

# **BAB I**

## **PENDAHULUAN**

### **A. Latar Belakang**

Data pribadi merupakan data yang dimiliki oleh seseorang, didalamnya berisi informasi penting mengenai identitas seseorang. Umumnya di dalam data pribadi terdapat informasi faktual mengenai identitas seseorang yang sifatnya sensitif dan privasi. Pada hakikatnya data pribadi melekat pada setiap orang. Data pribadi menjadi suatu sumber informasi mengenai individu serta dapat membedakan karakteristik antar individu satu dengan individu lainnya.<sup>1</sup> Karena sifatnya yang privasi maka sangat penting untuk menjaga kerahasiaan dalam penggunaan data pribadi juga perlunya pembatasan terhadap akses pada data pribadi.

Dasar hukum terkait pentingnya perlindungan data pribadi di Indonesia tertuang dalam Pasal 28G Undang-Undang Dasar Negara Republik Indonesia Tahun 1945 yang didalamnya menyatakan: “Setiap orang berhak atas perlindungan diri pribadi, keluarga, kehormatan, dan harta benda dibawah kekuasaannya, serta berhak atas rasa aman dan perlindungan dari ancaman ketakutan untuk berbuat atau tidak berbuat sesuatu yang merupakan hak asasi”. Dalam pasal tersebut menjelaskan begitu pentingnya adanya aturan perundang-undangan sebagai payung hukum untuk melindungi data pribadi.

Di Indonesia saat ini mengenai data pribadi sendiri telah diatur dalam Undang-Undang Republik Indonesia Nomor 27 Tahun 2022 tentang

---

<sup>1</sup> Rosadi, Shinta Dewi, 2015, *Cyber Law: Aspek Data Privasi Menurut Hukum Internasional, Regional, dan Nasional*, Cetakan 1, PT Refika Aditama, Bandung, hlm. 30.

Perlindungan Data Pribadi (selanjutnya disebut Undang-Undang PDP) yang mulai diberlakukan pada 17 oktober 2022. Undang-undang ini dibuat sebagai bentuk dari upaya pemerintah dalam melindungi masyarakat dari penyalahgunaan data pribadi dan rangkaian lainnya dalam pemrosesan data pribadi untuk menjamin hak konstitusional subjek data pribadi. Dimana pada Pasal 1 butir 1 disebutkan: “Data Pribadi adalah Data tentang orang perseorangan yang teridentifikasi atau dapat diidentifikasi secara tersendiri atau kombinasi dengan informasi lainnya baik secara langsung maupun tidak langsung melalui sistem elektronik atau non elektronik”. Data pribadi terbagi menjadi beberapa jenis diantaranya yang sifatnya umum dapat berupa nama, alamat, agama, pekerjaan dan lainnya. Sedangkan data pribadi yang sifatnya rahasia diantaranya nomor NIK, informasi rekening bank, sandi kartu atm, *password* sosial media dan sebagainya.

Pesatnya perkembangan teknologi informasi saat ini memengaruhi berbagai aspek terutama dalam aspek penggunaan dan pengelolaan data dalam hal ini yaitu data pribadi yang hampir seluruhnya dilakukan berbasis digital. Penggunaan data pribadi saat ini tidak hanya digunakan dalam penggunaan *website*, aplikasi, media sosial namun dalam situs atau aplikasi milik pemerintah. Baik dalam urusan penting maupun sederhana sekalipun.

Rendahnya kesadaran masyarakat terhadap pentingnya kerahasiaan data pribadi menjadikan munculnya berbagai macam kejahatan siber yang berkaitan dengan data pribadi, salah-satu jenis kejahatan yang menyerang data pribadinyaitu *Doxing*. *Doxing* sendiri merupakan tindak pidana yang sangat meresahkan bagi masyarakat karena menyerang data pribadi seseorang yang

kemudian disebarluaskan tanpa izin pemilik data pribadi yang dapat merugikan si pemilik data pribadi yang karena disalahgunakan.

