bahwa data adalah informasi yang dapat diketahui atau diasumsikan.
c. Dalam Undang-Undang Administrasi Kependudukan, data pribadi didefinisikan sebagai data perseorangan tertentu yang disimpan, dirawat, dan dijaga kebenarannya serta dilindungi kerahasiaannya.
d. Data pribadi adalah informasi tentang individu yang dapat diidentifikasi secara langsung atau tidak langsung, baik secara tersendiri maupun jika dikombinasikan dengan informasi lainnya.

Penggunaan internet sebagai media informasi, komunikasi, dan elektronik telah membuka berbagai peluang di berbagai sektor seperti kesehatan (e-health), pemerintahan (e-government), dan keuangan (e-payment). Selain itu, perkembangan komputasi awan (cloud computing) telah menyediakan layanan penyimpanan data seperti Google Drive, iCloud, Dropbox, YouTube, dan lainnya. Ini mencerminkan inovasi dalam teknologi informasi dan komunikasi yang memungkinkan pengumpulan, penyimpanan, pembagian, dan analisis data secara efektif dan efisien di antara industri atau perusahaan dalam masyarakat. Saat ini, data pribadi menjadi elemen krusial yang berisi informasi pribadi yang sering digunakan dalam berbagai kegiatan di platform digital. Data ini biasanya diberikan oleh pemiliknya untuk menerima layanan di media digital kepada pengendali

data, namun keamanannya tidak selalu terjamin. Risiko penyalahgunaan data pribadi bisa sulit dipertanggungjawabkan. Perlindungan data pribadi seharusnya dijamin secara hukum oleh pemerintah karena merupakan bagian dari hak asasi warga negara. Sebagai negara hukum, Indonesia harus memberikan perlindungan hukum yang sesuai dengan nilai-nilai Pancasila kepada seluruh rakyatnya.

Di Indonesia, telah disahkan Undang-Undang Nomor 27 tahun 2022 yang mengatur perlindungan data pribadi warga negara. Undang-undang ini menegaskan bahwa data pribadi dilindungi secara hukum sebagai jaminan terhadap hak dasar warga negara. Data Pribadi terdiri atas:

a. Data pribadi yang bersifat spesifik;
b. Data pribadi yang bersifat umum.
c. Data pribadi yang bersifat spesifik, seperti yang dinyatakan dalam pasal 4 undang-undang perlindungan data pribadi ayat 1 huruf a meliputi:
    1) Informasi kesehatan dan data yaitu, informasi atau catatan individu yang berkaitan dengan kesehatan fisik, kesehatan mental, dan pelayanan kesehatan.
    2) Data biometrik yaitu, data yang berkaitan dengan karakter fisik, fisiologis, dan perilaku seseorang yang memungkinkan identifikasi unik, seperti gambar wajah atau bekas sidik jari tangan. Data biometrik juga menjelaskan sifat keunikan atau karakteristik seseorang yang harus dirawat dan dijaga, namun tidak termasuk pada rekam sidik jari, retina mata, dan sampel DNA.
    3) Data genetika yaitu, mencakup semua tentang informasi karakteristik seseorang yang diwariskan dan diperoleh selama perkembangan prenatal awal.
    4) Catatan kejahatan yaitu, catatan yang tertulis tentang seorang yang pernah melakukan pelanggaran atau melanggar hukum dalam proses peradilan atas pelanggaran, seperti catatan kepolisian
    5) Data anak.
    6) Data pribadi keuangan yaitu, data yang termasuk tentang jumlah simpanan bank, seperti deposito, tabungan, atau data kartu kredit.
d. Data pribadi yang bersifat umum, seperti yang dinyatakan dalam pasal 4 undang-undang perlindungan data pribadi ayat 1 huruf a meliputi:
    a. Nama lengkap
    b. Jenis kelamin
    c. Kewarganegaraan
    d. Agama
    e. Status perkawinan

