TINDAKAN DOXING DI MEDIA SOSIAL BERDASARKAN UNDANG-UNDANG NOMOR 19 TAHUN 2016 TENTANG PERUBAHAN ATAS UNDANG-UNDANG NOMOR 11 TAHUN 2008 TENTANG INFORMASI DAN TRANSAKSI ELEKTRONIK DIKAITKAN DENGAN KONSEP PERLINDUNGAN PRIVASI

Dinda Salsabila, Sinta Dewi dan Widati Wulandari
Fakultas HukumUniversitas Padjadjaran
Jl. Raya Bandung-Sumedang KM.21, Kabupaten Sumedang, Jawa Barat 45363
Email: dinda18005@mail.unpad.ac.id1, isntadewi@gmail.com2,
widatiwulandari@gmail.com3

Abstract: There is a phenomenon on the internet called doxing or the act of publishing private information about someone on the internet, typically with malicious intent. Doxing act violates people rights of their privacy of personal data. Not only with malicious intent, doxing act often carried out by victims of crime to seek justice. This study aims to determine the application of the protection of personal data principals from doxing act in ITE Law and to identify the legal liability of doxing actions on social media that is carried out by victims of crime in related to the concept of privacy protection.This research was conducted using normative juridical approach and descriptive analytical research specifications, namely by describing the issue with the phenomenon being studied as the research object, in this case doxing act, and then reviewed with secondary data. The data analysis was carried out using a qualitative juridical method.The results of the study show that in the ITE Law, the protection of personal data from doxing act can be found in Article 26 (1) regarding the consent to disclose personal data, Article 27 (1), (3), and (4) regarding to the content of personal data that is disclosed, and Article 30 (2) regarding to the method in obtaining the content or personal data that is disclosed. Doxing actions on social media carried out by victims of crime to seek justice in the concept of privacy protection can be held legally responsible under the ITE Law Article 26 by filing a lawsuit, criminal sanctions and fines based on Article 45 (1), (3), and (4) and Article 46 (2), or administrative sanctions based on the Ministry of Communication and Informatics Regulation No. 20 of 2016 Article 36 such as verbal and written warnings, temporary suspension of activities and/or announcements on online websites.
Keywords: Privacy and Personal Data Protection, Doxing, Legal Liability

Abstrak: Terdapat fenomena di internet yaitu tindakan doxing atau tindakan mempublikasikan data pribadi seseorang tanpa izin di internet dengan maksud atau niat jahat. Tindakan doxing melanggar privasi seseorang atas data pribadinya. Tidak hanya dengan maksud atau niat jahat, tindakan doxing sering dilakukan korban kejahatan untuk mencari keadilan. Penelitian ini bertujuan untuk mengetahui penerapan prinsip-prinsip perlindungan data pribadi dari tindakan doxing dalam UU ITE serta untuk mengidentifikasi pertanggungjawaban hukum atas tindakan doxing di media sosial yang dilakukan oleh korban kejahatan dikaitkan dengan konsep perlindungan privasi.Penelitian ini dilakukan menggunakan metode pendekatan yuridis normative dengan spesifikasi penilitian deskriptif analitis yaitu dengan menggambarkan permasalahan terkait peristiwa yang menjadi objek penelitian, dalam hal ini tindakan doxing, kemudian ditinjau dengan data sekunder. Kemudian dilakukan analisis data dengan metode yuridis kualitatif.Hasil penelitian menunjukkan bahwa dalam UU ITE perlindungan data pribadi dari tindakan doxing dapat ditemukan pada Pasal 26 ayat 1 berkaitan ada atau tidaknya persetujuan (consent) diungkapkan suatu data pribadi, Pasal 27 ayat 1, 3 dan 4 berkaitan dengan muatan atau bentuk data pribadi yang diungkapkan, serta Pasal 30 ayat 2 berkaitan cara perolehan muatan atau data pribadi yang diungkapkan. Tindakan doxing di media sosial yang dilakukan oleh korban kejahatan untuk mencari keadilan secara konsep perlindungan privasi dapat diminta pertanggungjawaban hukum berdasarkan UU ITE Pasal 26 dengan mengajukan gugatan perbuatan melawan hukum, penjatuhan sanksi pidana dan denda sesuai Pasal 45 ayat 1, 3 dan 4 dan Pasal 46 ayat 2 atau dengan sanksi administratif sesuai Permen Kominfo 20/2016 Pasal 36 berupa peringatan lisan, tertulis, penghentian sementara kegiatan dan/atau pengumuman di situs dalam jaringan (website online).
Kata Kunci: Perlindungan Privasi dan Data Pribadi, Tindakan Doxing, Pertanggungjawaban hukum

Pendahuluan

Salah satu cara bagi masyarakat dalam memanfaatkan perkembangan teknologi internet yaitu dengan berkomunikasi melalui media sosial. Media sosial memungkinkan penggunanya untuk berkomunikasi di mana saja dan kapan saja dengan pengguna lainnya. Saat ini media sosial juga salah satu sumber informasi yang masyarakat bisa dapatkan tanpa dibatasi ruang dan waktu. Masyarakat yang dapat mengakses internet dapat menggunakan media sosial untuk berkomunikasi antar sesama pengguna ataupun mengkses informasi-informasi penting. Perkembangan media sosial ini ditandai dengan adanya media sosial seperti Twitter, Instagram, Facebook, dan lain sebagainya, terlebih lagi era covid-19 kita semua dipaksa memanfaatkan perkembangan informasi teknologi sebagai media social.

Pemanfaatan teknologi internet dan juga penggunaan media sosial sangat erat kaitannya dengan data pribadi yang merupakan privasi seseorang dan harus dilindungi. Masyarakat dalam menggunakan internet dan juga media sosial terlebih dahulu harus memiliki akun yang berisikan data pribadi seperti nama, tanggal lahir, e-mail, password, ataupun tempat tinggal. Data pribadi seseorang yang merupakan hal yang bersifat privasi sangat mudah untuk didapatkan dengan pesatnya perkembangan teknologi informasi ini yang menawarkan berbagai kemudahan, dimana saja, kapan saja dan tanpa batas waktu. Adanya kemungkinan pengguna lain yang tidak bertanggungjawab menggunakan data pribadi orang lain tersebut tanpa izin dan disalahgunakan yang akhirnya melanggar privasi seseorang atas data pribadinya.Tindakan kejahatan yang dilakukan di dunia maya ini diantaranya carding, hacking, cracking, phising, booting, viruses, cybersquatting, pornografi, perjudian, penipuan, terorisme, ataupun penyebaran informasi yang sifatnya membahayakan dan lain sebagainya. Banyaknya kejahatan baru yang hadir di dunia maya ini mengakibatkan banyak kerugian bagi masyarakat. Hal ini menjadi alasan mengapa pemerintah harus membuat peraturan-peraturan baru secara khusus mengatur kejahatan siber. Pemerintah harus memperhatikan perkembangan upaya penanggulangan dan pengaturan terkait teknologi informasi baik dalam lingkup regional ataupun internasionaldemi memberikan perlindungan bagi masyarakat.

Salah satu fenomena yang terjadi saat ini di dunia maya, khususnya di media sosial yaitu tindakan doxing yang melanggar privasi seseorang. Berdasarkan Oxford British & World English Dictionary, doxing merupakan tindakan mencari dan mempublikasikan informasi yang bersifat privasi tentang seorang individual tertentu di Internet, biasanya dengan niat jahat. Pada dasarnya, tindakan Doxing ini dilakukan bertujuan untuk mempermalukan, menghina ataupun mengancam target yang mana dapat mengancam privasi target.Tindakan doxing dilakukan dengan target yang memang sudah ditetapkan dan kemudian dimulai dengan mengumpulkan data-data yang sangat mudah didapat di Internet seperti nama, alamat, jenis kelamin, e-mail, username akun media sosial, foto dan lain sebagainya. Kemudian setelah data atau informasi tersebut terkumpul, pelaku mengajak para pengguna lain untuk melakukan hal yang sama dan juga mengedarkan informasi targetnya.