Di Indonesia *Doxing* sudah banyak terjadi, tidak hanya menyerang tokoh-tokoh publik atau orang-orang dengan profesi tertentu namun seiring perkembangan teknologi informasi semua orang dapat menjadi korban *Doxing*. berdasarkan data dari SAFEnet dalam kurun waktu 2017-2020 terdapat 13 kasus *Doxing* yang dialami oleh jurnalis dan 10 kasus juga menimpa aktifis dan warga.<sup>2</sup> beberapa contoh *Doxing* yang terjadi di Indonesia yaitu pada tahun 2020 seorang jurnalis Liputan6.com Cakrayuni Nurlaman yang mengalami serangan *Doxing* Setelah menulis artikel Cek Fakta Politikus PDIP Arteria Dahlan kemudian kasus Bjorka yang membocorkan data pribadi beberapa pejabat negara salah satunya Johnny G Plate, Puan Maharani dan Erick Thohir, kasus pada tahun salah satu anggota BEM UNY yang mengalami *Doxing* yang kemudian menjadi korban hoaks terkait pelecehan seksual terhadap sesama mahasiswa

Terakhir kasus *Doxing* yang sampai ke pengadilan yaitu pada tahun 2020 kasus Denny Siregar seorang *influencer* politik yang informasi pribadinya bocor lewat akun *twitter* @opposite6891 yang kemudian pelaku dijerat dengan Pasal 46 Ayat (2) Jo Pasal 30 Ayat (2) Undang-Undang Nomor 19 Tahun 2016 Tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik (UU ITE) dimana hakim menjatuhkan sanksi pidana penjara selama 8 bulan dan denda sebesar 2 juta rupiah.

---

<sup>2</sup>Abu Hasan Banimal, dkk. 2020, <https://safenet.or.id/id/2020/12/riset-peningkatan-serangan-doxing-dan-tantangan-perlindungannya-di-indonesia/>, Diakses 14 Februari 2024.

Kasus *Doxing* dapat terjadi dikarenakan, mudahnya mengakses identitas pribadi milik seseorang, baik dari informasi yang dicantumkan pada media sosial sampai melacak lokasi seseorang menggunakan alamat *IP (Internet Protocol Address)*.<sup>3</sup> *Doxing* menjadikan rasa tidak nyaman bagi seseorang dalam menggunakan internet karena adanya rasa takut melakukan kesalahan yang mengakibatkan terbongkarnya informasi pribadi ketika menggunakan media sosial. *Doxing* yang banyak terjadi dan sering ditemukan yaitu berupa postingan foto atau video yang berisi informasi pribadi dengan tujuan untuk menggiring atau membangkitkan opini publik. *Doxing* dapat mengancam privasi seseorang terutama pada saat ini dimana perkembangan teknologi sangat pesat dan penyebaran data di internet yang cepat menyebabkan data menjadi rentan terhadap penyalahgunaan sehingga dapat merugikan orang lain.

Sebagai negara yang baru mengesahkan undang-undang mengenai perlindungan data pribadi, salah satu tindak pidana yang diatur dalam undang-undang PDP yaitu terhadap kejahatan siber yang berkaitan dengan data pribadi yang belakangan banyak terjadi yaitu *Doxing*. Indonesia melarang tindakan *Doxing* sebagai mana yang telah dinyatakan pada Pasal 65 Ayat (2) “Setiap Orang dilarang secara melawan hukum mengungkapkan Data Pribadi yang bukan miliknya”. Ancaman pidana yang dijatuhkan terhadap pelaku *Doxing* cukup berat, sebagaimana diatur dalam Pasal 67 Ayat (2) Undang-Undang PDP, yang menyebutkan: “Setiap Orang yang dengan sengaja dan melawan hukum mengungkapkan Data Pribadi yang bukan miliknya sebagaimana yang

---

<sup>3</sup> Cindi Novita Putri, 2023, *Kajian Kriminologi Kejahatan Penyebaran Data Pribadi (Doxing) Melalui Media Sosial*, Skripsi, Universitas Lampung, Bandar Lampung, hlm. 3.

dimaksud dalam Pasal 65 Ayat (2) dipidana dengan penjara paling lama 4 (empat) tahun dan/atau pidana denda paling banyak Rp5.000.000.000,00 (lima milyar rupiah)”.

Indonesia dapat dikatakan cukup tertinggal dalam hal perlindungan data pribadi terhadap warga negaranya. Hal ini dapat dilihat diantara negara-negara tetangga dalam lingkup ASEAN seperti Malaysia, Thailand, Filipina dan Singapura yang telah dulu memiliki peraturan perundang-undangan terkait perlindungan data pribadi untuk warga negaranya. Sebelum Indonesia memiliki peraturan perundang-undangan mengenai perlindungan data pribadi