Data pribadi yang dapat dikombinasikan untuk mengidentifikasi seseorang termasuk nomor telepon atau identitas komputer dalam suatu jaringan internet (IP Address). Perlindungan data pribadi dalam sistem elektronik tidak diatur secara khusus dalam Undang-Undang ITE. Perlindungan data pribadi terkait dengan praktik doxing sangat terkait dengan privasi individu di internet. Di Indonesia, perlindungan terhadap privasi dan data pribadi diatur secara implisit dalam Pasal 28G UUD 1945 yang menegaskan hak setiap orang atas perlindungan diri pribadi, keluarga, kehormatan, martabat, dan harta benda yang berada di bawah kekuasaannya, serta hak atas rasa aman dan perlindungan dari ancaman. Regulasi perlindungan data pribadi juga mengatur berbagai aspek terkait, seperti lingkup data yang termasuk, keterlibatan pihak-pihak dalam penegakan hukum, dan konsekuensi pidana atas pelanggaran yang terjadi. Undang-undang ini bertujuan utama untuk menjaga hak-hak dasar dan kebebasan individu terkait pengolahan dan penyimpanan data pribadi, yang merujuk pada informasi yang bisa mengidentifikasi seseorang baik secara langsung maupun

tidak langsung. Berikut beberapa langkah yang dapat diambil untuk melindungi data pribadi dari tindakan doxing:

1. Peningkatan Pengetahuan dan Pemahaman: Mengadakan program edukasi dan kampanye publik tentang pentingnya melindungi data pribadi. Memberikan pelatihan kepada masyarakat mengenai praktik menjaga informasi pribadi secara online dan cara melaporkan tindakan doxing.
2. Memperkuat Kebijakan Privasi: Mengimplementasikan kebijakan privasi yang lebih kuat di platform digital dan media sosial untuk mencegah penumpukan dan penyebaran data pribadi tanpa izin. Memastikan platform online memiliki kebijakan yang jelas mengenai pelaporan dan penanganan kasus doxing.
3. Penggunaan Teknologi Keamanan: Menggunakan teknologi enkripsi untuk menjaga kerahasiaan data pribadi saat penyimpanan dan pengiriman. Menerapkan otentikasi dua faktor dan langkah-langkah keamanan lainnya untuk menghalangi akses yang tidak sah terhadap informasi pribadi.
4. Penegakan Hukum yang Ketat: Memperkuat penegakan hukum terhadap pelanggaran Undang-undang Perlindungan Data Pribadi (PDP) dengan memberlakukan sanksi yang tegas terhadap pelaku doxing. Mendirikan badan pengawas independen untuk memonitor dan menangani pelanggaran perlindungan data pribadi. Menegakkan perlindungan hukum untuk mendukung hak asasi manusia dan memastikan masyarakat dapat menikmati hak-hak mereka yang diberikan oleh hukum.
5. Kolaborasi dengan Penyedia Layanan Online: Mendorong kerja sama antara pemerintah dan penyedia layanan daring untuk mengidentifikasi dan menghapus konten yang mengandung data pribadi tanpa izin. Membangun prosedur respons cepat antara pemerintah dan penyedia layanan untuk menangani insiden doxing secara efektif.

Berikut beberapa upaya lain yang dapat dilakukan untuk melindungi data pribadi dari doxing berdasarkan Undang-Undang Perlindungan Data Pribadi (UU PDP) Nomor 27 Tahun 2022:

1. Pemetaan dan Klasifikasi Data: Identifikasi dan klasifikasikan jenis data pribadi yang Anda miliki untuk memahami tingkat sensitivitasnya. Hal ini memungkinkan Anda untuk menerapkan tingkat perlindungan yang sesuai dengan risiko yang ada.
2. Pengelolaan Izin dan Persetujuan: Pastikan untuk meminta izin atau persetujuan dari pemilik data sebelum mengumpulkan, menggunakan, atau mengungkapkan data pribadi mereka. UU PDP menetapkan bahwa pengolahan data pribadi harus didasarkan pada persetujuan yang jelas dari pemilik data.
3. Pengelolaan Keamanan Data: Terapkan standar keamanan yang tepat untuk melindungi data pribadi dari akses, penggunaan, atau pengungkapan yang tidak sah. Ini termasuk penggunaan teknologi enkripsi, firewall, dan langkah-langkah keamanan IT lainnya.
4. Keterbukaan dan Transparansi: Berikan informasi yang jelas kepada pemilik data mengenai bagaimana data pribadi mereka akan diproses, siapa yang akan mengaksesnya, dan tujuan dari pengolahan data tersebut.
5. Hak Pemilik Data: Pastikan bahwa pemilik data memiliki hak untuk mengakses, memperbaiki, menghapus, atau membatasi pengolahan data pribadi mereka sesuai dengan yang diatur dalam UU PDP. Respon terhadap permintaan ini harus dilakukan dengan cepat dan tepat.
6. Pelaporan dan Respons Terhadap Pelanggaran: Sediakan mekanisme pelaporan yang jelas bagi pemilik data jika terjadi pelanggaran keamanan yang mengancam data pribadi mereka. Tanggapi pelanggaran tersebut

dengan segera dan berkoordinasi dengan badan pengawas atau otoritas yang berwenang sesuai dengan UU PDP.