Sebagai contoh tindakan doxing yang dilakukan dengan niat jahat dan dapat ditemukan di media sosial yaitu kasus yang dialami seorang perempuan yang berinisial M melaporkan pemuda berusia 25 tahun dengan inisial FIR yang merupakan mantan pacarnya. FIR dilaporkan karena telah menyebarkan foto tidak senonoh M ke group chat Whatsapp mahasiswa kampus pelaku dengan alasan sakit hati karena ajakan nikahnya ditolak dan M kemudian berpacaran dengan orang lain. Korban kemudian melaporkan ke kepolisian dan pelaku FIR kemudian ditangkap dan dijerat Pasal 27 ayat 1 jo Pasal 45 ayat 1 UU ITE dan Pasal 29 jo Pasal 4 UU Pornografi.

Selain itu terdapat kasus doxing yang terjadi terhadap Denny Siregar yang merupakan seorang influencer politik. Pada tahun 2020 lalu data pribadi Denny disebar oleh akun Twitter @opposite6891 yang kemudian diketahui milik Febriansyah Puji Handoko. Pelaku mengatakan bahwa ia melakukan doxing terhadap data pribadi Denny atas keinginannya sendiri karena kesal atas postingan Denny di Twitter. Pelaku mengakui bahwa ia mengakses data Denny

karena merupakan pelanggan Telkomsel yang dulu pelaku bekerja sebagai pegawai GraPari Telkomsel Surabaya. Pelaku menyebarkan data pribadi Denny seperti nama lengkap, alamat, Nomor Induk Kependudukan (NIK), Nomor Kartu Keluarga, IMEI hingga jenis perangkat lalu dipublikasikan di akun twitter @ opposite6891. Pelaku kemudian dijerat Pasal 46 ayat 2 jo. Pasal 30 ayat 2 UU ITE dengan vonis hukuman 8 bulan penjara dan denda Rp2 juta.

Tindakan doxing dengan niat jahat tersebut banyak dilakukan untuk mengancam orang yang serta membahayakan fisik ataupun mental. Namun tidak semua tindakan doxing dilakukan dengan niat jahat, ada juga yang dilakukan sebagai bentuk pembalasan atas kejahatan yang dialami seseorang. Tindakan doxing dilakukan untuk mengekspos suatu ketidakadilan atau untuk meminta peranggungjawaban kepada pelaku kejahatan. Sehingga tindakan doxing juga berkaitan dengan vigilantism atau digital vigilantism karena dilakukan menggunakan teknologi digital.

Contoh yang dapat ditemukan di media sosial Twitter yaitu penipuan yang terjadi ketika melakukan transaksi jual-beli secara online. Pemegang akun yang menjadi korban penipuan tersebut kemudian menyebarkan data ataupun informasi terkait pelaku penipuan, seperti nama lengkap, akun media sosial, nomor telepon, nomor rekening bank, serta foto wajah pelaku penipuan tersebut. Kemudian postingan korban penipuan tersebut di-retweet ataupun disebarkan oleh pengguna lain dengan maksud agar pengguna lain waspada dan tidak terjadi lagi penipuan oleh orang yang sama. Tindakan doxing ini dilakukan karena korban penipuan yang sudah melaporkan ke kepolisian merasa kasusnya terlalu lama dan tidak kunjung selesai ditindak lanjuti.

Contoh lain juga dapat ditemukan di Twitter yaitu postingan terkait korban pelecehan seksual yang menceritakan pengalaman yang dialami dan mempublikasikan informasi pelaku secara online dengan alasan tak kunjung diprosesnya kasus yang sudah dilaporkan ataupun proses kasus tersebut tidak selesai ditindak lanjuti. Kemudian korban mempublikasikan nama, foto pelaku, tempat serta divisi pekerjaan, alamat rumah, nomor telepon, serta data-data lain yang seharusnya tidak dapat dipublikasikan oleh orang lain tanpa izin dari pemilik data tersebut. Postingan tersebut kemudian tersebar luas dan cepat oleh sesama pengguna dengan harapan agar mencapai pihak kepolisian dan kasus ditindak lanjuti sampai selesai.

Tindakan doxing sangat erat kaitannya dengan hak privasi seseorang (right to privacy) yang merupakan bagian dari hak asasi manusia yang diatur konstitusi dan dilindungi. Tindakan doxing dapat mengancam hak privasi seseorang khususnya melihat dari perkembangan teknologi informasi yang sangat pesat dan cepatnya pergerakan data di internet sehingga rentan terjadinya penyalahgunaan data. Maka tindakan doxing juga rentan terhadao pelanggaran privasi yang diatur dalam undang-undang dasar ataupun UU ITE.

Rumusan Masalah

1. Bagaimana penerapan prinsip-prinsip perlindungan data pribadi dari tindakan doxing dalam UU ITE?
2. Bagaimana pertanggungjawaban hukum atas tindakan doxing di media sosial yang dilakukan oleh korban kejahatan dikaitkan dengan konsep perlindungan privasi?

Tujuan Penelitian

1. Untuk mengetahui dan mendeskripikan penerapan prinsip-prinsip perlindungan data pribadi dari tindakan doxing dalam UU ITE.
2. Untuk mengetahui dan mendeskripsikan pertanggungjawaban hukum atas tindakan doxing di media sosial yang dilakukan oleh korban kejahatan dikaitkan dengan konsep perlindungan privasi.

Metode Penelitian

Penelitian ini menggunakan metode pendekatan

[1]Khairiah, K., Hidayat, M. N., Kurnia, I., Harmaida, M., Rusydi, I., & Warto, W. (2021). MUTU KINERJA TENAGA PENDIDIK (GURU) DALAM MANAJEMEN PENDIDIKAN ERA PANDEMIC COVID-19. Al-Khair Journal: Management, Education, And Law, 1(1), 20-29.

[2]Ita Purnama Sari, Syarifuddin Syarifuddin,(2022). Evaluasi Penggunaan Teknologi Dalam Meningkatkan Mutu Pembelajaran Madrasah Ibtidaiyah Di Kota BengkuluAl-Khair Journal: Management, Education, And Law, 2(2), 59-66.

Yuridis Normatif, yaitu dengan menggunakan sumber data sekunder sebagai sumber utama. Pendeketan Yuridis Normatif yaitu meneliti bahan-bahan kepustakaan seperti peraturan perundang-undangan dan bahan lain yang berkaitan dengan penulisan penelitian. Spesifikasi penelitian yaitu Deskriptif Analitis dengan menggambarkan permasalahan yang merupakan objek penelitian dan menganalisis fakta-fakta yang ada secara sistematis dengan memperhatikan data, peraturan, dan teori hukum serta praktik pelaksanaan hukum positif yang berkaitan dengan permasalahan. Metode yang digunakan untuk menganalisa data dalam penelitian ini yaitu Yuridis Kualitatif yang mengacu pada norma hukum dalam suatu peraturan perundang-undangan dengan memperhatikan hierarki peraturan perundang-undangan, mewujudkan kepastian hukum serta menggali nilai-nilai tertulis ataupun tidak tertulis yang hidup di masyarakat

Pembahasan

Tindakan doxing atau doxing secara etimologi berasal dari ungkapan "dropping dox" atau "dropping documents". Definisi Doxing dalam Oxford British and World English Dictionary yaitu:

''[s]earch for and publish private or identifying information about (a particular individual) on the internet, typically with malicious intent''

Yang artinya adalah mencari dan mempublikasikan atau mengidentifikasikan informasi privat tentang seseorang tertentu di internet, biasanya dengan maksud atau niat jahat.