Negara Malaysia menjadi negara pertama di ASEAN yang lebih dulu memiliki peraturan perundang-undangan tentang perlindungan data pribadi. Di Malaysia undang-undang mengenai data pribadi lebih dikenal dengan nama *Personal Data Protection Act 2010 Malaysia* (PDPA Malaysia) yang mulai diberlakukan sejak tahun 2013. Dalam undang-undang ini secara tegas memberikan jaminan perlindungan mengenai hak privasi kepada warga negaranya. Dalam PDPA Malaysia mengatur secara detail terkait prinsip-prinsip dalam perlindungan data pribadi, hak hak yang dimiliki pemilik data, tata cara pemindahtanganan data, dan kewajiban terhadap pihak yang melakukan penyimpanan data.<sup>4</sup> Dalam PDPA Malaysia terdapat larangan mengenai kejahatan *Doxing* yang mana dalam peraturan tersebut melarang seseorang dengan sengaja atau sembarangan tanpa izin pemilik data mengumpulkan dan mengungkapkan data pribadi milik orang lain. Sanksi yang

---

<sup>4</sup> Muhammad Saiful Rizal, 2019, Perbandingan Perlindungan Data Pribadi Indonesia dan Malaysia, *Jurnal Cakrawala Hukum*, Volume X, Nomor 2, hlm. 223.

dikenakan pada pelanggar yang melanggar ketentuan PDPA Malaysia yaitu sanksi pidana berupa penjara dan denda.

Negara lainnya di ASEAN yang juga lebih dulu memiliki undang-undang mengenai perlindungan data pribadi yaitu Singapura. Undang-undang perlindungan data pribadi Singapura dikenal dengan nama *Personal Data Protection Act 2012* (PDPA Singapura) merupakan sistem untuk perlindungan terhadap hak atas data pribadi bagi warga negara di Singapura yang mulai diberlakukan secara penuh pada tahun 2014. Mengenai kejahatan *Doxing*, dalam PDPA Singapura seseorang dilarang mengungkapkan data pribadi baik yang dikuasai oleh individu, organisasi atau badan hukum. Jika seseorang terbukti bersalah melanggar ketentuan dalam PDPA Singapura maka akan diancam dengan sanksi pidana berupa penjara dan/atau pidana.

Negara selanjutnya yang memiliki Peraturan terkait perlindungan data pribadi yaitu Thailand. Undang-undang perlindungan data pribadi Thailand atau yang dikenal dengan nama *Personal Data Protection Act 2019* (PDPA Thailand) yang mulai berlaku penuh pada Juni 2022. Dalam PDPA milik negara Thailand terdapat larangan mengenai pengumpulan, penggunaan, pengungkapan data pribadi seseorang tanpa persetujuan pemilik data pribadi kecuali dalam hal hal-tertentu yang diatur dalam undang-undang. Di dalam PDPA Thailand terdapat aspek-aspek yang mengatur mengenai siapa saja yang boleh mengungkapkan mengenai data pribadi dan larangan mengungkapkan informasi pribadi dengan tujuan selain yang diatur dalam undang-undang. Sanksi yang dapat dikenakan bagi yang melanggar ketentuan dalam PDPA Thailand adalah pidana penjara dan/atau denda.

Adanya peraturan yang sama oleh keempat negara mengenai perlindungan data pribadi menunjukkan pentingnya perlindungan data pribadi dalam era perkembangan teknologi informasi sebagai bentuk pemenuhan hak privasi dan keamanan data bagi warga negara.

Berdasarkan latar belakang di atas, maka penulis tertarik untuk mengkaji mengenai *Doxing* sebagai tindak pidana serta penjatuhan pidana di Indonesia, Malaysia, Singapura dan Thailand dengan judul “**STUDI PERBANDINGAN TENTANG *DOXING* DI INDONESIA, MALAYSIA, SINGAPURA, DAN THAILAND**”.

## **B. Rumusan Masalah**

Adapun yang menjadi permasalahan yang akan dibahas dalam penelitian ini adalah;

1. Bagaimanakah pengaturan mengenai unsur delik dalam tindak pidana *Doxing* di Indonesia, Malaysia, Singapura, dan Thailand?
2. Bagaimanakah pengaturan mengenai sistem sanksi dalam tindak pidana *Doxing* di Indonesia, Malaysia, Singapura, dan Thailand?

## **C. Tujuan Penelitian**

Sedangkan yang menjadi tujuan dalam penelitian ini adalah;

1. Menganalisis pengaturan mengenai unsur delik dalam tindak pidana *Doxing* di Indonesia, Malaysia, Singapura, dan Thailand.
2. Menganalisis pengaturan mengenai sistem sanksi dalam tindak pidana *Doxing* di Indonesia, Malaysia, Singapura, dan Thailand.

