

## PERTANGGUNGJAWABAN PIDANA BAGI PARA PELAKU DOXING MENURUT UU ITE DAN UU PDP

Muhammad Arvy Chico Armando<sup>1</sup>, Hari Soeskandi<sup>2</sup>

<sup>1,2</sup>Fakultas Hukum, Universitas 17 Agustus 1945 Surabaya

Email : [chico.armandooo@gmail.com](mailto:chico.armandooo@gmail.com)<sup>1</sup>, [soeskandihari@gmail.com](mailto:soeskandihari@gmail.com)<sup>2</sup>

### Abstrak

Penelitian ini akan membahas mengenai *Doxing*, yaitu kejahatan internet yang dilakukan dengan mengumpulkan data pribadi seseorang, kemudian data pribadi tersebut akan disebarluaskan gunanya untuk mengintimidasi targetnya. Korban *doxing* umumnya adalah wartawan, politikus, kelompok aktivis, dan masyarakat biasa. Tujuan pelakunya melakukan *doxing* adalah untuk membungkam seseorang dan terkadang hanya untuk bergurau. Penelitian ini menggunakan metode yuridis normatif, dengan teknik inventaris dan menganalisis dalam data sekunder yang terdiri dari bahan hukum primer dan bahan hukum sekunder dengan teknik memahami hukum sebagai pedoman didalam sebuah perundang-undangan yang mengatur mengenai *doxing* yang tujuannya untuk menemukan prinsip-prinsip hukum, aturan-aturan hukum, dan doktrin hukum tujuannya untuk memberikan jawaban dalam memecahkan isu masalah hukum yang sudah diteliti. Dengan menggunakan konsep tersebut, peneliti ingin menjelaskan hukuman pidana bagi para pelaku doxing menurut aturan yang berlaku. Sehingga mampu untuk memberikan jawaban mengenai kajian penelitian yang sedang diteliti.

### Abstract

*This research will discuss Doxing, which is an internet crime that is committed by collecting someone's personal data. Then this personal data will be disseminated to intimidate the target. Victims of doxing are generally journalists, politicians, activist groups, and ordinary people. The purpose of doxing is to silence someone and sometimes just for fun. This study uses a normative juridical method, with inventory techniques and analyzes in secondary data consisting of primary legal materials and secondary legal materials with the technique of understanding the law as a guide in a legislation that regulates doxing whose aim is to find legal principles, rules -rule of law, and legal doctrine aim to provide answers in solving legal issues that have been researched. By using this concept, researchers want to explain criminal penalties for doxing perpetrators according to applicable regulations. So as to be able to provide answers regarding the research study being studied.*

## PENDAHULUAN

Perkembangan teknologi membawa dampak kebebasan berbagai lapisan masyarakat untuk berpendapat di Internet. Sebelum berkembangnya teknologi masyarakat telah bebas untuk berpendapat dimuka umum namun setelah kemunculan Internet maka masyarakat semakin bebas untuk berpendapat di sosial media pada era digital. Perkembangan teknologi informasi dan komunikasi telah membantu masyarakat, namun perkembangan teknologi informasi telah mengubah perilaku masyarakat secara besar-besaran. Dampak dari perkembangan teknologi tersebut membawa dampak positif dan negatif.

Pemanfaatan teknologi yang bersifat negatif memunculkan kejahatan jenis baru disebut cybercrime. Kejahatan cybercrime memiliki banyak jenis, salah satunya doxing. Secara

singkat doxing adalah kejahatan yang dilakukan di internet dengan cara mengumpulkan data pribadi korban kemudian menyebarkan di Internet maupun sosial media dengan tujuan mengintimidasi serta mengancam korban. Pada mulanya doxing didasari karena pelaku tidak menyukai korban, baik karena korban melakukan kesalahan maupun korban memaparkan pendapatnya di sosial media yang menyebabkan pelaku tidak menyukai korban.