Julia M. MacAllister dalam artikel jurnal yang berjudul The Doxing Dilemma, menjelaskan definisi doxing yang diberikan oleh Professor Mary Anne Frank yaitu:

"The public release of an individual's private, sensitive, personal information, such as:

- Home address, email address, phone number
- Social security number
- Employer and employer contact info
- Family member's contact info
- Photos of victim's children and the school they attend"

David M. Douglas berpendapat bahwa tindakan doxing tidak harus dilakukan dengan niat jahat. Kemudian mengkategorikan tindakan doxing sebagai berikut:

1. Deanonymizing
   Tindakan doxing deanonymizing ini mempublikasikan informasi yang mengungkapkan identitas seseorang atau orang banyak yang sebelumnya tidak diketahui (anonim) atau hanya dikenal dengan nama samaran (pseudonym). Deanonymizing sangat mempengaruhi seluruh bentuk identity knowledge atas kerahasiaan identitas seseorang dan dapat mengintimidasi mereka yang memang menginginkan untuk tidak diketahui identitasnya untuk mendapat kebebasan berekspresi.
2. Targeting
   Tindakan doxing Targetingini mempublikasikan informasi spesifik tentang keberadaan seseorang secara fisik yang memperkenankan seseorang dapat dilacak atau ditemukan lokasi keberadaannya. Tindakan doxing ini mengungkapkan physical locatability, bukan communicative locatability seperti nomor telepon atau e-mail. Targeting meningkatkan kemungkinan seseorang secara fisik dapat ditemukan dan diketahui tempat tinggal ataupun tempat bekerja. Hal ini mengakibatkan seseorang akan lebih terancam bahaya secara fisik seperti serangan. Tindakan doxing inidilakukan setelah deanonymization.
3. Delegitimizing
   Tindakan doxing Delegitimizing mempublikasikan informasi privat seseorang dengan maksud untuk merusak atau menjatuhkan kredibilitas, reputasi ataupun karakter. Delegitimizing dilakukan dengan maksud untuk mempermalukan dan juga menghina ses-

[3]Sugeng, Hukum Telematika Indonesia. Jakarta: Prenadamedia Group, 2020, hlm 85

[4]David M. Douglas, "Doxing: A Conceptual Analysis", Ethics and Information Technology 18 (3), 2016, hlm. 200

eorang biasanya dengan menggambarkan orang tersebut sebagai pelanggar norma sosial. Douglas menjelaskan bahwa delegitimizing ini sering terjadi untuk menjatuhkan reputasi atau karakter seseorang dengan menggunakan informasi privat yang mudah disalahpahami atau informasi yang memang rahasia

Pedro Anguita kemudian mengidentifikasikan tindakan doxing menjadi:

1. Positive Doxing
   Positive doxing dilakukan dalam kegiatan investigasi oleh institusi untuk mengidentifikasi pelaku yang melanggar hukum, misalnya pelaku yang melakukan korupsi. Selain itu tindakan doxing dapat dilakukan dalam bentuk pencarian di internet oleh pekerja profesional seperti pengacara, psikolog, dokter, dan sebagainya dengan maksud untuk mengetahui latar belakang dari calon pekerja yang akan mereka pekerjakan.
2. Negative Doxing
   Tindakan doxing ini dilakukan untuk mengekspos seseorang secara public atau dengan cara pemerasan, pelecehan dan pemaksaan. Dilakukan dengan mencari, mengumpulkan serta mengekspos data pribadi subjek dengan maksud untuk menjatuhkan harga diri dan mentalnya.

Penerapan Prinsip-Prinsip Perlindungan Data Pribadi Dari Tindakan Doxing Dalam UU ITE

Indonesia pada dasarnya masih belum memiliki pengaturan yang secara khusus untuk tindakan doxing. Dalam peraturan perundang-undangan baik di Indonesia ataupun di negara lain seperti Hong Kong yang penulis ambil sebagai negara pembanding, sebenarnya tidak ada penggunaan istilah "doxing". Ketika Hong Kong mengumumkan adanya perubahan pada Personal Data Privacy Ordinance (PDPO) tahun 2021 yang menambahkan aturan dalam melindungi privasi dan data pribadi dari tindakan doxing, pemerintah Hong Kong tidak menggunakan istilah "doxing" dalam amandemen tersebut melainkan menggunakan istilah "disclosing personal data without consent".

Tindakan doxing pada dasarnya berkaitan erat dengan privasi dan data pribadi seseorang di internet. Perlindungan atas hak privasi dan data pribadi di Indonesia secara implisit diatur dalam Undang-Undang Dasar 1945 (UUD 1945) dalam Pasal 28G yang berbunyi:

"Setiap orang berhak atas perlindungan diri pribadi, keluarga, kehormatan, martabat, dan harta benda yang dibawah kekuasannya, serta berhak atas rasa aman dan perlindungan dari ancaman ketakutan untuk berbuat atau tidak berbuat sesuatu yang merupakan hak asasi"

Kemudian Pemerintah bersama dengan lembaga legislatif membuat undang-undang yang berisikan aturan-aturan dalam berkegiatan di dunia siber yaitu Undang-Undang Nomor 19 Tahun 2016 tentang Perubahan atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE). Dengan disahkan UU ITE ini diharapkan memberikan rasa aman, keadilan dan kepastian hukum baik bagi pengguna ataupun bagi penyelenggara sistem elektronik.

[5]Roney Simon M, S. Aghili, & Dale L, "A Study of Doxing, its Security Implications and Mitigation Strategies for Organizations", Master of Information Systems Security Management (MISSM) and Master of Information Systems Assurance Management (MISAM) Project Reports (Concordia University of Edmonton),2014

[6]Daniel Trottier, "Denunciation and doxing: towards a conceptual model of digital vigilantism", Global Crime, 21:3-4, 2020, hlm.206

[7]Jogja Tribun News, "Cemburu Mantan Kekasih Punya Pacar Baru, Pria di Aceh Ini Sebar Foto Syur, Akhirnya Ditangkap Polisi." https://jogja.tribunnews.com/2021/04/21/cemburu-mantan-kekasih-punya-pacar-baru-pria-di-aceh-ini-sebar-foto-syur-akhirnya-ditangkap-polisi?page=2

[8]CNN Indonesia, "Pembocor Data Pribadi Denny Siregar Divonis 8 Bulan Penjara" https://www.cnnindonesia.com/nasional/20210303175401-12-613324/pembocor-data-pribadi-denny-siregar-divonis-8-bulan-penjara

[9]Pedro Anguita R, "Freedom of Expression in Social Networks and Doxing" The Handbook of Communication Rights, Law, and Ethics, 2021, hlm. 285

[10]David M. Douglas, Op.cit.,hlm. 208

[11]Julia M. MacAllister, Op.Cit., hlm.2456

[12]David M. Douglas, Op.cit., hlm.200-205

[13]Pedro Anguita R, Op.cit., hlm. 284-287

[14]Penjelasan Pasal 26 ayat 1 Undang-Undang Nomor 19 Tahun 2016 tentang Perubahan atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE)

[15]David M. Douglas, Op.cit., hlm.204

[16]Ibid.,hlm. 205

[17]Pasal 26 ayat 2 Undang-Undang Nomor 19 Tahun 2016 tentang Perubahan atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE)

[18]Section 64 (6) Personal Data Privacy Ordinance (PDPO) Amandemen tahun 2021

[19]Personal Data (Privacy) (Amendment) Ordinance 2021 Implementation Guideline, https://www.pcpd.org.hk/english/resources_centre/publications/guidance/guidance.html

[20]David M. Douglas, Op. cit., hlm.206

[21]Section 61 (3) Personal Data Privacy Ordinance (PDPO) Amandemen tahun 2021

Setelah memahami konsep tindakan doxing, terdapat beberapa hal penting yang perlu diperhatikan ketika terjadinya tindakan doxing yaitu:

1) Ada atau tidaknya persetujuan (consent) diungkapkan data
2) Muatan atau bentuk data pribadi yang diungkapkan
3) Cara perolehan muatan atau data pribadi yang diungkapkan
4) Akibat atau bentuk kerugian yang diderita oleh korban (target)
5) Alasan atau motif dilakukannya tindakan doxing

Pada poin pertama, ketentuan dalam UU ITE yang dapat melindungi privasi dan data pribadi seseorang dari tindakan doxing tercantum pada Pasal 26 ayat 1 yaitu:

"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."