## D. Metode Penelitian

### 1. Jenis Penelitian

Jenis penelitian yang digunakan adalah penelitian hukum normatif. Penelitian hukum normatif merupakan penelitian hukum yang dilakukan melalui penelitian bahan pustaka maupun data sekunder yang menjadi dasar dalam penelitian yang dilakukan dengan mengadakan penelusuran pada peraturan-peraturan serta literatur-literatur berkaitan permasalahan yang diteliti.<sup>5</sup> Penelitian ini untuk menggambarkan norma-norma hukum sebagai data rujukan dalam pedoman bertingkah laku bagi kehidupan bermasyarakat. Penelitian yang dilakukan khususnya mengenai perbandingan hukum

### 2. Pendekatan

Pendekatan yang digunakan dalam penelitian ini yaitu Pendekatan perbandingan (*comparison approach*) dan pendekatan perundang-undangan (*statute approach*). Pendekatan perbandingan yaitu jenis pendekatan yang digunakan untuk membandingkan hukum antara satu negara dengan negara lainnya. Pendekatan perbandingan dalam penelitian ini dilakukan dengan cara membandingkan undang-undang di negara Indonesia, Malaysia, Singapura, dan Thailand. Dalam hal ini terkait dengan *Doxing*.

Pendekatan perundang-undang yaitu pendekatan yang dilakukan dengan cara menelaah regulasi dan peraturan perundang-undangan yang terkait dengan masalah hukum yang akan diteliti. Pendekatan perundang-

---

<sup>5</sup> Soerjono Soekanto, 2022, *Penelitian Hukum Normatif suatu (Suatu Tinjauan Singkat)*, Cetakan ke-21, PT RajaGrafindo Persada, Depok, hlm. 13.

undangan menjadi tema serta fokus utama dalam penelitian yaitu mengenai undang-undang terkait perlindungan data pribadi.<sup>6</sup>

### 3. Sumber Data

Data yang digunakan dalam penelitian ini adalah data sekunder. Data sekunder yaitu data yang didapat dari pihak lain secara tidak langsung dari subjek penelitiannya seperti melalui studi kepustakaan yang dilakukan dengan cara mencari relevansi antara teori yang diteliti dengan masalah penelitian.<sup>7</sup> Data sekunder yang digunakan dalam penelitian ini meliputi:

a. Bahan hukum primer yaitu bahan-bahan hukum yang bersifat mengikat.<sup>8</sup> Bahan hukum primer yang digunakan diantaranya:

- 1) Undang-Undang Republik Indonesia Nomor 1 Tahun 1946 tentang Peraturan Hukum Pidana (KUHP)
- 2) Undang-Undang Republik Indonesia Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi dan Undang-Undang Nomor 19 Tahun 2016 tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik;
- 3) *Personal Data Protection Act 2010* Malaysia;
- 4) *Personal Data Protection Act 2012* Singapura dan *Protection from Harassment Act 2014* dan;
- 5) *Personal Data Protection Act 2019* Thailand.

b. Bahan hukum sekunder yaitu bahan hukum yang menjelaskan mengenai bahan hukum primer.<sup>9</sup> Bahan hukum sekunder yang

---

<sup>6</sup> Peter Mahmud Marzuki, 2011, *Penelitian Hukum*, Kencana Prenada Media Group, Jakarta, hlm. 24.

<sup>7</sup> *Ibid.*

<sup>8</sup> *Ibid.*

digunakan diantaranya, buku-buku yang berkaitan dengan perlindungan data pribadi dan hasil-hasil penelitian/karya ilmiah mengenai perlindungan data pribadi dan *Doxing*.

- c. Bahan hukum tersier yaitu bahan hukum yang memberikan penjelasan yang terdapat dalam bahan hukum primer serta sekunder<sup>10</sup>. Bahan hukum tersier yang digunakan yaitu abstrak perundang-undangan, ensiklopedia hukum, bibliografi hukum, kamus hukum, indeks majalah hukum dan sebagainya.

#### 4. Teknik Pengumpulan Data

Teknik pengumpulan data yang digunakan adalah studi dokumen atau studi dokumentasi. Studi dokumen yaitu teknik pengumpulan data dengan memperoleh informasi atau data yang relevan dengan masalah dalam objek penelitian yang dibuat dalam karya tulis ilmiah.<sup>11</sup>

Studi dokumen yang digunakan dalam penelitian ini yaitu membandingkan peraturan perundang-undangan yang berlaku di Indonesia, Malaysia, Singapura, dan Thailand.