Doxing biasanya dilakukan secara individu maupun berkelompok, Doxing sendiri telah diatur didalam pasal 27 ayat 4 UU Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik yang telah diubah menjadi UU Nomor 19 Tahun 2016, Namun terdapat keganjilan yaitu pada pasal 27 ayat 4 UU Nomor 11 Tahun 2008 tentang ITE yang memaparkan "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"

Pada frasa memiliki muatan pemerasan dan/atau pengancaman yang memiliki arti yang membingungkan, apakah doxing dilakukan dengan pemerasan dan atau ancaman dokumen yang bersifat pribadi akan disebar luaskan? atau tindakan doxing yang memuat pemerasan dan atau ancaman seperti kekerasan dan lain sebagainya ?

Sementara pada perubahan UU Nomor 19 Tahun 2016 tidak dijelaskan kembali pasal 27 ayat 4 apakah maksud dari frasa tersebut, hanya tertulis sudah jelas. Sehingga menimbulkan kekhawatiran terjadinya multi tafsir dalam menentukan tindakan doxing.

Berdasarkan pada uraian yang telah dijabarkan diatas, dikarenakan hal tersebut penulis melakukan penelitian apakah pelaku doxing dapat dijerat pidana menurut UU ITE dan Bagaimana ketentuan pidana doxing dalam UU PDP.

## **METODE PENELITIAN**

Dalam Penelitian ini, penulis menggunakan penelitian hukum normatif. Penelitian hukum normatif merupakan suatu tahap dalam mencari tahu maupun menemukan suatu prinsip hukum, aturan hukum maupun doktrin hukum pada masa mendatang akan digunakan untuk menjawab permasalahan hukum yang dihadapi.

Penulis dalam penelitian ini menggunakan pendekatan perundang-undangan yaitu dengan meneliti berbagai peraturan yang berkaitan dengan doxing yang menjadi fokus penelitian. Kemudian pendekatan secara konseptual yaitu dengan merujuk analisis

pandangan para ahli hukum, doktrin-doktrin, konsep-konsep dan asas-asas hukum dalam ilmu hukum.

## HASIL DAN PEMBAHASAN PENELITIAN

Sebelum memasuki pembahasan terlebih dahulu memahami secara mendalam apa itu yang dimaksud doxing.

Arti kata doxing sendiri dalam Black Law Dictionary yaitu Publikasi data pribadi seperti alamat rumah, alamat e-mail, foto sensitif yang bersifat pribadi, data riwayat penyakit seseorang, dan lain sebagainya tanpa persetujuan orang tersebut tujuannya untuk mengintimidasi. (Garner, 2019)

Secara tidak sadar kita menyerahkan data pribadi kita pada sosial media dengan gratis. Maksudnya yaitu dibalik menyenangkannya memakai sosial media, data pribadi kita sebagai bayarnya. Mengapa demikian, dikarenakan secara tidak sadar kita mempublikasikan dokumen maupun data pribadi kita pada sosial media maupun platform lainnya misalnya penyimpanan awan atau cloud storage.

Penyimpanan awan atau cloud storage adalah sebuah metode menyimpan suatu data komputer yang berbentuk digital, cara menyimpannya yaitu dengan memakai server yang biasanya tersebar diberbagai negara dan penyimpanan awan ini disewakan oleh yang namanya perusahaan hosting. Guna adanya penyimpanan awan ini yaitu untuk memudahkan penyimpanan pengguna data komputer dan dapat diakses dimana saja kapan saja tanpa perlu membawa komputer maupun penyimpanan tambahan.

Penggunaan penyimpanan awan banyak dirasakan manfaat oleh berbagai lapisan masyarakat, baik kalangan individu maupun pemerintahan. Dikalangan individu penggunaan penyimpanan awan memiliki banyak manfaat untuk menyimpan berbagai data pribadi ,begitu pula dengan kalangan pemerintahan. Penggunaan penyimpanan awan banyak memudahkan berbagai pekerjaan. Dengan adanya penyimpanan awan pemerintah daerah A tidak perlu lagi pergi menemui pemerintahan daerah B karena pada penyimpanan awan data sudah terintegrasi sehingga dapat diakses oleh pemerintahan baik daerah A maupun B.