Dalam pasal tersebut dapat digarisbawahi adanya prinsip persetujuan (consent) dalam perlindungan data pribadi. Prinsip persetujuan (consent) dalam perlindungan data pribadi dapat melindungi seseorang dari tindakan doxing yang pada konsepnya menyangkut data pribadi seseorang yang diungkapkan tanpa persetujuan (consent) pemilik data pribadi ke internet. Pada penjelasan Pasal 26 ayat 1 dijelaskan bahwa perlindungan data pribadi merupakan bagian dari hak pribadi (privacy rights) yang merupakan hak untuk menikmati kehidupan dan bebas dari gangguan, hak bebas dari tindakan memata-matai dalam berkomunikasi serta hak untuk mengawasi akses informasi tentang kehidupan pribadi dan data seseorang. Sehingga setiap orang memiliki hak agar tidak di ganggu dan untuk tidak digunakan data pribadinya tanpa adanya persetujuan terlebih dahulu. Prinsip persetujuan ini juga ditegaskan kembali dalam Pasal 21 Peraturan Menteri Komunikasi dan Informatika Nomor 20 Tahun 2016 Tentang Perlindungan Data Pribadi (Permen Kominfo 20/2016) beserta aturan-aturan yang berkaitan dengan pelaksanaan pemrosesan data pribadi.

Pada poin kedua, ketika pelaku tindakan doxing mengungkapkan data pribadi seseorang ke internet, para ahli berpendapat bahwa data-data yang didapatkan biasanya memang sudah tersebar di internet. Definisi data pribadi tidak diatur dalam UU ITE melainkan diatur dalam Permen Kominfo 20/2016 Pasal 1 yaitu data perseorangan tertentu yang disimpan, dirawat, dan dijaga kebenaran serta dilindungi kerahasiaannya. Begitu juga dengan jenis data pribadi yang tidak diatur dalam UU ITE ataupun Permen Kominfo 20/2016. Dalam Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi, jenis data pribadi diatur dalam Pasal 4 yang terdiri atas data pribadi yang bersifat umum meliputi nama lengkap, jenis kelamin, kewarganegaraan, agama, dan data pribadi yang dikombinasikan untuk mengidentifikasi seseorang, serta data pribadi yang bersifat spesifik meliputi informasi kesehatan, data biometric, data genetika, orientasi seksual, pandangan politik, catatan kejahatan, data anak, data keuangan pribadi, dan data-data lain yang sesuai ketentuan perundang-undangan.

Meskipun tidak mengatur terkait definisi ataupun jenis data pribadi, UU ITE mengatur terkait perbuatan yang dilarang terhadap informasi dan dokumen elektronik yang memiliki muatan tertentu. Dalam Pasal 27 ayat 1, 3, dan 4 dijelaskan bahwa setiap orang tidak boleh baik dengan sengaja dan tanpa hak untuk mendistribusikan dan/atau mentransmisikan dan/atau membuat dapat diaksesnya informasi dan/atau dokumen elektronik yang memiliki muatan kesusilaan, penghinaan dan/atau pencemaran nama baik, serta pemerasan dan/atau pengancaman. Dalam kaitannya dengan tindakan doxing, pasal ini mengatur berkaitan dengan data-data yang diungkapkan pelaku ke internet. Seperti contoh kasus tindakan doxing yang dilakukan FIR kepada mantan pacarnya MDN, pelaku

[22]Samuel D. Warren dan Louis D. Brandeis, "The Right to Privacy," Harvard Law Rev, vol. IV, no. 5, hlm. 193–220, 1890, hlm. 1

[23]Neng Yani Nurhayani, Hukum Perdata, Bandung: CV.Pustaka Setia, 2015

[24]Moeljatno, Asas-Asas Hukum Pidana, Cetakan IX, Jakarta: Rineka Cipta, 2015

[25]Julia M. MacAllister, Op.Cit.,hlm. 2456

[26]David M. Douglas, Op. cit., hlm.206

dengan sengaja dan tanpa hak menyebarluaskan foto tidak senonoh milik MDN di group Whatsapp mahasiswa kampus yang mana membuat foto tersebut dapat diakses oleh orang lain. Dalam kasus tersebut data yang diungkapkan memiliki muatan kesusilaan yang mana pelaku melanggar Pasal 27 ayat 1 dan dapat dikenakan sanksi.

Kemudian berkaitan dengan poin ketiga, perlindungan terhadap tindakan doxing dalam UU ITE juga terdapat pada Pasal 30 yang berkaitan dengan pengaksesan komputer atau sistem elektronik untuk memperoleh data. Dalam Pasal 30 ini terdapat perlindungan dari pengaksesan secara melawan hukum dengan cara apapun, dengan tujuan memperoleh informasi dan dokumen elektronik, serta dengan melanggar, menerobos, atau menjebol sistem pengamanan.Seperti dalam kasus tindakan doxing yang dialami Denny Siregar, pelaku memperoleh data pribadi Denny dengan cara mengaksesnya menggunakan sistem elektronik milik Telkomsel tempat pelaku dulu pernah bekerja sebagai karyawan outsourcing. Saat mengakses data pribadi Denny pelaku sudah tidak lagi berstatus sebagai karyawan aktif di Telkomsel, maka dari itu pelaku dikatakan secara melawan hukum mengakses sistem elektronik milik Telkomsel untuk memperoleh data pribadi Denny. Maka dari itu pelaku dikenakan Pasal 30 ayat 2.

Jika melihat konsep dari tindakan doxing yang dipaparkan, terdapat alasan atau motif tertentu dilakukannya tindakan doxing serta akibat atau bentuk kerugian yang diderita korban (target) yang menjadi hal penting untuk mengetahui apakah tindakan doxing yang dilakukan pelaku perlu diminta pertanggungjawaban atau tidak. Dalam konsep yang dipaparkan David M. Douglas, terdapat kategori dari tindakan doxing yang berkaitan dengan sejauh mana alasan atau motif dilakukannya tindakan doxing tersebut mempengaruhi korban atau targetnya. Pada kategori tindakan doxing Deanonymizing, Douglas menyatakan bahwa informasi yang diungkapkan yaitu identitas seseorang yang pada awalnya memang tidak pernah diketahui identitasnya (anonim) atau hanya dikenal dengan nama samaran saja. Ketika seseorang melakukan deanonymizing maka hak privasi seseorang atas kerahasiaan identitas pribadinya dilanggar, hal ini kemudian dapat mengintimidasi orang yang tidak ingin identitasnya diketahui publik. Menurut Douglas, deanonymizing ini mungkin tidak mengakibatkan bahaya yang terlalu besar terhadap korban namun kembali lagi kepada sejauh mana kerahasiaan identitas seseorang dan bentuk identitas yang diungkapkan seperti apa oleh pelaku.

Berbeda dengan tindakan doxing Targeting, yang mempublikasikan informasi spesifik tentang keberadaan fisik seseorang yang memungkinkan dapat dilacak dan ditemukan lokasi keberadaannya. Dalam tindakan doxing ini seseorang sangat rentan dalam bahaya fisik seperti serangan hingga pelecehan. Douglas menjelaskan bahwa biasanya pelaku tindakan targeting ini mempublikasikan identitas pribadi targetnya dengan bentuk ajakan untuk menyerang ataupun melecehkan targetnya. Tindakan doxing targeting ini seperti pada kasus yang peneliti bahas sebelumnya yaitu dimana korban penipuan transaksi jual-beli secara online mengungkapkan identitas pelaku penipuan ke media sosial Twitter bersamaan dengan foto dan alamat lengkap tempat tinggalnya. Tindakan tersebut dapat mengakibatkan pelaku penipuan untuk diketahui keberadaannya dan meningkatkan kemungkinan terjadinya bahaya fisik.