#### 5. Teknik Analisis Data

Teknik analisis data yang digunakan peneliti yaitu data kualitatif. Data kualitatif yaitu penelitian yang dilakukan dengan tujuan memahami sebuah fenomena dalam hal konteks sosial yang terjadi secara alamiah

---

<sup>9</sup> *Ibid.*

<sup>10</sup> *Ibid.*

<sup>11</sup>Harris Herdiansyah, 2010, *Metode Penelitian Kualitatif Untuk Ilmu-Ilmu Sosial*, Salemba Humanika, Jakarta, hlm. 143.

dengan mengutamakan proses interaksi secara mendalam antara peneliti dengan fenomena yang sedang diteliti.<sup>12</sup>

---

<sup>12</sup> *Ibid.*, hlm. 17.

## **BAB II TINJAUAN PUSTAKA**

### **A. Pidana dan Pemidanaan**

#### **1. Teori-Teori Pemidanaan**

Pidana merujuk pada konsep dalam sistem hukum yang didalamnya mengatur mengenai tindakan-tindakan yang dianggap melanggar hukum serta dikenakan sanksi oleh negara. Pidana melibatkan prosedur hukum dan aturan-aturan yang digunakan untuk menentukan jenis sanksi apa yang dapat dikenakan berdasarkan jenis pelanggaran yang telah dilakukan.

Sedangkan pemidanaan yaitu upaya untuk menyadarkan terpidana untuk menyesali perbuatannya dan mengembalikannya menjadi warga masyarakat yang baik, taat pada hukum, menjunjung tinggi nilai moral, sosia dan agama sehingga kehidupan masyarakat yang aman tertib dan damai dapat tercapai.<sup>13</sup>

Dalam pemidanaan terdapat tujuan pemidanaan yang memiliki beberapa teori yang berhubungan erat dengan subjektif *strafrecth* sebagai hak atau wewenang untuk menjatuhkan pidana. Dalam perkembangan hukum pidana, pada dasarnya terdapat 3 teori dalam tujuan pemidanaan diantaranya:

##### 1) Teori absolut

Teori absolut atau yang sering juga disebut teori pembalasan.

Teori ini memandang bahwa penjatuhan pidana semata-mata karena

---

<sup>13</sup> Gatot Supramono, 2000, *Hukum Acara Pengadilan Anak*, Djambatan, Jakarta, hlm. 200.

tindak kejahatan atau tindak pidana yang telah dilakukan oleh seseorang<sup>14</sup>. Dalam teori ini dijatuhkannya pidana sebagai bentuk pembalasan terhadap pelaku tindak pidana.

## 2) Teori Relatif

Teori relatif atau teori tujuan memandang bahwa pidana bukan hanya sekedar sebagai bentuk pembalasan terhadap pelaku kejahatan namun terdapat tujuan-tujuan yang bermanfaat. Dalam teori relatif dasar dari pemidanaan adalah yaitu penegakan terhadap ketertiban dalam masyarakat dan tujuan pemidanaan yaitu untuk mencegah terjadinya kejahatan.

## 3) Teori Gabungan

Teori ini terbentuk akibat dari penggabungan antara teori absolut dan teori relatif. Teori ini berpendapat bahwa pidana tidak hanya sebagai pembalasan namun juga sebagai pencegah agar tindak pidana yang sama tidak lagi terulang dimasa depan sehingga terdapat keseimbangan antara penjatuhan pidana dengan kejahatan yang sudah diperbuat. Dengan adanya hal ini diharapkan pemidanaan dapat memberikan kepuasan kepada hakim, pelaku kejahatan serta kepada masyarakat.

Dalam pemidanaan terdapat hal yang perlu diperhatikan yakni terkait delik formil dan delik materil. Pada delik formil adalah perbuatan pidana yang tidak delik dianggap telah selesai dengan hukuman oleh undang-undang, yang mana pada perbuatan pidana yang dilarang tidak

---

<sup>14</sup> Niniek Suparni, 2007, *Eksistensi Pidana Denda Dalam Sistem Pemidanaan*, Sinar Garafika, Jakarta, hlm. 16.

memerlukan akibat yang ditimbulkan untuk dilarang oleh undang-undang. Sedangkan pada delik materiil adalah delik yang dianggap telah selesai dengan ditimbulkannya akibat yang dilarang dan diancam oleh undang-undang, dimana dalam perbuatan pidana yang dilarang memerlukan akibat yang timbul untuk dilarang oleh undang-undang.<sup>15</sup>