Pada kalangan pemerintahan penyimpanan awan digunakan untuk menyimpan data-data pribadi masyarakat, misalnya data kartu tanda penduduk yang berisikan nama, alamat rumah, golongan darah, sidik jari, riwayat penyakit dan lain sebagainya.Tak jarang terjadi

kebocoran data yang dilakukan oleh peretas atau hacker, Biasanya peretas melakukan aksinya dengan cara membobol server pemerintah dan mengunduh data-data tersebut kemudian akan diperjual belikan pada dark-web. Meskipun pemerintah telah memiliki server sendiri nyatanya di Indonesia masih kita temui kebocoran data milik pemerintah yang diperjual belikan di dark-web.

Namun kita tidak bisa juga menyalahkan pemerintah dalam kebocoran data pribadi, terkadang kita sendiri yang membocorkan data pribadi tersebut. Misalnya membuat kiriman pada timeline baik berupa foto maupun video pada sosial media kita yang memuat alamat rumah, nama ibu kandung, nomor telepon genggam dan lain sebagainya. Kebocoran data pribadi pada sosial media sering dilakukan tanpa sadar misalnya mengikuti tren untuk membuat konten foto kartu tanda penduduk atau foto kartu keluarga, Masih banyak masyarakat yang tidak sadar foto tersebut bersifat pribadi dan sangat berbahaya jika dibagikan pada sosial media dengan cuma-cuma.

Kegiatan mencuri data pribadi bertambah mudah karena secara tidak sadar data tersebut sudah ada pada sosial media kita, diperparah dengan pola pikir masyarakat yang meremehkan data pribadinya yang dianggap tidak penting karena mereka hanya orang biasa. Doxing adalah kegiatan yang bukan didasarkan pada kebencian baik untuk menghina ataupun merusak karakter orang saja, doxing juga merupakan cara untuk melakukan sebuah kritik terhadap suatu individu maupun kelompok, terkadang dijadikan bahan lelucon bagi pelakunya. Realitanya doxing digunakan untuk membungkam wartawan, kelompok aktivis, maupun politikus agar korbannya untuk tidak vokal dalam menyampaikan pendapatnya.

Pelaku doxing terkadang bukan hanya dari kalangan peretas profesional bahkan masyarakat biasa pun dapat menjadi pelakunya, hanya dengan bermodalkan stalking atau menguntit sosial media targetnya maka data pribadi pun dapat ditemukan semua ini didukung dengan internet yang bersifat open for everyone atau terbuka untuk siapa saja, namun pada kalangan orang-orang yang memiliki pengaruh terkadang tidak sadar terdapat data pribadi yang tersebar tentu saja bukan mereka yang menyebarkan data pribadinya namun melalui berita-berita dengan bentuk foto maupun video maka akan mudah ditemukan. Mudahnya mencari data pribadi orang dapat dicoba dengan mengetikkan nama target pada google maka akan muncul nama-nama terkait target yang biasanya dapat berupa foto maupun video yang bersifat pribadi.

## **Doxing Dalam UU ITE**

Berkembangnya internet dan sosial media membuat munculnya berbagai macam kejahatan bentuk barunya atau biasa disebut *cybercrime*. Beberapa diantaranya yaitu penipuan online, *carding*, *cracking*, dan *doxing* oleh karena itu lahirnya Undang-Undang Informasi dan Transaksi Elektronik (UU ITE). *Doxing* sendiri telah diatur didalam pasal 27 ayat 4 UU No.11 tahun 2008 Jo UU No.19 tahun 2016 bahwa setiap individu dilarang untuk mendistribusikan data pribadi seseorang dengan ditambah muatan yang berisi ancaman.

*Doxing* biasanya dialami oleh orang-orang yang berpengaruh misalnya wartawan, politikus, artis, kelompok-kelompok yang berpengaruh (Winarmo, 2020) dan tak jarang sesama masyarakat biasa melakukan *doxing* dengan maksud untuk melakukan intimidasi kepada korbannya. Data tersebut dikumpulkan kemudian akan di publikasikan satu persatu dengan memberikan informasi yang membuat orang lain ikut terhasut mengintimidasi korban *doxing* tersebut.