7. Pendidikan dan Pelatihan: Edukasi terus-menerus kepada karyawan dan staf tentang pentingnya perlindungan data pribadi, serta kebijakan dan prosedur yang harus diikuti untuk mencegah doxing dan pelanggaran data lainnya.
8. Audit dan Penilaian Reguler: Lakukan audit internal secara berkala untuk mengevaluasi kepatuhan terhadap kebijakan perlindungan data pribadi dan untuk memastikan bahwa sistem keamanan data berfungsi secara efektif.

Dengan mengimplementasikan langkah-langkah ini, perusahaan atau organisasi dapat meminimalkan risiko doxing dan memastikan bahwa data pribadi yang mereka kelola terlindungi sesuai dengan ketentuan UU PDP. Indonesia memberikan usaha untuk melindungi secara hukum data pribadi. Perlindungan hukum merujuk pada perlindungan yang diberikan kepada individu dalam bentuk peraturan hukum, baik sebagai langkah pencegahan maupun penindakan, yang dapat bersifat tertulis maupun tidak tertulis. Dengan melakukan langkah-langkah tersebut, pengguna dapat menjaga keamanan data pribadi mereka dari doxing dan menghentikan penyebaran informasi pribadi yang tidak sah. Mencegah doxing membutuhkan kerjasama dari individu, organisasi, dan pemerintah. Pendidikan dan kesadaran masyarakat tentang perlindungan data pribadi sangat penting. Individu perlu memahami hak-hak mereka dan cara melindungi data pribadi. Organisasi juga harus menerapkan praktik keamanan data yang kuat dan mematuhi regulasi perlindungan data pribadi. Pemerintah perlu terus memperhatikan dan mengembangkan regulasi serta infrastruktur yang mendukung perlindungan data pribadi.

SIMPULAN DAN SARAN

A. Simpulan

1. Konsekuensi hukum bagi pelaku doxing mencakup hukuman penjara maksimal tujuh tahun dan denda sebesar lima miliar rupiah, sebagaimana diatur dalam undang-undang perlindungan data pribadi. Selain itu, pelaku juga bisa dikenai sanksi administratif berupa peringatan atau pengumuman di situs web.
2. Untuk melindungi data pribadi dari doxing, ada beberapa langkah yang bisa diambil, seperti menggunakan media sosial dengan bijaksana, menerapkan teknologi keamanan yang tepat, menggunakan kata sandi yang kuat untuk setiap akun media sosial, dan memanfaatkan fitur-fitur privasi yang tersedia.

B. Saran

1. Dihimbau untuk kepada masyarakat agar tidak melakukan *doxing*, sebab apabila seseorang melakukan *doxing* maka dapat dikenakan sanksi pidana dan denda maupun saksi administratif.
2. Dihimbau kepada masyarakat untuk tidak membagikan informasi pribadi dimedia platfom manapun sebab informasi data pribadi tersebut dapat disalahgunakan orang lain.

DAFTAR PUSTAKA

Abul Hasan Banimal, Damar Juniarto, Ika Ningtyas (2020), "Peningkatan Serangan Doxing dan Tantangan Perlindungan di Indonesia". Tersedia di: https://id.safenet.or.id/wp-content/uploads/2020/12/Peningkatan-Serangan-Doxing-SAFEnet.pdf.

Anggada Perkasa dan Kartina Pakpahan, 'Kebijakan Penegakan Hukum dalam Memerangi Kejahatan Perjudian Media Elektronik di Indonesia', Jurnal Sibatik 2.7 (2023): 2067–84. URL: https://publish.ojs-indonesia.com/index.php/SIBATIK.

Danrivanto Budhijanto, "Hukum Telekomunikasi, Penyiaran & Teknologi Informasi" (Bandung: PT. Refika Aditama, 2010), hal. 4.