## 2. Sanksi Pidana

Dalam hukum pidana dikenal beberapa jenis perumusan sanksi pidana yaitu pertama sistem perumusan tunggal/imperatif yakni sistem perumusan satu jenis pidana yang bersangkutan. Dapat berupa pidana penjara saja, pidana kurungan saja atau pidana denda saja. Kedua sistem perumusan alternatif, yaitu dimana pidana penjara dirumuskan secara alternative dengan pidana lainnya berdasarkan urutan sanksi pidana dari yang terberat sampai yang teringan. Ketiga sistem perumusan kumulatif yang memiliki ciri khas menggunakan kata “dan” sebagai redaksi kata penghubung antar dua jenis pidana seperti “pidana penjara dan denda”. Keempat sistem perumusan alternative kumulatif atau sering juga disebut sistem perumusan gabungan/campuran, yang mana didalamnya mengandung dimensi kumulatif, alternatif dan tunggal didalamnya.<sup>16</sup>

Dalam sistem pemidanaan secara garis besar mencakup 3 hal pokok yaitu jenis pidana (*strafsoort*), lamanya ancaman pidana (*strafmaat*) dan pelaksanaan pidana (*strafmodus*).

---

<sup>15</sup> P.A.F Lamintang, *Dasar-Dasar Hukum Pidana* Indonesia, Cetakan ke-2, Sinar Baru, Bandung, hlm. 200

<sup>16</sup> Wisnu Murtopo Nur Muhammad, 2023, *Rekonstruksi Strafsoort dalam Hukum Pidana Indonesia*, Penerbit Adab, Indramayu, hlm. 24

a. Jenis Pidana (*strafsoort*)

Dalam ketentuan pada Pasal 10 KUHP terdapat jenis-jenis pidana diantaranya: pidana pokok berupa: pidana mati; pidana penjara; pidana kurungan; pidana denda; pidana tutupan. pidana tambahan berupa: pencabutan hak-hak tertentu; perampasan barang tertentu; Pengumuman putusan hakim.

Dalam KUHP baru jenis jenis pidana terdapat pada pasal 64 KUHP Baru. Dimana pidana terdiri dari: pidana pokok, pidana tambahan dan pidana yang bersifat khusus untuk Tindak pidana tertentu yang di tentukan dalam Undang-Undang. Dalam pidana pokok terdiri atas: pidana penjara; pidana tutupan; pidana pengawasan; pidana denda dan pidana kerja sosial, pada pidana tambahan tersiri atas: Pencabutan hak-hak tertentu; perampasan barang-barang tertentu dan/atau tagihan; Pengumuman putusan hakim; Pembayaran ganti rugi; pencabutan izin tertentu; dan pemenuhan kewajiban adat setempat.

b. Lamanya Ancaman Pidana (*Strafmaat*)

Pada penjatuhan pidana pokok seringkali diancam secara alternatif pada tindak pidana yang sama. Dalam menentukan lamanya ancaman pidana terdapat 2 alternatif sistem yaitu:<sup>17</sup>

- 1) Sistem pendekatan absolut yaitu untuk setiap tindak pidana ditetapkan bobot atau kausalitasnya tersendiri dengan menetapkan

---

<sup>17</sup> *Ibid.*

ancaman pidana maksimum atau dapat juga ancaman pidana minimum untuk setiap tindak pidana.

- 2) Sistem pendekatan relatif yaitu untuk setiap tindak pidana tidak ditetapkan maksimum pidananya akan tetapi dilakukan secara relatif dengan melakukan penggolongan tindak pidana dalam beberapa tingkatan sekaligus menetapkan maksimum pidana untuk setiap kelompok pidana tersebut.

Di dalam KUHP Indonesia hanya mengenal maksimum umum dan maksimum khusus minimum umum. Maksimum bagi pidana penjara adalah 15 tahun dan bagi pidana kurungan 1 tahun. Dan maksimum khusus dijelaskan pada tiap-tiap rumusan delik, sedangkan pidana denda tidak ada ketentuan maksimum khususnya.

c. Pelaksanaan Pidana (*Strafmodus*)

Dalam KUHP Indonesia belum mengenal terkait pedoman pembedaan sehingga hakim dalam memutus perkara diberi kebebasan memilih jenis pidana yang dikenhdaki sesuai dengan sistem alternatif dalam pengancaman dalam undang-undang. Hakim juga dapat menentukan sendiri berat ringannya pidana yang akan dijatuhkan, karena hanya ditentukan mengenai maksimum dan minimum pidana. Dalam KUHP mengatur empat bentuk pengenaan pidana yaitu bentuk pengenaan pidana tunggal, alternatif, kumulatif dan kombinasi.<sup>18</sup>