UU ITE telah menetapkan perbuatan-perbuatan mana yang termasuk tindak pidana dibidang ITE (*cybercrime*) dan telah ditentukan sifat jahatnya dan penyerangan terhadap berbagai kepentingan hukum dalam bentuk rumusan-rumusan tindak pidana tertentu (Adam and Ardi 2015)

Ciri-ciri kegiatan pelaku kejahatan dalam *cybercrime* yaitu tidak ada perbedaan dengan *cybercrime* lainnya misalnya, tidak ada kontak fisik dalam ancamanya antara pelaku dan korban hanya melalui teknologi dan peralatan tertentu.

Unsur pada pasal 27 yang dianggap sebagai kegiatan kejahatan *doxing* yaitu sebagai berikut:

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

Pasal 27 ini memunculkan uraian yang ambigu, sehingga dilakukan revisi karena pasal ini dapat menjadi pasal karet yang dapat digunakan korbannya untuk memidanakan pelakunya yang secara tidak sengaja melakukan *doxing*.

Contoh terjadinya *doxing* yaitu terjadi pada salah satu wartawan yang meliput berita di kendari pada 2021 silam, setelah munculnya berita tersebut wartawan tersebut terkena

doxing setelah di selidiki ternyata pelakunya adalah ormas setempat. Mereka melakukan doxing pada wartawan tersebut dengan cara menyebarkan data pribadinya secara luas dan juga mengalami ancaman kekerasan. Kasus lainnya yaitu Ade Armando, Pada kasusnya Ade Armando dikeroyok kemudian muncul akun anonim pada twitter yang menampilkan photo terduga pelaku pengeroyokan, setelah diselidiki photo tersebut tidaklah benar. Orang yang berada di photo tersebut tidak ada di lokasi kejadian perkara. Meskipun orang yang photonya disebar tidak terbukti bersalah ia tetap merasa dirugikan karena namanya tercemar. Karena itulah doxing sangat merugikan. (Taher, 2022)

Menurut hemat penulis, makna berisi muatan ancaman yaitu dapat berupa perundungan (bully). Disertai menyebarkan data pribadi korbannya dengan maksud membungkam korban. Doxing juga dapat dikenakan pidana jika memuat kekerasan atau ancaman baik memuat ancaman yang berupa penyebaran data pribadi maupun muatan ancaman kekerasan berupa secara fisik. Disebutkan bahwa pada pasal 27 adalah kegiatan doxing yang dapat diancam pidana dengan ancaman pidana penjara paling lama 6 tahun dan atau denda paling banyak Rp.1.000.000.000.

Setelah dilakukan revisi pasal ini memperjelas maksud dari isinya ,unsurnya yaitu sebagai berikut:

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

Maknanya dalam revisi UU ITE yang terbaru telah dipersempit arti uraian pasal 27 tersebut sehingga memudahkan pemidanaan bagi pelaku *doxing* yang dimana UU ITE sebelumnya merujuk kepada KUHP. Pemberat pidana dapat dikenakan jika *doxing* memuat kekerasan atau ancaman pula, misalnya berupa ancaman secara fisik didunia nyata maka pelakunya dapat dikenakan pasal 368 KUHP yang ancamannya pidana paling lama penjara 9 tahun.

Doxing juga dapat bertautan dengan KUHP Pasal 513 bahwa dilarang menggunakan suatu barang yang bersifat informasi pribadi tanpa persetujuan orang tersebut. Pelaku doxing dapat dikenakan hukuman dari UU ITE maupun KUHP. (Nugroho, 2022)

Mencuri dan mendistribusikan data pribadi seseorang juga merupakan pelanggaran hak terhadap korbannya, yaitu melanggar hak untuk mendapatkan privasi dan kebebasan berpendapat hal ini disebutkan didalam pasal 28E ayat 2 dan 3 serta dimuat juga didalam pasal 28G ayat 1 UUD 1945.

### ***Doxing* Dalam UU Perlindungan Data Pribadi**

Tumbuhnya internet dan sosial media menimbulkan berbagai macam tantangan hukum bagi Indonesia, salah satunya dalam menanggulangi kejahatan internet dan mengatur regulasi platform sosial media guna mencegah terjadinya kebocoran data. Maka pemerintah Indonesia membuat Undang-Undang Perlindungan Data Pribadi, gunanya yaitu menjamin hak perlindungan data pribadi bagi masyarakat Indonesia dan menjamin penghormatan atas pentingnya data pribadi masyarakat Indonesia.