Dewi, S. (2016). "Konsep Perlindungan Hukum terhadap Privasi dan Data yang Terkait dengan Penggunaan Komputasi Awan di Indonesia".

Elvira Fitriyani Pakpahan, Lionel Ricky Chandra, dan Ananta Aria Dewa, 'Perlindungan Hukum Data Pribadi di Industri Teknologi Keuangan', Jurnal Veritas et Justitia 6.2 (2020): 298–323. DOI: 10.25123/vej.3778.

Hanifan Niffari, "Perlindungan Data Pribadi sebagai Bagian dari Hak Asasi Manusia terhadap Perlindungan Data Pribadi (Suatu Tinjauan Perbandingan dengan Legislasi di Negara Lain)", Jurnal Yuridis Vol. 7, No. 1 (Juni 2020): 107. DOI: 10.35814/selisik.v6i1.1699.

Indonesia. Undang-Undang Nomor 27 Tahun 2022 Tentang Perlindungan Data Pribadi.

Johnny Ibrahim, Teori dan Metodologi Penelitian Hukum Normatif (Malang: Bayumedia Publishing, 2006), hal. 295.

Kartina Pakpahan. Perlindungan Hukum Terhadap Pihak Ketiga Sebagai Pemilik Alat Berat Yang Digunakan Dalam Melakukan Tindak Pidana Perambahan Hutan. Jurnal Selat Volume 6. URL: https://sg.docworkspace.com/d/sIJz5hMxq5Jj_swY. 26 Agustus 2019.

Khikam, D. (2023). KAJIAN HUKUM PERLINDUNGAN DATA PRIBADI DALAM PERATURAN PERUNDANG–UNDANGAN DI INDONESIA (Disertasi Doktoral, Universitas Islam Sultan Agung Semarang).

Manurung, E. A. P., & Thalib, E. F. (2022). Tinjauan Yuridis Perlindungan Data Pribadi Berdasarkan UU Nomor 27 Tahun 2022. Jurnal Hukum Saraswati (JHS), 4(2), 139-148.

Mazmur Septiani Rumapea. Perlindungan Hukum terhadap Perusahaan Transportasi Online dalam Tindak Pidana Penipuan Order Fiktif. Ilmu Hukum Prima (IHP). URL: https://sg.docworkspace.com/d/sIFL5hMxq_J__swY. 2019.

Navis, A. A. (2023). Perlindungan Data Pribadi Menurut Undang-Undang Nomor 27 Tahun 2022 dan Perspektif Siyasah Syar'iyyah: Studi di Dinas Komunikasi dan Informatika Kota Malang (Disertasi Doktoral, Universitas Islam Negeri Maulana Malik Ibrahim).

Rizal, M. S. (2019). Perbandingan Perlindungan Data Pribadi Indonesia dan Malaysia, Jurnal Cakrawala Hukum 10(2): 218-227.

Situmorang, Muda, I., Doli, M. & Fadli F.S. (2010) Analisis Data untuk Riset Manajemen dan Bisnis. Medan: USU Press.

Soerjono Soekanto, Pengantar Penelitian Hukum (Jakarta: Penerbit UI Press, 2005), hal. 51.

Undang-Undang Nomor 23 Tahun 2006 tentang Administrasi Kependudukan.

Undang-Undang Perlindungan Data Pribadi Nomor 27 Tahun 2022 Pasal 1 ayat 1.

Undang-Undang Perlindungan Data Inggris 2018.

Yanti Agustina. Perlindungan Hukum bagi Pencipta Lagu atas Lagu Ciptaannya yang Dipakai Orang Lain tanpa Izin. Jurnal Collegium Studiosum Volume 6. DOI: 10.56301/csj.v6i2.1083. 12 Desember 2023.

Yanti Agustina dkk., 'Pemanfaatan Teknologi dalam Membangun Generasi yang Sadar Hukum', PKM Maju UDA 4.2 (2023): 36. DOI: 10.46930/pkmmajuuda.v4i2.3687.

Yopi Makdori, 2020, "Komnas HAM: Doxing Termasuk Pelanggaran HAM Digital", Liputan6, 21 November 2021.

Zainuddin Ali, Metode Penelitian Hukum (Jakarta: Sinar Grafika, 2015), hal. 105.