Kemudian tindakan doxing Delegitimizingyaitu pelaku mempublikasikan informasi yang bersifat privat dengan maksud merusak atau menjatuhkan reputasi dan karakter seseorang. Seperti contoh kasus yang penulis bahas pada bab sebelumnya yaitu kasus revenge porn MDN yang menjadi korban dari mantan pacar yang mempublikasikan foto dan video seksual ke media sosial karena tidak terima hubungan diselesaikan. Tindakan yang dilakukan pelaku tersebut termasuk delegitimizing karena berakibat kepada reputasi MDN yang tercoreng serta mempengaruhi psikologis mereka. David M. Douglas dalam artikel jurnalnya memang berpendapat bahwa tindakan doxing biasanya berkonotasi negative, dari ketiga kategori tindakan doxing tersebut terlihat bahwa akibat ataupun kerugian yang diderita dari data pribadi yang diungkapkan oleh pelaku tindakan doxing ke internet karena alasan ingin mengintimidasi korban dapat mempengaruhi privasi pemilik data hingga ke keadaan psikologis dan juga keadaan fisiknya.

Dalam pengaturan UU ITE, perlindungan terhadap tindakan doxing hanya pada pelanggaran atas penggunaan data pribadi tanpa persetujuan (consent), muatan atau data pribadi yang diungkapkan serta cara perolehan atas data pribadi saja. Seperti pada Pasal 26 ayat 2 dijelaskan bahwa ketika setiap orang terbukti menggunakan data pribadi orang lain tanpa hak maka dapat mengajukan gugatan atas kerugian yang timbul berdasarkan dengan undang-undang. Kemudian dalam Permen Kominfo 20/2016 Pasal 36 dijelaskan bahwa setiap orang yang mengumumkan dan/atau menyebarluaskan data pribadi tanpa hak atau tidak sesuai ketentuan dalam peraturan menteri tersebut atau peraturan perundang-undangan lain dikenakan sanksi administratif berupa peringatan lisan, peringatan tertulis, penghentian sementara kegiatan dan/atau pengumuman di situs dalam jaringan (website online). Kemudian dalam hal muatan atau data pribadi yang diungkapkan sesuai UU ITE, bagi setiap orang yang melanggar Pasal 27 ayat 1, 3 dan 4 maka berdasarkan Pasal 45 ayat 1 dan 4 dapat dipidana penjara paling lama 6 (enam) tahun dan/atau denda paling banyak Rp1.000.000.000,00 (satu miliar rupiah) serta Pasal 45 ayat 3 dapat dipidana penjara paling lama 4 (empat) tahun dan/atau denda paling banyak Rp750.000.000,00 (tujuh ratus lima puluh juta rupiah). Dalam hal perolehan atas data pribadi yang dilakukan secara melawan hukum yaitu Pasal 30 UU ITE khususnya pada ayat 2, bagi setiap orang yang memenuhi unsur pasal tersebut maka dapat dipidana penjara paling lama 7 (tujuh tahun) dan/atau denda paling banyak Rp700.000.000,00 (tujuh ratus juta rupiah).

Perlindungan tindakan doxing dalam UU ITE hanya terbatas kepada pengungkapan di internet tersebut memiliki muatan atau data pribadi yang melanggar asusila, penghinaan dan/atau pencemaran nama baik serta pengaksesan sistem elektronik dalam memperoleh data pribadi saja tidak mencakup akibat baik fisik ataupun non fisik dan alasan dilakukannya tindakan doxing tersebut. Berbeda dengan Hong Kong PDPO 2021 yang mana mengatur hingga ke akibat yang diderita korban serta alasan dilakukannya tindakan doxing itu sendiri. Dalam PDPO 2021 Section 64 terdapat ketentuan yang berbunyi:

(3A)A person commits an offence if the person discloses any personal data of a data subject without the relevant consent of the data subject—

(a) with an intent to cause any specified harm to the data subject or any family member of the data subject; or

(b) being reckless as to whether any specified harm would be, or would likely be, caused to the data subject or any family member of the data subject. (Added 32 of 2021 s. 6)

(3B)A person who commits an offence under subsection (3A) is liable on conviction to a fine at level 6 and to imprisonment for 2 years. (Added 32 of 2021 s. 6)

Pada ketentuan diatas terdapat beberapa hal yang dilindungi yaitu tidak hanya pada pengungkapan data pribadi tanpa persetujuan (consent) namun juga pada niat dilakukannya tindakan doxing tersebut berakibat membahayakan tidak hanya pemilik data, namun juga keluarganya.

Terdapat juga penjelasan sejauh mana bahaya atau 'specified harm' yang dapat diderita korban ataupun keluarganya akibat tindakan doxing yang dialami meliputi:

a. harassment, molestation, pestering, threat or intimidation to the person
b. bodily harm or psychological harm to the person
c. harm causing the person reasonably to be concerned for the person's safety or well-being
d. damage to the property of the person.

Penjelasan seperti bahaya atau kerugian seperti apa yang diakibatkan oleh tindakan doxing ini belum diatur dalam pengaturan di Indonesia. Dalam penjelasan Section 64 (3A) dan (3B), ketentuan ini dapat digunakan untuk kasus tindakan doxing meski tidak memiliki bukti adanya bahaya yang terjadi kepada korban ataupun keluarganya.

Sedangkan apabila terbukti adanya bahaya yang terjadi, maka dapat mengacu pada ketentuan berikut:

(3C) A person commits an offence if—

(a) the person discloses any personal data of a

data subject without the relevant consent of the data subject—

(i) with an intent to cause any specified harm to the data subject or any family member of the data subject; or

(ii) being reckless as to whether any specified harm would be, or would likely be, caused to the data subject or any family member of the data subject; and

(b) the disclosure causes any specified harm to the data subject or any family member of the data subject. (Added 32 of 2021 s. 6)

(3D) A person who commits an offence under subsection (3C) is liable on conviction on indictment to a fine of $1,000,000 and to imprisonment for 5 years. (Added 32 of 2021 s. 6)

Perbedaan dari ketentuan sebelumnya yaitu pada ketentuan (3C) poin (b) yang menegaskan terbukti adanya bahaya tertentu (specified harmed) terjadi kepada korban ataupun keluarganya. Ketentuan harus terbukti atau tidak terbukti terjadi bahaya tertentu kepada korban ataupun keluarga korban ini memberikan perbedaan dalam penjatuhan sanksi terhadap pelaku. Jika tindakan doxing terjadi tanpa terbukti adanya bahaya yang terjadi kepada korban ataupun keluarga korban maka dapat dikenakan denda level 6 atau sebesar maksimal HK$100,000 (seratus ribu dollar Hong Kong) dan pidana penjara maksimal 2 tahun. Sedangkan jika terbukti adanya bahaya yang terjadi kepada korban ataupun keluarganya maka dapat dikenakan denda hingga HK$1,000,000 (satu juta dollar Hong Kong) dan pidana penjara maksimal 5 tahun. Terlihat perbedaan dalam pemberian sanksi terhadap tindakan doxing dalam PDPO 2021 dengan UU ITE.