Data Pribadi merupakan salah satu hak yang tercantum didalam pasal 28G UUD 1945, perlindungan pribadi tersebut berupa privasi dengan adanya UU PDP ini diharapkan dapat mengurangi doxing, dikarenakan mempersempit laju pelakunya dengan adanya UU PDP ini masyarakat diuntungkan dengan mendapat haknya untuk mengatur sendiri data pribadi apa saja yang akan disimpan oleh platform sosial media tersebut, dan masyarakat ber hak untuk meminta data pribadinya dihapus jika sudah tidak menggunakan platform tersebut.

Pentingnya data pribadi dihapus jika sudah tidak menggunakan platform tersebut karena digital footprint jejak digital dapat memicu terjadinya doxing, karena secara tidak sadar jejak digital dapat digali bagi pelakunya guna bahan mengintimidasi korbannya.

Adanya UU PDP ini sangat diperlukan pada sistem hukum di Indonesia. Secara filosofis, perlindungan data pribadi adalah sebuah perwujudan perlindungan hak dasar manusia sesuai nilai pancasila. Secara sosiologis, UU ini merupakan sebuah pedoman untuk melindungi hak data pribadi seseorang pada era digital. (G.Plate, 2020)

Ruang lingkup UU PDP mencakup 2 sektor yakni privat dan publik. Pada sektor privat yang tercakup yaitu individu maupun korporasi yang berbentuk badan hukum maupun bukan badan hukum. Kemudian pada sektor publik yakni pada pemerintahan.

Pada UU PDP pasal 4 ayat 1 dipaparkan bahwa

Data pribadi terdiri atas

- a. Data Pribadi yang bersifat spesifik; dan
- b. Data Pribadi yang bersifat umum

yang dimaksud dengan data pribadi yang bersifat spesifik menurut UU PDP pasal 4 ayat 2 yaitu:

- a. data dan informasi kesehatan
- b. data biometrik
- c. data genetika
- d. catatan kejahatan
- e. data anak
- f. data keuangan pribadi dan atau
- g. data lainnya sesuai dengan ketentuan peraturan perundang-undangan

yang dimaksud dengan data pribadi yang bersifat umum menurut UU PDP pasal 4 ayat 3 yaitu:

- a. nama lengkap
- b. jenis kelamin
- c. kewarnegaraan
- d. agama
- e. status perkawinan dan atau
- f. data pribadi yang dikombinasikan untuk mengidentifikasi seseorang

Kedua data pribadi tersebut diharuskan dilindungi oleh individu masing-masing dan dijamin oleh negara keamanannya, Namun tetap saja *cybercrime* akan tetap terus terjadi sehingga terjadi pembobolan data pribadi baik yang di simpan sendiri maupun yang dilindungi pemerintah.

Inti dari isi UU PDP yang berkaitan dengan *doxing* yaitu:

1. Jenis data pribadi
2. Hak pemilik data pribadi
3. Ketentuan pidana

Pada UU PDP BAB XIV Ketentuan Pidana dapat kita temui bahwa pelaku *doxing* dapat dikenakan pidana, yaitu tepatnya pada pasal 67 ayat 1 dan ayat 2. Pada pasal tersebut pelakunya disebut sebagai orang yang mengumpulkan data pribadi seseorang dan

mengungkapkan data pribadi yang bukan miliknya, Kalimat ini merupakan definisi dari *doxing*. Maka pelaku *doxing* yang mengumpulkan data pribadi seseorang menurut UU PDP diancam dengan pidana penjara paling lama 5 tahun atau denda paling banyak Rp.5.000.000.000. Kemudian untuk pelaku yang mengungkapkan data pribadi hasil dari mengumpulkan data pribadi tersebut diancam dengan pidana penjara paling lama 4 tahun dan denda paling banyak Rp.4.000.000.000.