---

<sup>18</sup> Joko Sriwidodo, 2019, *Kajian Hukum Pidana Indonesia (Teori dan Praktek)*, Kepel Press, Yogyakarta Cetakan 1, hlm. 92

## B. *Doxing*

### 1. Pengertian *Doxing*

*Doxing* atau sering disebut “*doxxing*” berasal dari kata *doc* yang merupakan akronim dari kata *dropping document*, yang artinya dokumen yang diambil dan dibagikan.<sup>19</sup> Awalnya kata *Doxing* merujuk pada perbuatan pengumpulan, pengungkapan, dan/atau pelepasan data pribadi milik seseorang atau suatu kelompok di dunia internet. Istilah ini sering digunakan di dunia *hacker*, pertama kali digunakan pada tahun 1990an dalam konteks *hacker* yang melakukan *Doxing* pada *hacker* saingannya.<sup>20</sup>

*Doxing* merupakan suatu penindasan di dunia maya dimana informasi pribadi orang lain dicari dan disebarluaskan sehingga melanggar privasi pemilik data pribadi.<sup>21</sup> *Doxing* dapat diartikan sebagai sebagai suatu tindakan yang dilakukan berbasis internet mengetahui serta menyebarkan informasi pribadi milik orang lain secara publik (termasuk didalamnya data pribadi) terhadap seseorang atau organisasi.<sup>22</sup> Menurut David M. Douglas. Menyatakan bahwa *Doxing* merupakan tindakan yang secara sengaja mengungkapkan data digital seseorang dengan tujuan untuk mempermalukan, mengancam menghukum atau

---

<sup>19</sup> Angga Prastiyo, 2018, Pemaknaan Objektifikasi Perempuan sebagai Hasil *Doxing* pada Akun Instagram Undip Cantik, Tesis, Program Pascasarjana, Fakultas Ilmu Sosial dan Politik Universitas Diponegoro, Semarang, hlm. 3.

<sup>20</sup> Teguh Cahya Yudiana dkk, 2022, The Urgency of *Doxing* on Social Media Regulation and Implementation of Right to Be Forgotten on Related Content for the Optimization of Data Privacy Protection in Indonesia, *Padjajaran Journal of Law*, Volume IX, Nomor 1, hlm. 27.

<sup>21</sup> Chen M, dkk, 2019, *Doxing: What adolescents look for and their intentions*, *International Journal of Environmental Research and Public Health*, Volume XVI, Nomor 2, hlm. 218.

<sup>22</sup> Dewi Septiani, 2021, *Apa itu Doxxing dan Dampaknya pada Privasi Online*, 15 oktober 2023 (<https://bpptik.kominfo.go.id/2021/06/21/8958/apa-itu-doxxing-dan-dampaknya-pada-privasi-online/>).

mengintimidasi seseorang sebagai bentuk protes atau mengungkapkan tindakan yang dilakukan oleh orang lain.<sup>23</sup>

*Doxing* adalah tindakan mengumpulkan dan mengungkapkan informasi data pribadi milik orang lain secara tidak sah atau tanpa izin dari orang tersebut. Informasi yang diungkapkan pada *Doxing* tidak hanya terbatas pada nama asli, alamat tempat tinggal atau kantor, foto pribadi, *e-mail* namun juga informasi lainnya yang sifatnya rahasia. Praktik *Doxing* dilakukan dengan tujuan untuk merugikan, mengintimidasi atau melanggar privasi orang yang dijadikan target.

Para pelaku *Doxing* biasanya menyerang targetnya dengan bersembunyi dibalik akun-akun anonim palsu tanpa diketahui dengan jelas identitasnya yang kemudian akun tersebut dibiarkan begitu saja. Perbuatan *Doxing* merupakan pengumuman ke publik yang dilakukan dengan sengaja melalui media internet mengenai informasi data pribadi seseorang oleh pihak lain tanpa persetujuan pemilik data itu sendiri yang tujuannya untuk mempermalukan, mengancam dan mengintimidasi atau menghukum individu yang diidentifikasi.

## 2. Bentuk-bentuk *Doxing*

Secara umum *Doxing* dapat dikategorikan menjadi beberapa bagian. Beberapa kategori mengenai *Doxing* diantaranya; Pertama yaitu *Deanonymizing*, merupakan tindakan *Doxing* dengan mempublikasikan informasi mengenai identitas pribadi seseorang/kelompok yang identitasnya tidak diketahui oleh publik dengan nama samara (anonim).

---

<sup>23</sup> David M Douglas, 2016, *Doxing: a conceptual analysis*, *Ethics and Information Technology*, Volume XVII, hlm. 2.

*Deanonymizing* sangat mempengaruhi kerahasiaan identitas seseorang serta dapat mengintimidasi bagi seseorang atau sekelompok orang yang tidak ingin identitasnya tidak diketahui oleh publik sebagai bentuk kebebasan berekspresi.

Kedua *Targeting*, merupakan tindakan *Doxing* dengan mempublikasikan informasi tentang keberadaan fisik seseorang, artinya tindakan ini mampu melacak hingga menemukan lokasi tempat hingga keberadaannya dalam waktu nyata. *Targeting* dapat meningkatkan kemungkinan korbannya dapat ditemukan secara fisik serta diketahuinya tempat tinggal. Hal ini dapat membahayakan karena seseorang dalam kondisi terancam secara fisik seperti serangan. Tindakan ini dilakukan setelah dilakukannya *Deanonymizing*.

Ketiga *Delegitimizing*, merupakan tindakan mempublikasikan informasi pribadi milik seseorang/kelompok dengan tujuan untuk menjatuhkan, merusak kredibilitas atau reputasi.<sup>24</sup> Tujuan dilakukannya *Delegitimizing* yaitu untuk mempermalukan, menjatuhkan, dan menghina korbannya menggunakan data pribadinya yang mudah disalahpahami atau informasi yang memang rahasia. *Doxing* dengan bentuk ini melibatkan pengungkapan dengan bukti yang menyebabkan targetnya kehilangan kredibilitasnya.

---

<sup>24</sup> Jeane Nelte Saly dkk, 2022, Pelindungan Data Pribadi dalam Tindakan *Doxing* Berdasarkan Undang-Undang Nomor 27 Tahun 2022, *Jurnal Kewarganegaraan*, Volume VII, Nomor 2, Desember 2022, hlm. 1711.

Terdapat beberapa klasifikasi dari tujuan dilakukannya *Doxing* antara lain<sup>25</sup>:

- 1) *Doxing* dengan tujuan jahat, dimana dalam hal ini seseorang melakukan *Doxing* kepada orang lain agar menimbulkan kesusahan, kerugian atau pun rasa malu dengan dimotivasi rasa balas dendam, amarah atau sekedar keinginan untuk melecehkan. Dilakukannya *Doxing* dapat menimbulkan kerugian yang lebih besar dibandingkan pelecahan secara langsung.
- 2) *Doxing* dengan tujuan politik, tujuan dilakukannya *Doxing* dalam hal ini sebagai bentuk transparansi, dimana untuk mengungkapkan suatu hal yang dianggap tidak adil untuk mengungkapkan informasi yang layak diungkapkan/diberitakan demi kepentingan publik.
- 3) *Doxing* dengan tujuan pengaturan mandiri, dalam hal ini *Doxing* dimanfaatkan untuk mengungkapkan identitas orang lain untuk mencari dukungan terhadap orang yang kehilangan dukungan dari rekan-rekannya karena berbagai alasan.

Pelaku *Doxing* biasanya mencari informasi mengenai data pribadi milik orang lain melalui berbagai platform online seperti media sosial atau direktori publik. Informasi yang ditemukan kemudian digunakan untuk nerugikan orang lain seperti penyebaran informasi pribadi secara massal atau penipuan. *Doxing* termasuk dalam kategori cyber bullying yang seringkali berkaitan dengan penguntitan atau *stalking*, dan informasi yang disebarakan melalui *doxing* sering kali digunakan dalam

---

<sup>25</sup> Julia MacAllister, 2017, *The Doxing Dilemma: Seeking A Remedy for the Malicious Publication of Personal Information*, *Fordham Law Review*, Vol. 85, Issue 5, hlm. 2457.

konteks yang dapat menimbulkan ketakutan dan ketidaknyamanan, sehingga meresahkan pada individu yang menjadi target. *Doxing* dapat berdampak serius pada kehidupan seseorang karena mengancam resiko keamanan, pelecehan dan pencemaran nama baik. *Doxing* juga dapat menimbulkan rasa takut terhadap korban karena identitas, pekerjaan dan domisilinya disebar atau dipublikasikan di media sosial.<sup>26</sup>

---

<sup>26</sup> Halif, dkk, 2023, *Regulating Doxing and Personal Data Dissemination in Indonesia*, *Jurnal Kajian Pembaruan Hukum* Volume III, Issue 1, hlm. 77.