Ketika melihat alasan atau motif dilakukannya tindakan doxing, terdapat beberapa kasus dilakukannya tindakan doxing untuk kepentingan transparansi publik, jurnalistik, hingga untuk mencari keadilan atau online vigilantism. Dalam perundang-undangan di Indonesia, khususnya dalam penelitian ini yaitu UU ITE, belum ada ketentuan yang mengatur khusus untuk pengecualian diberlakukannya pengaturan terhadap suatu tindakan ketika dilakukan dengan alasan atau motif tersebut. Douglas berpendapat bahwa tindakan doxing boleh dilakukan namun harus ada alasan tertentu yang memang berpengaruh kepada kepentingan publik seperti dilakukan kepada pelaku kejahatan. Namun perlu diingat bahwa informasi yang diungkapkan hanya yang memperlihatkan identitas seseorang dan masih berkaitan dengan kejahatan yang dilakukannya. Sehingga ketika tindakan doxing tersebut terjadi, maka alasan itulah yang akan membenarkan identitas seseorang untuk diungkapkan ke internet. Namun ketika tindakan doxing dilakukan untuk mengintimidasi serta dapat meningkatkan kemungkinan targetnya terkena bahaya fisik, maka tidak dapat dibenarkan karena hal ini sudah mengganggu privasi.

Melihat konsep tindakan doxing tersebut maka penting sekali untuk mengetahui apa yang mendasari terjadinya tindakan doxing di media sosial. Dalam hal tindakan doxing dilakukan untuk kepentingan publik dapat dilihat pada contoh kasus pelecehan seksual yang dilakukan pelatih futsal diKabupaten Bogor berinisial GJ. Tindakan doxing yang dilakukan di Twitter dan Instagram ini terjadi karena sudah terlalu banyak anak laki-laki dibawah umur yang menjadi korban pelecehan seksual yang dilakukan namun takut untuk melaporkan karena masih ingin tetap dalam akademi futsal tersebut. Dalam kasus tersebut data pribadi yang diekspos hanya yang berkaitan dengan kejahatan yang dilakukan dan identitas pelaku seperti nama lengkap, akun media sosial, foto, hingga percakapan atau chat Whatsapp yang merupakan bukti tindakan pelaku melakuan pelecehan. Dalam kasus seperti ini, pengguna media sosial yang melakukan tindakan doxing terhadap pelaku pelecehan seksual ini dapat dibenarkan karena dilakukan dengan harapan tidak ada lagi korban-korban baru dan pelaku diproses kepolisian.

Dalam Section 64 Hong Kong PDPO 2021 terdapat ketentuan yang menjelaskan bahwa adanya pengecualian untuk orang yang diancam ketentuan (1), (3A) atau (3C) karena melakukan tindakan doxing. Pada ketentuan (4) yang dijelaskan bahwa dalam proses peradilan dapat melakukan pembelaan atas tuduhan yang dibebankan dengan cara harus dapat membuktikan bahwa pengungkapan data yang dilakukannya memang diperlukan untuk mencegah atau mendeteksi kejahatan, pengungkapan perlu untuk di-

lakukan atau secara sah atau berlaku oleh ketentuan hukum atau dengan perintah pengadilan, memang sudah mendapat persetujuan dari pemilik data, serta pengungkapan data pribadi dilakukan dengan tujuan untuk 'news activity' dan memiliki alasan yang pasti dalam mempublikasikan atau menayangkan data pribadi seseorang untuk kepentingan umum. News activity ini maksudnya adalah aktivitas jurnalistik yang meliputigathering, preparation or compiling articles or programmes, observations on news or current affairs for the purpose of dissemination to public.

Pertanggungjawaban Hukum Atas Tindakan Doxing di Media Sosial Yang Dilakukan Oleh Korban Kejahatan Dikaitkan Dengan Konsep Perlindungan Privasi

Pada konsep perlindungan privasi oleh para ahli ditegaskan bahwa privasi merupakan hak manusia untuk menikmati hidup dan hak untuk tidak diganggu. Hak privasi tersebut diantaranya hak atas diri pribadi, untuk bebas dari gangguan orang lain, rumah tangga atau keluarga, hak untuk tidak dikenal atau diketahui identitasnya, keberadaan tempat tinggal ataupun tempat kerja, hak dalam berkomunikasi, hingga hak atas informasi atau data pribadi.

Tindakan doxing merupakan tindakan mencari informasi atau data pribadi orang lain kemudian dipublikasikan atau disebarluaskan ke internet tanpa persetujuan (consent) pemilik data dengan maksud tertentu ataupun dengan niat jahat. Definisi tindakan doxing tersebut secara jelas memperlihatkan bahwa tindakan doxing tersebut sebenarnya melanggar hak privasi seseorang yang dilindungi.

Hak privasi atas data pribadi merupakan suatu bentuk dari hak asasi manusia yang harus dilindungi karenasetiap orang tetap berhak untuk mengontrol informasi atau data pribadinya agar terbebas dari pelecehan, ancaman ataupun perasaan takut yang dapat diakibatkan oleh tindakan doxing, meskipun tindakan doxing terjadi dengan mendapatkan data pribadi yang sudah semi-public. Jika merujuk kepada kategori oleh para ahli, tindakan doxing dapat mempengaruhi privasi seseorang mulai dari hak seseorang untuk tidak dikenal atau diketahui identitasnya, hak atas informasi atau data pribadi, hak atas keluarga atau rumah tangga, hak atas berkomunikasi, hingga hak untuk dapat diketahui keberadaan fisik seseorang misalnya dalam hal tempat tinggal hingga tempat bekerjanya.

Melihat beberapa kasus tindakan doxing yang dilakukan oleh korban kejahatan biasanya dilakukan dengan alasan untuk memperingatkan orang lain agar tidak menjadi korban selanjutnya atau mencari keadilan karena lamanya kasus untuk diproses ataupun tidak kunjung diproses oleh kepolisian. Dalam konsep perlindungan privasi, para korban kejahatan yang melakukan tindakan doxing ini sebenarnya dapat diminta pertanggungjawaban karena secara sadar melanggar ketentuan hukum yang melindungi penggunaan data pribadi seseorang tanpa persetujuan pemiliknya.

Selain UUD 1945, Indonesia memberikan perlindungan privasi atas data pribadi dari tindakan doxing yaitu pada Pasal 26 UU ITE yang berbunyi:

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 dilanggar haknya sebagaimana dimaksud pada ayat (1) dapat mengajukan gugatan atas kerugian yang ditimbulkan berdasarkan Undang-Undang ini.

Pelaku tindakan doxing yang pada dasarnya menggunakan informasi pribadi orang lain tanpa persetujuan melalui media elektronik dapat diminta pertanggungjawabannya sesuai Pasal 26 ayat 2 dengan mengajukan gugatan Perbuatan Melawan Hukum (PMH) berdasarkan kepada unsur kesalahan pada Pasal 1365 Kitab Undang-Undang Hukum Perdata (KUHPerdata) yang berbunyi:

"Tiap perbuatan yang melawan hukum dan membawa kerugian kepada orang lain, mewajibkan orang yang menimbulkan kerugian itu karena kesalahannya untuk mengganti kerugian tersebut"

Kerugian yang dimaksud di atas diantaranya kerugian materiil (fisik) yaitu kerugian terhadap harta benda korban tindakan doxing serta kerugian imma-

teriil (non fisik) yaitu seperti rasa takut, cemas, atau trauma.

Lalu dalam Permen Kominfo 20/2016 dijelaskan juga bahwa penggunaan data pribadi orang lain tanpa hak atau melanggar ketentuan dalam peraturan menteri tersebut atau peraturan perundang-undangan lain maka dapat dikenakan sanksi administratif yang diberikan oleh menteri atau pimpinan instansi pengawas dan pengatur sektor terkait sesuai ketentuan. Sanksi administrasi atas penggunaan data pribadi tanpa hak tersebut diatur dalam Pasal 36 yang berbunyi:

(1) Setiap Orang yang memperoleh, mengumpulkan, mengolah, menganalisis, menyimpan, menampilkan, mengumumkan, mengirimkan, dan/atau menyebarluaskan Data Pribadi tanpa hak atau tidak sesuai dengan ketentuan dalam Peraturan Menteri ini atau peraturan perundang-undangan lainnya dikenai sanksi administratif sesuai dengan ketentuan peraturan perundang-undangan berupa:

a. peringatan lisan;
b. peringatan tertulis;
c. penghentian sementara kegiatan; dan/atau
d. pengumuman di situs dalam jaringan (website online).