## KESIMPULAN

Doxing merupakan salah satu kejahatan *cybercrime*, Kegiatannya yaitu mengumpulkan data pribadi seseorang dapat berupa nama lengkap, alamat rumah, nama orang tua, riwayat penyakit, rekening di bank dan lain sebagainya yang kemudian akan di publikasikan guna untuk mengintimidasi korbannya. Doxing merupakan kejahatan yang dilakukan menggunakan sistem teknologi tidak dilakukan secara fisik, Tujuan utama doxing yaitu berbagai macam, misalnya untuk bahan lelucon, membungkam seseorang dan lain sebagainya.

Target sasaran doxing biasanya wartawan, politikus, selebritis, kalangan aktifis bahkan masyarakat biasa. Tujuan dilakukan doxing selama ini di Indonesia sesungguhnya untuk membungkam seseorang padahal kegiatan tersebut melanggar hak dasar manusia yaitu melanggar hak mendapatkan privasi dan bebas berpendapat.

Doxing sendiri diatur didalam UU ITE dan UU PDP, pada UU ITE doxing disebutkan pada pasal 27 ayat 3 pada UU No.11 Tahun 2008 yang kemudian menimbulkan arti yang ambigu pada frasa berisi muatan kekerasan atau ancaman. Yang kemudian di revisi dan memperjelas maksud dari pasal tersebut yaitu pada UU No.19 Tahun 2016 bahwa yang dimaksud muatan ancaman yaitu menyebarkan data pribadi seseorang kemudian jika disertai ancaman kekerasan secara fisik maka dapat dikenakan pemberat pidana yaitu pasal 368 KUHP.

Kemudian pada UU PDP Disebutkan juga berbagai macam jenis data pribadi dan ruang lingkupnya terdapat 2 yaitu privat dan publik, privat yaitu dapat berupa individu maupun korporasi kemudian publik adalah pemerintahan. Pada UU PDP doxing disebutkan didalam BAB XIV Ketentuan pidana yaitu terdapat pada pasal 67 ayat 1 dan 2, disebutkan bahwa doxing kegiatannya yaitu mengumpulkan data pribadi seseorang kemudian menungkapkan data tersebut. dapat di ancam pidana penjara dan sanksi.

Dengan demikian makna ambigu pada pasal 27 ayat 3 telah menemukan titik terang setelah ada nya revisi kemudian disertai disahkan nya Undang-Undang Perlindungan Data Pribadi yang akan memberikan jawaban bagi praktisi hukum dalam mempidanakan pelaku doxing serta memberi jaminan keamanan data pribadi masyarakat.

## DAFTAR PUSTAKA

- Adam, Chazawi, and Ferdian Ardi. 2015. *TINDAK PIDANA INFORMASI & TRANSAKSI ELEKTRONIK*, 1st edn (Malang: Media Nusa Creative)
- G.Plate, J. (2020, Februari 25). *PENJELASAN PEMERINTAH MENGENAI RUU TENTANG PERLINDUNGAN DATA PRIBADI*. Retrieved Desember 18, 2022, from DPR RI: <https://www.dpr.go.id/dokakd/dokumen/RJ5-20200305-121009-3116.pdf>
- Garner, B. A. (2019). *Black Law Dictionary 11th edition*. Saint Paul: Thomson Reuters.
- Nugroho, I. I. (2022, January 30). *Doxing dan Penggerusan Privasi Online*. Retrieved 12 17, 2022, from Heylaw.id: <https://heylawedu.id/blog/doxing-dan-penggerusan-privasi-online>
- Pasya, K. (2022, June 26). Ancaman Pidana Pelaku Doxxing. *Kumparan*.
- Taher, A. P. (2022, April 13). *Hukum*. Retrieved December 16, 2022, from Tirto.id: <https://tirto.id/kasus-ade-armando-doxing-data-terduga-pelaku-tak-bisa-ditolerir-grai>
- Winarmo, S. (2020). Waspada Doxing. 1.  
Pasal 4 UU PDP Tentang Jenis Data Pribadi  
Pasal 368 KUHP Tentang Pemerasan  
Pasal 513 KUHP Tentang Menggunakan Barang Orang Lain