Dalam pertanggungjawaban pidana terdapat unsur-unsur yang harus dipenuhi untuk memastikan apakah seseorang dapat diminta pertanggungjawaban. Unsur-unsur tersebut diantaranya adanya suatu tindak pidana yang mana perbuatan yang dilakukan merupakan perbuatan yang dilarang dalam undang-undang sesuai dengan asas legalitas nullum delictum nulla poena sine praevia lege poenali yang artinya perbuatan tidak dapat dipidana apabila tidak terdapat aturan atau undang-undang yang mengatur terkait larangan perbuatan tersebut. Kemudian unsur kesalahan juga berperan penting untuk mengetahui apakah pelaku tindak pidana mampu untuk dimintakan pertanggungjawaban atas perbuatannya.

Pada dasarnya perbuatan melawan hukum di dunia siber atau internet dilakukan secara sadar atau dengan sengaja sehingga memenuhi unsur kesalahan dalam pertanggungjawaban pidana sehingga dapat dijatuhi hukuman atas perbuatannya. Dengan demikian pelaku tindakan doxing dapat dimintakan pertanggungjawaban atas tindakannya yang melawan hukum. Dalam UU ITE, ketentuan yang berkaitan dengan tindakan doxing yaitu Pasal 27 ayat 1, 3 dan 4. Pasal 27 ayat 2 tidak berkaitan dengan tindakan doxing karena mengatur unsur muatan perjudian. Maka jika melanggar Pasal 27 ayat 1, 3 dan 4 maka dapat dikenakan sanksi Pasal 45:

(1) Setiap Orang yang 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 kesusilaan sebagaimana dimaksud dalam Pasal 27 ayat (1) dipidana dengan pidana penjara paling lama 6 (enam) tahun dan/atau denda paling banyak Rp1.000.000.000,00 (satu miliar rupiah).

(3) Setiap Orang yang 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 sebagaimana dimaksud dalam Pasal 27 ayat (3) dipidana dengan pidana penjara paling lama 4 (empat) tahun dan/atau denda paling banyak Rp750.000.000,00 (tujuh ratus lima puluh juta rupiah).

(4) Setiap Orang yang 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 sebagaimana dimaksud dalam Pasal 27 ayat (4) dipidana dengan pidana penjara paling lama 6 (enam) tahun dan/atau denda paling banyak Rp1.000.000.000,00 (satu miliar rupiah).

Jika melihat dari contoh kasus korban penipuan jual-beli di Twitter yang mengungkapkan nama lengkap, foto, nomor telepon, akun pribadi, hingga alamat tempat tinggal pelaku penipuan ini berdasarkan konsep perlindungan privasi merupakan tindakan yang

melanggar privasi pelaku penipuan. Pengungkapan atas data-data tersebut sudah melanggar hak atas informasi atau data pribadi yang mempengaruhi hak seseorang untuk tidak dikenal atau diketahui identitasnya serta keberadaan tempat tinggal. Tindakan doxing tersebut mengungkapkan data seseorang yang dapat mengakibatkan pelaku penipuan dalam bahaya fisik atau dalam kategori Douglas termasuk dalam tindakan doxing Targeting karena dalam postingan tersebut terdapat ajakan yang membahayakan pelaku penipuan secara fisik. Korban penipuan yang tersebut dapat dikenakan sanksi karena pengungkapan data pribadi serta terdapat muatan pemerasan dan/atau pengancaman yang dapat membahayakan orang lain meski dalam kasus ini seorang pelaku penipuan.

Kemudian pada kasus tindakan doxing terhadap pelaku pelecehan pelatih futsal di Kabupaten Bogor berinisial GJ, informasi yang diungkapkan yaitu nama lengkap, foto, akun Instagram, tempat bekerja hingga isi percakapan dan foto berasal dari Whatsapp antara pelaku dengan korban yang tidak senonoh, Dalam kasus ini maka dapat dikatakan sudah melanggar hak atas informasi atau data pribadi yang mempengaruhi hak seseorang untuk tidak dikenal atau diketahui identitasnya, hak untuk tidak diketahui tempat bekerja, serta hak atas berkomunikasi. Pada kasus ini terlihat bahwa tindakan doxing yang dilakukan terhadap pelaku pelecehan seksual termasuk dalam tindakan doxing Delegitimizingkarena dilakukan untuk menjatuhkan reputasi atau mempermalukan pelaku tersebut karena telah melakukan pelecehan terhadap anak-anak didiknya yang masih dibawah umur. Pelaku tindakan doxing ini dapat dikenakan sanksi karena mengungkapkan percakapan dari Whatsapp chat yang memiliki muatan yang melanggar kesusilaan di internet yang dapat diakses oleh publik, maka pelaku tindakan doxing dapat dikenakan Pasal 45 ayat 1.

Dalam poin perolehan muatan atau data pribadi yang diungkapkan, apabila data pribadi targetnya didapatkan dengan cara illegal, maka pelaku tindakan doxing dapat dikenakan sanksi sesuai cara pemerolehan data pribadi tersebut sesuai pada Pasal 30:

(1) Setiap Orang dengan sengaja dan tanpa hak atau melawan hukum mengakses Komputer dan/atau Sistem Elektronik milik Orang lain dengan cara apa pun.
(2) Setiap Orang dengan sengaja dan tanpa hak atau melawan hukum mengakses Komputer dan/atau Sistem Elektronik dengan cara apa pun dengan tujuan untuk memperoleh Informasi Elektronik dan/atau Dokumen Elektronik.
(3) Setiap Orang dengan sengaja dan tanpa hak atau melawan hukum mengakses Komputer dan/atau Sistem Elektronik dengan cara apa pun dengan melanggar, menerobos, melampaui, atau menjebol sistem pengamanan.

Tindakan doxing selain dengan memperoleh data pribadi seseorang yang memang dapat ditemukan di internet, biasanya pelaku memperoleh data dengan cara hacking atau peretasan, yang mana melanggar Pasal 30 ayat 2 dan dapat dikenakan sanksi sesuai Pasal 46 ayat 2 yaitu pidana penjara paling lama 7 (tujuh) tahun dan/atau denda paling banyak Rp700.000.000,00 (tujuh ratus juta rupiah). Peraturan tersebut memiliki kesamaan dengan Computer Fraud and Abuse Act (CFAA) Amerika yang hanya mengatur pemberian sanksi ketika tindakan doxing dilakukan dengan hacking untuk memperoleh data targetnya, jika tidak dilakukan hacking dalam memperoleh data maka ketentuan tersebut tidak dapat berlaku.

Jika membandingkan dengan pengaturan tindakan doxing dalam Section 64 Hong Kong PDPO 2021, pemberian sanksi sebagai bentuk pertanggungjawaban atas perbuatan mengungkapkan data pribadi seseorang tanpa persetujuan (consent) pemilik data terdapat pada Section 64 (3A) dan (3C). Kedua ketentuan ini dibedakan atas dasar niat atau alasan dilakukannya tindakan doxing dan dampak kerugian atau bahaya yang dirasakan atas pemilik data serta keluarganya. Pada ketentuan (3A) dan (3C) ini dijelaskan dalam poin (ii) bahwa pengungkapan data pribadi seseorang dilakukan dengan niat jahat atau dengan lalai atas bahaya yang akan ataupun mungkin terjadi tidak hanya kepada pemilik data namun juga keluarganya. Perbedaan atas kedua ketentuan tersebut yaitu dalam ketentuan (3A) tidak terbukti adanya bahaya yang disebabkan oleh tindakan doxing tersebut ke-

pada pemilik data ataupun keluarganya yang disebut dengan first tier offence. Setiap orang yang melanggar ketentuan ini bertanggungjawab untuk menjalankan sanksi pidana maksimal 2 (dua) tahun penjara dan maksimal denda Level 6 atau sebesar HK$100,000 (seratus ribu dollar Hong Kong). Sedangkan pada ketentuan (3C) terdapat poin (iii) yaitu pengungkapkan mengakibatkan bahaya tertentu kepada pemilik data dan keluarganya sehingga disebut dengan second tier offence. Setiap orang yang melanggar ketentuan ini dan mengakibatkan bahaya kepada pemilik data dan keluarganya maka bertanggungjawab untuk menjalankan sanksi pidana maksimal 5 (lima) tahun penjara dan denda maksimal HK$1,000,000 (satu juta dollar Hong Kong).

Dalam hal apakah tindakan doxing dapat dibenarkan atau tidak, Douglas berpendapat bahwa ada dua bentuk tindakan doxing masih dapat diperbolehkan jika memang dilakukan demi kepentingan publik. Seperti tindakan doxing deanonymizing dan delegitimizing yang mengungkapkan identitas pelaku kejahatan ke internet dengan alasan untuk mengekspos tindakan pelaku. Alasan tersebutlah yang kemudian akan membenarkan dilakukannya tindakan doxing terhadap pelaku kejahatan. Sehingga informasi yang diungkapkan hanya memperlihatkan identitas pelaku dan yang masih berkaitan dengan kejahatan dilakukan. Hal ini kemudian berujung kepada pelaku tindakan doxing yang tidak perlu diminta pertanggungjawabannya karena tindakannya dilakukan dengan alasan mencari keadilan demi kepentingan publik. Sedangkan untuk tindakan doxing targeting, Douglas mengatakan bahwa tindakan doxing ini tidak dapat dibenarkan karena dilakukan dengan alasan untuk mengintimidasi dan mengarahkan orang lain untuk mengganggu hingga membahayakan fisik seseorang.

Perlu adanya batasan-batasan untuk dapat dilakukannya pengungkapan informasi atau data pribadi baik oleh setiap orang atau untuk kegiatan jurnalistik. Samuel Warren mengungkapkan bahwa hak privasi tidak bersifat absolut dan tidak menutup kemungkinan untuk mempublikasikan data privasi seseorang demi kepentingan publik. Peraturan di Indonesia seperti UU ITE sendiri belum memiliki pengaturan berkaitan dengan pengecualian ataupun pembelaan yang dapat dilakukan ketika seseorang melakukan tindakan doxing dengan alasan tertentu atau untuk kepentingan publik seperti peraturan yang dimiliki Hong Kong PDPO 2021. Maka dari itu dibutuhkan pengaturan yang secara khusus dan lebih komprehensif dalam mengatur terkait tindakan doxing atau pengungkapan data pribadi seseorang tanpa persetujuan (consent) pemilik data dalam peraturan perundang-undangan Indonesia.

Kesimpulan

Tindakan doxing merupakan tindakan pengungkapan informasi atau data pribadi seseorang di internet tanpa persetujuan (consent) pemilik data dan umumnya dengan maksud jahat. Pada dasarnya Indonesia belum memiliki pengaturan yang secara khusus mengatur tentang tindakan doxing namun dalam UU ITE perlindungan atas tindakan doxing tersebut dapat ditemukan pada Pasal 26 ayat 1 yang menegaskan prinsip persetujuan (consent) dalam menggunakan informasi menyangkut data pribadi seseorang. Perlindungan data pribadi dalam UU ITE dari tindakan doxing lainnya yaitu terdapat pada Pasal 27 ayat 1, 3 dan 4 serta Pasal 30 ayat 2.

Tindakan doxing di media sosial yang dilakukan oleh korban kejahatan terhadap pelaku kejahatan berdasarkan konsep perlindungan privasi yang dikemukakan para ahli dapat dimintakan pertanggungjawaban sesuai Pasal 26 UU ITE dengan mengajukan gugatan perbuatan melawan hukum, penjatuhan sanksi administratif sesuai Pasal 36 Permen Kominfo 20/2016 berupa peringatan lisan, peringatan tertulis, penghentian sementara kegiatan dan/atau pengumuman di situs dalam jaringan (website online), serta penjatuhan sanksi pidana dan denda sesuai pada Pasal 45 ayat 1, 3 dan 4 atas pelanggaran Pasal 27 ayat 1, 3 dan 4 lalu Pasal 46 ayat 2 atas pelanggaran Pasal 30 ayat 2 yang mengatur tentang larangan dengan sengaja dan tanpa atau melawan hukum mengakses komputer dan/atau sistem elektronik dengan cara apapun dengan tujuan untuk memperoleh informasi dan/atau dokumen elektronik.

Daftar Pustaka

Sugeng, Hukum Telematika Indonesia. Jakarta:

Prenadamedia Group, 2020

Neng Yani Nurhayani, Hukum Perdata, Bandung: CV. Pustaka Setia, 2015

Moeljatno, Asas-Asas Hukum Pidana, Cetakan IX, Jakarta: Rineka Cipta, 2015

Peraturan Menteri Komunikasi dan Informatika Nomor 20 Tahun 2016 tentang Perlindungan Data Pribadi dalam Sistem Elektronik

Personal Data (Privacy) (Amendment) Ordinance 2021 Implementation Guideline, https://www.pcpd.org.hk/english/resources_centre/publications/guidance/guidance.html

Daniel Trottier, "Denunciation and doxing: towards a conceptual model of digital vigilantism", Global Crime, 21:3-4, 2020

David M. Douglas, "Doxing: A Conceptual Analysis", Ethics and Information Technology 18 (3), 2016

Ita Purnama Sari, Syarifuddin Syarifuddin,(2022). Evaluasi Penggunaan Teknologi Dalam Meningkatkan Mutu Pembelajaran Madrasah Ibtidaiyah Di Kota BengkuluAl-Khair Journal: Management, Education, And Law, 2(2), 59-66.

Julia M. MacAllister, The Doxing Dilemma: Seeking a Remedy for the Malicious Publication of Personal Information, Fordham L.aw Review Volume 85, 2017

Khairiah, K., Hidayat, M. N., Kurnia, I., Harmaida, M., Rusydi, I., & Warto, W. (2021). MUTU KINERJA TENAGA PENDIDIK (GURU) DALAM MANAJEMEN PENDIDIKAN ERA PANDEMIC COVID-19. Al-Khair Journal: Management, Education, And Law, 1(1), 20-29.

Pedro Anguita R, "Freedom of Expression in Social Networks and Doxing" The Handbook of Communication Rights, Law, and Ethics, 2021

Roney Simon M, S. Aghili, & Dale L, "A Study of Doxing, its Security Implications and Mitigation Strategies for Organizations", Master of Information Systems Security Management (MISSM) and Master of Information Systems Assurance Management (MISAM) Project Reports (Concordia University of Edmonton), 2014

Samuel D. Warren dan Louis D. Brandeis, "The Right to Privacy," Harvard Law Rev, vol. IV, no. 5, hlm. 193–220, 1890

Jogja Tribun News, "Cemburu Mantan Kekasih Punya Pacar Baru, Pria di Aceh Ini Sebar Foto Syur, Akhirnya Ditangkap Polisi." https://jogja.tribunnews.com/2021/04/21/cemburu-mantan-kekasih-punya-pacar-baru-pria-di-aceh-ini-sebar-foto-syur-akhirnya-ditangkap-polisi?page=2

CNN Indonesia, "Pembocor Data Pribadi Denny Siregar Divonis 8 Bulan Penjara" https://www.cnnindonesia.com/nasional/20210303175401-12-613324/pembocor-data-pribadi-denny-siregar-divonis-8-bulan-penjara.

Undang-Undang Dasar Negara Republik Indonesia Tahun 1945

Undang-Undang Nomor 19 Tahun 2016 tentang Perubahan atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE)