

**PERLINDUNGAN HUKUM BAGI KORBAN *DOXING* SEBAGAI  
PENCEGAHAN TERJADINYA KEBOCORAN DATA PRIBADI**

**Skripsi**

Diajukan Sebagai Salah Satu Persyaratan untuk memperoleh  
Gelar Sarjana Strata Satu (S-1) Ilmu Hukum  
Program Kekhususan Hukum Pidana



Diajukan oleh :

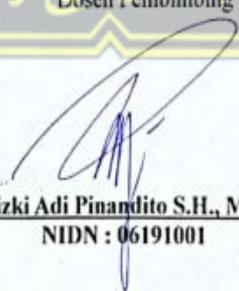
Sherliana Ika Pratiwi

NIM : 30302100310

**PROGRAM STUDI (S.1) ILMU HUKUM  
FAKULTAS HUKUM  
UNIVERSITAS ISLAM SULTAN AGUNG (UNISSULA)  
SEMARANG  
2025**

**HALAMAN PERSETUJUAN PEMBIMBING**  
**PERLINDUNGAN HUKUM BAGI KORBAN *DOXING* SEBAGAI**  
**PENCEGAHAN TERJADINYA KEBOCORAN DATA PRIBADI**



  
**Rizki Adi Pinandito S.H., M.H**  
**NIDN : 06191001**

HALAMAN PENGESAHAN

PERLINDUNGAN HUKUM BAGI KORBAN *DOXING* SEBAGAI  
PENCEGAHAN TERJADINYA KEBOCORAN DATA PRIBADI

Dipersiapkan dan disusun oleh :

Sherliana Ika Pratiwi

NIM : 30302100310

Telah dipertahankan di depan Tim Penguji

Pada tanggal 22 Mei 2025

Dan dinyatakan telah memenuhi syarat dan lulus

Tim Penguji

Ketua,

Dr. Muhammad Gazis, S.H., M.H

NIDN: 060128601

Anggota,

Anggota,

Dr. Lathifah Hanim, S.H., M.Hum., M.Kn.

NIDN: 0621027401

Rizki Adi Pinandito, S.H., M.H.

NIDN: 06191001

Mengetahui,

Dekan Fakultas Hukum UNISSULA



Dr. H. Jawade Hafidz, S.H., M.H

NIDN : 06-2004-6701

## MOTTO DAN PERSEMBAHAN

### MOTTO

- ❖ *I will no longer go full throttle. Instead, I will walk slowly enjoying every steps of the journey. At my own pace, following my own rhythms. It's not GOD doesn't know how sad you are, but GOD knows you are strong.*  
– Mark Lee
- ❖ *I think listening is more important than continuing to talk. It would be better if we listened to the concerns of those around us, and I would find it worthwhile to do so.*  
– Mark Lee
- ❖ *Thinking that everything will come naturally without trying is the worst mindset for mankind. -Sherly*

### Skripsi ini saya persembahkan kepada :

- ❖ Allah SWT sebagai bentuk terimakasih atas ilmu yang telah diberikan sehingga penulis dapat menyelesaikan penyusunan ini tanpa halangan yang berarti.
- ❖ Kepada orangtua saya Bapak Medi dan Ibu Fadrizul yang saya sayangi, karena telah memberikan dukungan dalam bentuk sarana maupun prasarana selama penulis menimba ilmu.
- ❖ Keluarga besar penulis yang tidak dapat penulis sebutkan satu per satu yang senantiasa mendukung.
- ❖ Kepada diri saya sendiri Sherliana Ika Pratiwi, terimakasih karena sudah berusaha dan bertahan sejauh ini sehingga dapat mencapai titik ini.
- ❖ Almamater Fakultas Hukum Universitas Islam Sutan Agung.

## PERNYATAAN KEASLIAN TESIS

Saya yang bertanda tangan di bawah ini:

Nama : Sherliana Ika Pratiwi

NIM : 30302100310

Program Studi : S-1 Ilmu Hukum

Fakultas : Hukum

Menyatakan dengan sebenarnya bahwa skripsi saya dengan judul "PERLINDUNGAN HUKUM BAGI KORBAN *DOXING* SEBAGAI PENCEGAHAN TERJADINYA KEBOCORAN DATA PRIBADI" benar – benar merupakan hasil karya tulisan saya sendiri, bebas dari peniruan hasil karya orang lain. Kutipan pendapat dan tulisan orang lain yang disertakan dalam skripsi sudah sesuai dengan cara – cara penulisan karya ilmiah yang berlaku.

Apabila dikemudian hari terbukti atau didalilkan dan dapat dibuktikan dalam skripsi ini terkandung ciri – ciri plagiat dan bentuk – bentuk peniruan lain yang dianggap melanggar peraturan, maka saya bersedia menerima sanksi atas perbuatan tersebut.

Semarang, 2 April 2025

Yang Menyatakan



Sherliana Ika Pratiwi

NIM. 30302100310

## SURAT PERNYATAAN PERSETUJUAN PUBLIKASI

Saya yang bertanda tangan dibawah ini :

Nama : Sherliana Ika Pratiwi

NIM : 30302100310

Program Studi : S-1 Ilmu Hukum

Fakultas : Hukum

Dengan ini menyerahkan karya ilmiah berupa Skripsi dengan judul :

“PERLINDUNGAN HUKUM BAGI KORBAN *DOXXING* SEBAGAI  
PENCEGAHAN TERJADINYA KEBOCORAN DATA PRIBADI”

dan menyetujuinya menjadi hak milik Universitas Islam Sultan Agung serta memberikan Hak Bebas Royalti Non-eksklusif untuk disimpan, dialihmediakan, dikelola dalam pangkalan data, dan publikasinya di internet atau media lain untuk kepentingan akademis selama tetap mencantumkan nama penulis sebagai pemilik Hak Cipta.

Pernyataan ini saya buat dengan sungguh – sungguh. Apabila dikemudian hari terbukti ada pelanggaran Hak Cipta/Plagiarisme dalam karya ilmiah ini, maka segala bentuk tuntutan hukum yang timbul akan saya tanggung secara pribadi tanpa melibatkan pihak Universitas Islam Sultan Agung.

Semarang, 2 April 2025

Yang Menyatakan

The image shows a signature in black ink over a yellow and red stamp. The stamp contains the text 'UNIVERSITAS ISLAM SULTAN AGUNG' and 'METEOR TEMER' along with a QR code and the number '40AMX302770655'.

Sherliana Ika Pratiwi

NIM. 30302100310

## KATA PENGANTAR

Assalamualaikum. Wr. Wb

Puji dan Syukur penulis ucapkan kepada Allah SWT atas rahmat dan hidayahnya, karena-Nya penulis diberi kesempatan untuk dapat menyelesaikan skripsi ini. Penulis sangat bersyukur karena telah berhasil menuntaskan skripsi dengan judul **"Perlindungan Hukum Bagi Korban *Doxing* Sebagai Pencegahan Kebocoran Data Pribadi"** sesuai dengan harapan penulis.

Skripsi ini disusun guna memenuhi persyaratan dalam menyelesaikan studi untuk mencapai gelar Sarjana Hukum jenjang Strata Satu (S.1) Fakultas Hukum Universitas Islam Sultan Agung Semarang. Penulis mengangkat judul tersebut dikarenakan penulis memiliki kekhawatiran di masa yang akan datang mengenai bagaimana teknologi semakin meluas dan mempermudah tidak kejahatan *doxing*.

Pada kesempatan ini penulis ingin menyampaikan terimakasih yang sebesar – besarnya pada para pihak yang telah membantu serta membimbing, penulis ucapkan terimakasih sebesar – besarnya kepada:

1. Orangtua penulis Bapak Medi dan Ibu Fadrizul tercinta dan tersayang yang telah mendoakan penulis dalam tiap Langkah selama penulis berproses.
2. Bapak Prof. Dr. H. Gunarto S.H., S.E, Akt, M.H Selaku Rektor Fakultas Hukum Universitas Islam Sultan Agung Semarang
3. Bapak Dr. H. Jawade Hafidz, S.H., M.H Selaku Dekan Fakultas Hukum Universitas Islam Sultan Agung Semarang

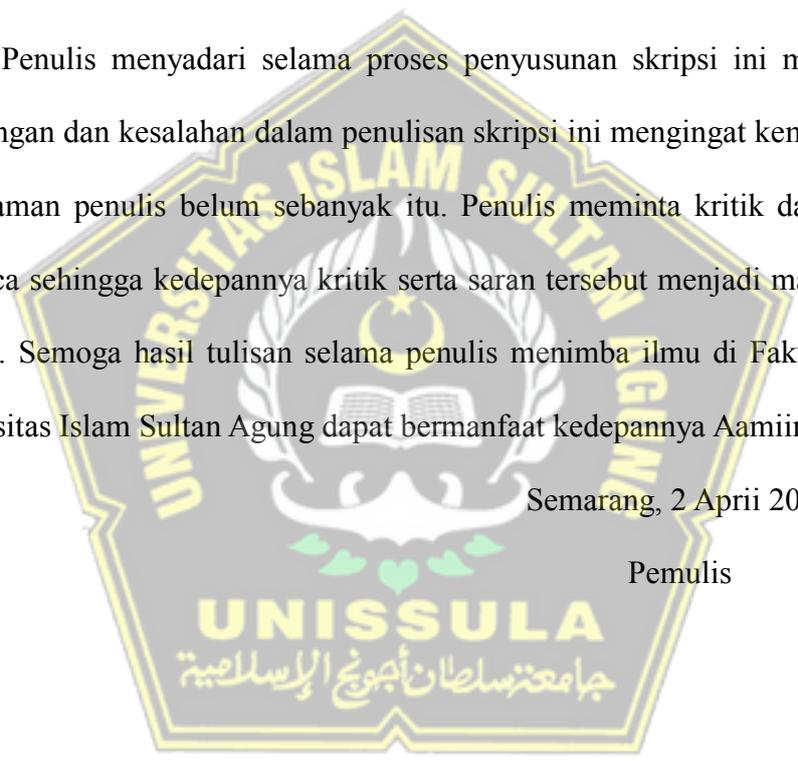
4. Ibu Dr. Widayati, S.H., M.H selaku Wakil Dekan I Fakultas Hukum Universitas Islam Sultan Agung Semarang
5. Bapak Dr. Denny Suwondo., SH., MH. Selaku Wakil Dekan II Fakultas Hukum Universitas Islam Sultan Agung Semarang
6. Bapak Dr. Muhammad Ngazis, SH., M.H Selaku Ketua Prodi Fakultas Hukum Universitas Islam Sultan Agung Semarang
7. Bapak Rizki Adi Pinandito, S.H., M.H selaku Dosen Pembimbing skripsi yang telah meluangkan waktunya dan memberikan ilmunya untuk membimbing, mendorong, mengarahkan penulis sehingga penulis dapat menyelesaikan penulisan skripsi ini di Fakultas Hukum UNISSULA Semarang
8. Seluruh Dosen dan Staf Fakultas Hukum Universitas Islam Sultan Agung yang selalu memberikan bimbingan serta ilmu pengetahuan yang bermanfaat bagi penulis selama kuliah hingga selesai.
9. Sherliana Ika Pratiwi selaku penulis segala bentuk terimakasih dan apresiasi untuk diri sendiri karena telah mampu menyelesaikan penulisan skripsi ini dengan segala kendala dan kesulitan namun tetap dilakukan hingga akhirnya penulis dapat berada pada titik ini.
10. Keluarga kedua penulis Salsa Jessica Devi dan Putri Lady Diana yang senantiasa kebersamai penulis dalam setiap proses penulisan skripsi ini dan selalu memastikan bahwa keadaan penulis baik – baik saja, semoga selalu dikelilingi hal baik.

11. Untuk seseorang yang tidak bisa penulis tuliskan namanya, terimakasih atas segala dukungan dan perhatian yang sudah diberikan kepada penulis secara maksimal, semoga selalu dalam lindungan Allah.
12. Teman – teman penulis yang tidak dapat penulis disebutkan satu per satu yang selalu berada disisi penulis dan selalu memberi semangat sehingga penulis dapat menyelesaikan penulisan ini.

Penulis menyadari selama proses penyusunan skripsi ini masih banyak kekurangan dan kesalahan dalam penulisan skripsi ini mengingat kemampuan dan pengalaman penulis belum sebanyak itu. Penulis meminta kritik dan saran dari pembaca sehingga kedepannya kritik serta saran tersebut menjadi masukan untuk penulis. Semoga hasil tulisan selama penulis menimba ilmu di Fakultas Hukum Universitas Islam Sultan Agung dapat bermanfaat kedepannya Aamiin.

Semarang, 2 April 2025

Pemulis



**Sherliana Ika Pratiwi**

**NIM : 30302100310**



## DAFTAR ISI

HALAMAN JUDUL.....	i
HALAMAN PERSETUJUAN PEMBIMBING .....	ii
HALAMAN PENGESAHAN.....	iii
MOTTO DAN PERSEMBAHAN .....	iv
PERNYATAAN KEASLIAN TESIS .....	v
SURAT PERNYATAAN PERSETUJUAN PUBLIKASI.....	vi
KATA PENGANTAR.....	vii
DAFTAR ISI.....	xi
ABSTRAK.....	xiii
<i>ABSTRACT</i> .....	xiv
BAB I PENDAHULUAN.....	15
A. Latar Belakang Masalah.....	15
B. Rumusan Masalah .....	24
C. Tujuan Penelitian.....	24
D. Kegunaan Penelitian.....	24
E. Terminologi .....	25
F. Metode Penelitian.....	27
G. Sistematika Penulisan.....	32
BAB II TINJAUAN PUSTAKA.....	34
A. Tinjauan Umum Perlindungan Hukum .....	34
B. Tinjauan Umum Tindak Pidana.....	37
1. Penjelasan Umum Tindak Pidana .....	37
2. Unsur – Unsur Tindak Pidana.....	38
C. Tinjauan Umum Tentang <i>Cyber crime</i> .....	42
D. Tinjauan Umum Tentang <i>Doxing</i> .....	46
1. Dampak psikologis .....	51
2. Dampak Sosial .....	51
3. Dampak Ekonomi dan Karier .....	52
4. Dampak hukum.....	52

E. Pengertian Data Pribadi.....	53
F. Perlindungan Data Pribadi Dalam Perspektif Islam.....	54
BAB III HASIL PENELITIAN DAN PEMBAHASAN .....	58
A. Perlindungan Hukum Bagi Korban <i>Doxing</i> Sebagai Pencegahan Kebocoran Data.....	58
1. Perlindungan Hukum Bagi Korban <i>Doxing</i> .....	58
2. Perlindungan Hukum Korban <i>Doxing</i> Sebagai Pencegahan Kebocoran Data Pribadi.....	73
B. Kendala Dan Solusi Dalam Menjalankan Perlindungan Korban <i>Doxing</i> .....	76
1. Pemerintah .....	78
2. Pemilik data pribadi .....	79
3. Aparat penegak hukum .....	79
4. Masyarakat.....	80
BAB IV PENUTUP .....	89
A. Kesimpulan.....	89
B. Saran.....	90
DAFTAR PUSTAKA .....	92



## ABSTRAK

*Doxing* pasti tidak asing untuk beberapa masyarakat Indonesia, meskipun ada beberapa masyarakat yang belum mnegerti ap aitu *doxing* namun secara tidak sadar tindak kejahatan berupa *doxing* selalu ada setiap harinya bahkan ada di sekeliling kita. *Doxing* juga selalu mempersamai masyarakat dalam kehidupan sehari – sehari terutama dalam kegiatan interaksi yang dilakukan di sosial media. *Doxing* sendiri merupakan Tindakan menyebarkan data pribadi secara sepihak yang dilakukan oleh orang yang tidak bertanggungjawab. Perlunya membahas serta mengkaji mengenai perlindungan hukum bagi korban *doxing* adalah untuk memberi pemahaman mengenai materi – materi yang berkaitan dengan *doxing*, dampak serta bagaimana sanksi bagi pelaku sebagai bentuk perlindungan terhadap korban.

Penelitian ini menggunakan metodologi pendekatan hukum normatif yang memanfaatkan data primer dan sekunder. Sumber data dari penelitian ini diperoleh melalui dokumen – dokumen, karya tulis ilmiah, peraturan perundang – undangan hingga tulisan pendukung lainnya. Metode analisis yang digunakan yakni metode deskriptif kualitatif.

Berdasarkan hasil penelitian dapat disimpulkan bahwa dalam perlindungan hukum bagi korban *doxing* sebagai pencegahan kebocoran data pribadi, dalam kenyataannya masih memiliki kendala yang beberapa dari beberapa factor seperti factor individu, pemerintah dan aparat penegak hukum. Tulisan ini dimaksudkan untuk sekurang – kurangnya memberikan pemahaman mengenai perlindungan korban *doxing* serta hubungan antara perlindungan hukum yang sudah ada dalam implementasi pencegahan kebocoran data.

**Kata Kunci :** Perlindungan Hukum; Korban *Doxing*; Pencegahan; Data Pribadi

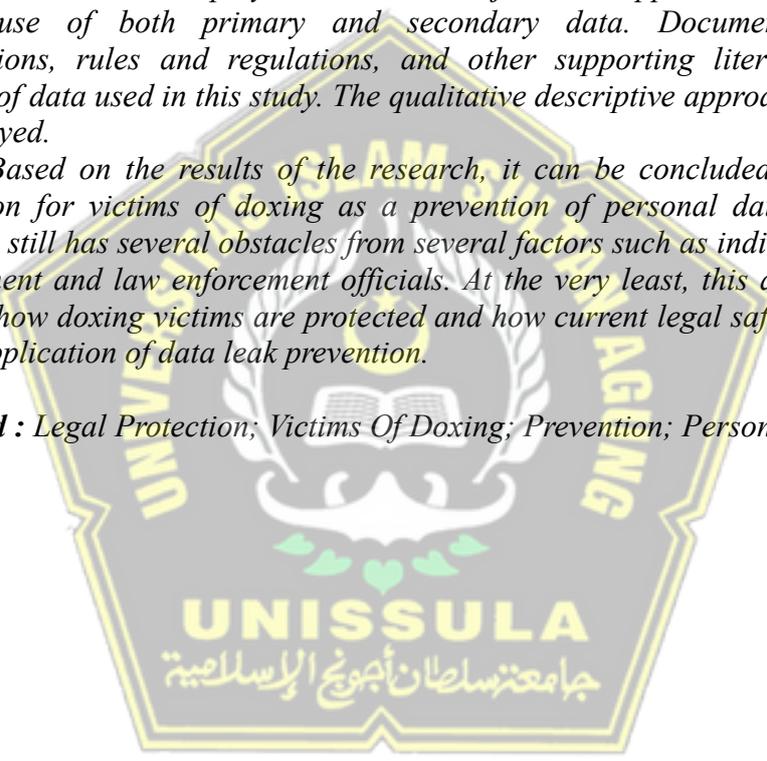
## **ABSTRACT**

*Doxing is certainly familiar to some Indonesians, although there are some people who do not understand what doxing is, but unconsciously the crime of doxing is always there every day and even around us. Doxing also always accompanies people in their daily lives, especially in interaction activities carried out on social media. Doxing itself is an act of spreading personal data unilaterally carried out by irresponsible people. The need to discuss and examine the legal protection for victims of doxing is to provide an understanding of the materials related to doxing, the impact and how sanctions for perpetrators as a form of protection for victims.*

*The research employs the normative juridical approach method, which makes use of both primary and secondary data. Documents, scientific publications, rules and regulations, and other supporting literature are the sources of data used in this study. The qualitative descriptive approach of analysis is employed.*

*Based on the results of the research, it can be concluded that in legal protection for victims of doxing as a prevention of personal data leakage, in reality it still has several obstacles from several factors such as individual factors, government and law enforcement officials. At the very least, this article aims to explain how doxing victims are protected and how current legal safeguards relate to the application of data leak prevention.*

**Keyword :** *Legal Protection; Victims Of Doxing; Prevention; Personal Data*



# BAB I

## PENDAHULUAN

### A. Latar Belakang Masalah

Penggunaan media sosial pada era digital sekarang seringkali salah digunakan, beberapa pengguna media sosial pada kenyataannya kurang bijak dalam menggunakan media sosial. Ketidakbijakan dalam penggunaan inilah yang selanjutnya akan berdampak negatif dan menimbulkan tindak pidana kejahatan siber. Kejahatan siber atau biasa disebut *cyber crime* dapat digambarkan sebagai aktivitas ilegal yang dilakukan secara daring dan bergantung pada teknologi komputer dan telekomunikasi canggih.<sup>1</sup> Meskipun teknologi informasi ini memiliki peran yang cukup penting dalam bidang perdagangan serta meningkatkan pertumbuhan perekonomian, namun apabila teknologi seperti media sosial ini dalam penggunaannya disalahgunakan maka dapat merugikan orang lain.

Selain itu beberapa pengguna media sosial juga tidak sering yang sadar bahwa mereka sedang melakukan tindak pidana *doxing*. Dalam permasalahan ini maka akan menjadi masalah berkelanjutan bagi korban karena mereka mungkin menderita kerugian finansial selain penderitaan immaterial materiil. Kerugian immaterial korban *doxing* sangat jelas dimana korban merasakan penderitaan karena data yang bocor diluar kendalinya meyebabkan beberapa pihak dengan mudah mengakses datanya dan dapat digunakan oleh orang lain

---

<sup>1</sup> Sari, I. (2023). Perbedaan Bentuk Kejahatan Yang Dikategorikan Sebagai *Cyber crime* Dan *Cyber Warfare*. *JSI (Jurnal Sistem Informasi) Universitas Suryadarma*, 10(1), hlm. 246. <https://doi.org/10.35968/jsi.v10i1.1002>

secara bebas. Sedangkan kerugian korban secara materiil dapat berupa kehilangan pekerjaan yang kemudian korban menjadi kehilangan penghasilannya. Oleh karena itu tindak pidana *doxing* perlu dikaji lebih lanjut mengenai bagaimana perlindungan hukum bagi korbannya. Yang menjadi titik fokusnya yakni karena semua korban kejahatan atau korban tindak pidana berhak atas perlindungan hukumnya atau semua orang berhak mendapatkan perlindungan hukum.

Kejahatan siber seringkali terjadi karena media sosial yang merupakan suatu *platform* yang gunanya sebagai wadah berinteraksi dan berbagi informasi secara daring (*online*) menjadikan banyak pengguna membagikan beberapa informasi pribadinya yang kemudian dapat menjadi sasaran empuk bagi pelaku kejahatan siber. Rata-rata pengguna internet di seluruh dunia menghabiskan sekitar 143 menit (2 jam 33 menit) per hari di media sosial, menurut studi We Are Social yang dirilis pada Januari 2024. Dengan predikat sebagai negara dengan basis pengguna media sosial terbesar, khususnya di aplikasi Facebook, Instagram, YouTube, dan Twitter, Indonesia berhasil masuk ke dalam 10 peringkat teratas data ini (sudah berganti nama serta logo pada 23 Juli 2023 dan telah diumumkan pada 22 Juli 2023), dan *TikTok*. Sehingga melalui data durasi penggunaan media sosial maka kasus kejahatan siber selalu meningkat setiap tahunnya.

Menurut DataIndonesia.id dari laporan SAFEnet ada 302 serangan digital di Indonesia pada tahun 2022. Untuk kasus *doxing* ini ada sebanyak 15 kejadian dalam setahun. Selain itu, Badan Siber dan Sandi Negara (BSSN)

memperkirakan ratusan juta serangan siber terjadi setiap tahunnya, dengan estimasi 279,84 juta terjadi pada tahun 2023 saja.<sup>2</sup> Banyaknya kasus *doxing* ini sayangnya menimpa anggota jurnalis yang seharusnya dilindungi oleh undang – undang karena memiliki kode etiknya sendiri. Beberapa korban *doxing* juga berasal dari *content creator* dan bahkan tak jarang pula tokoh publik menjadi sasaran pelaku *doxing*, biasanya melakukan ancaman terhadap independensi mereka didalam menjalankan pekerjaannya serta mempengaruhi kehidupan sehari – harinya. Kemudian Nenden Sekar Arum selaku Direktur Eksekutif Safenet dalam wawancaranya menyatakan bahwa dari hasil pemantauan Safenet, serangan digital kepada aktivis atau pembela HAM meningkat beberapa tahun terakhir. Pada tahun 2020, serangan digital yang tercatat 147 kasus. Kemudian, pada 2021 meningkat menjadi 193 kasus, 2022 menjadi 302 kasus, dan pada 2023 melonjak menjadi 323 kasus.<sup>3</sup>

*Doxing* secara etimologis yakni berasal dari kata document dan tracking, documents tracking artinya tindakan pemantauan serta pencatatan aktivitas dokumen dari mulai pembuatan hingga pendistribusian dokumen tersebut.<sup>4</sup> *Doxing* atau biasa juga disebut sebagai *doxxing* atau biasa disingkat *doxx* yang merupakan singkatan dari dokumen, namun secara etimologi *doxing* berasal dari kalimat “*dropping box*” atau “*dropping documents*”.

---

<sup>2</sup> Permata Ayunda P. dan Lucky Nurhayanto, 2024, Perspektif Perilaku *Doxing* Sebagai Bentuk Cancel Culture pada Pengguna Media Sosial X, *Jurnal Hukum, Humaniora Dan Politik*, Vol.4, No. 4, hlm. 674.

<sup>3</sup> Dian Dewi Purnamasari, “*Doxing* pada Peneliti ICW dan Pentingnya Penguatan Perlindungan kepada Aktivis” <https://www.kompas.id/artikel/serangan-digital-masih-mengintai-aktivis-dan-kelompok-kritis> diakses pada 28 April 2025 pkl. 23.36. DOXING ADALAH

<sup>4</sup> Racha Chotia, “What is document tracking? Why is it important?”, <https://signeasy.com/blog/business/document-tracking/> Diakses pada 28 April; 2025 pkl. 23.50.

*Doxing* diartikan sebagai tindakan mencari, berbagi, atau mengunggah informasi pribadi seseorang secara daring.<sup>5</sup> Namun *doxing* bukan hanya semata menyebarkan data pribadi seseorang saja, seringkali pelaku *doxing* melakukan ini untuk kejahatan dan tidak jarang pula mengundang *cyberbullying* pada beberapa kasus. *Doxing* bukan menyebarkan data pribadi untuk sekedar informasi biodata pada umumnya, seringkali *doxing* dijadikan sebagai alat balas dendam di media sosial.

David M. Douglas mengategorikan *doxing* dalam 3 kategori yakni *Deanonymizing*, *Targeting* dan *Delegitimizing*. *Deanonymizing* merupakan Doxxing adalah tindakan mempublikasikan identitas pribadi seseorang atau sekelompok orang yang identitasnya tidak diketahui oleh masyarakat umum (informasi anonim) atau diketahui melalui nama samaran. Sebagai bentuk kebebasan berbicara, *deanonymizing* memiliki dampak signifikan pada identitas seseorang dan dapat menakutkan bagi seseorang atau sekelompok orang yang tidak ingin identitasnya diketahui dunia.<sup>6</sup>

*Targeting* adalah *doxing* Hal ini membuat informasi tentang lokasi fisik seseorang menjadi publik, sehingga dapat dilacak hingga lokasi orang tersebut ditemukan secara *real time* *targeting* dapat meningkatkan kemungkinan seseorang dan/atau sekelompok Orang dapat ditemukan secara langsung, dan tempat tinggal mereka diketahui. Hal ini dapat berisiko karena dapat

---

<sup>5</sup> Terjemahan *Oxford British and World English Dictionary*

<sup>6</sup> Douglas, David M, '*Doxing: A Conceptual Analysis*', *Ethics and Information Technology* 18 (3), 2016, hlm. 200

membahayakan seseorang, terutama jika mereka diancam secara fisik, seperti dalam suatu serangan. Aktivitas doxing ini dilakukan setelah *deanonymizing*.<sup>7</sup>

Kemudian yang terakhir yakni *delegitimizing* dimana ini adalah suatu tindakan menyebarkan informasi pribadi seseorang atau suatu kelompok dengan tujuan merusak atau mencemarkan nama baik, kredibilitas, atau karakternya. Doxing adalah praktik mengeksploitasi informasi pribadi seseorang yang mudah disalahartikan atau informasi yang sebenarnya rahasia untuk memermalukan, menyinggung, dan menghancurkannya.<sup>8</sup>

Perkembangan teknologi informasi yang begitu pesat telah membawa berbagai perubahan dalam kehidupan masyarakat sehari-hari di sejumlah bidang, yang berdampak langsung pada terciptanya berbagai peraturan perundang-undangan yang sebelumnya tidak pernah ada, serta pada pemanfaatan dan penerapan teknologi informasi memicu banyak tindak kejahatan siber. Setelah memahami bagaimana konsep mengenai *doxing* yang menjadi fokus selanjutnya adalah apa saja kemungkinan yang dapat terjadi jika *doxing* terjadi pada seseorang.

*Doxing* merupakan tindak pidana yang memiliki dampak berkelanjutan sebagai contoh apabila seseorang terkena *doxing* selain dari kebocoran data pribadi yang dianggap merugikan korban seringkali dampak lain juga turut dirasakan korban, salah satunya adalah *cyberbullying*. *Cyberbullying* adalah tindakan kekerasan yang dilakukan oleh sekelompok orang atau individu dengan menggunakan teknologi digital atau media elektronik untuk menyakiti

---

<sup>7</sup> *Ibid*, hlm. 200

<sup>8</sup> *Ibid*, hlm. 200

orang lain secara berulang dengan tujuan membuat korban merasa tidak nyaman dan takut, baik secara verbal maupun nonverbal.<sup>9</sup> Terjadinya *doxing* tidak jarang memicu pelanggaran lebih lanjut yang dilakukan oleh mereka yang tidak suka dengan korban *doxing*, pelaku dari tindak pidana ini biasanya berbeda dengan pelaku *doxing*. Dimana pelaku *doxing* yang mengunggah data pribadi korban ke media sosial kemudian pelaku dari dampak mengambil kesempatan dengan ikut serta berkomentar dengan menggunakan kalimat yang mengandung konotasi negatif bagi korban.

Islam menjelaskan mengenai keharusan menjaga privasi seseorang, dalam islam dijelaskan untuk menjaga privasi dalam beberapa kondisi salah satunya dijelaskan dalam HR Ibnu Abid Duniya yang berbunyi:

أخيك بسر تحدث أن الخيانة من إن الحسن وقال أمانة بينكم الحديث مطلقا وقال

Artinya, “Percakapan di antara kalian merupakan amanah,” tegas Nabi Muhammad SAW (HR Ibnu Abid Duniya). Menurut Imam Al-Hasan, "membocorkan rahasia saudaramu termasuk jenis pengkhianatan," (Al-Ghazali, 2018 M/1439 H-1440 H: III/137).<sup>10</sup> Ayat tersebut menunjukkan bahwa apapun yang kita ketahui tentang kehidupan orang lain maka sejauh apapun pengetahuan kita, kita tidak memiliki hak untuk menyebarkan “sesuatu” milik orang lain yang rahasia baginya terutama apabila menyebarkan dan mengakibatkan saudara kita mengalami kerugian baik secara fisik maupun materi.

---

<sup>9</sup> Lianthy Nathania Paat, 2020, KAJIAN HUKUM TERHADAP CYBER BULLYING BERDASARKAN UNDANG – UNDANG NOMOR 19 TAHUN 2016, *Journal Lex Crimen*, Vol. IX, No. 1, hlm. 14.

<sup>10</sup> “Hukum membuka rahasia orang”, Quran Online, <https://nu.or.id/syariah/hukum-membuka-rahasia-orang-lain-rA1ts> diakses tanggal 21 April 2025 pk1. 22.30.

Selanjutnya mengenai tindak perundungan dalam islam diatur dalam Q,S Al Hujurat Ayat 11 yang berbunyi:

يَكُنَّ أَنْ عَسَى نُسَاءٍ مِّنْ نِّسَاءٍ وَلَا مِّنْهُمْ خَيْرًا يَكُونُوا أَنْ عَسَى قَوْمٍ مِّنْ قَوْمٍ يَسْحَرُونَ لَا آمَنُوا الَّذِينَ يَأْتِيهَا  
فَأُولَئِكَ يَنْبَغُ لَمْ وَمَنْ الْإِيمَانِ بَعْدَ الْفُسُوقِ الْإِسْمِ بِئْسَ الْأَلْفَابُ تَنَابَزُوا وَلَا أَنْفُسَكُمْ تَلْمِزُوا وَلَا مِّنْهُمْ خَيْرًا  
○ الظالمون هم

Artinya : Wahai orang-orang yang beriman, janganlah kamu biarkan manusia mengolok-olok manusia lain, karena bisa jadi mereka lebih baik dari orang-orang yang mengolok-olok mereka, dan janganlah kamu biarkan wanita-wanita mengolok-olok wanita-wanita lain, karena bisa jadi mereka lebih baik dari orang-orang yang mengolok-olok mereka. Janganlah kamu saling mencaci dan menghina. Seburuk-buruk panggilan bagi orang-orang fasik setelah agama. Sesungguhnya orang-orang yang zalim adalah orang-orang yang tidak mau bermusyawarah. (Q.S AL – HUJURAT AYAT 11).<sup>11</sup>

Pada ayat tersebut dijelaskan bahwa seharusnya sesama muslim dilarang keras untuk saling mencela dan mengolok – olok. Karena hal tersebut juga dianggap sangat buruk dan bahkan haram untuk dilakukan dan harus dihindari oleh umat muslim.

Selanjutnya *doxing* atau juga kebocoran data Undang-Undang Informasi dan Transaksi Elektronik memberikan penjelasan yang komprehensif. Dalam Undang-Undang Nomor 1 Tahun 2024 tentang Perubahan Kedua atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik, Pasal 26 ayat (1), dilarang melakukan pengolahan data pribadi seseorang tanpa persetujuan orang tersebut. Menurut pasal tersebut: “Setiap orang yang

<sup>11</sup> “Al – Hujurat Ayat 11”, Quran Online, <https://quran.nu.or.id/al-hujurat/11> diakses tanggal 21 April 2025 pkl. 22.40.

secara terang-terangan melakukan kegiatan yang menimbulkan kerugian tanpa izin atau melawan hukum atau gangguan pada sistem komputer dan/atau system elektronik".

Sebagai contohnya yaitu kasus *doxing* yang menimpa seorang jurnalis Liputan6.com Bernama Cakrayuri Nuralam, kasus ini terjadi pada tahun 2020. Kasus ini berangkat dari terbitnya artikel cek fakta yang berjudul "*Cek Fakta: tidak Benar Arteri Dahlan Sebut Semua Agama Sama di Acara Mata Najwa*". Artikel tersebut dibuat dengan maksud meluruskan informasi yang keliru serta beredar luas dalam masyarakat mengenai suatu pernyataan seorang tokoh publik (politisi) dalam acara televisi.

Namun terbitnya artikel ini justru memicu kemarahan pihak – pihak yang merasa tidak senang dengan hasil pemeriksaan fakta tersebut. Hal ini juga dianggap bahwa karena adanya perbedaan yang akhirnya memunculkan tindak pidana *doxing*. Setelah terbitnya artikel tersebut, seorang pengguna media sosial dengan akun Instagram yang bernama @d34th.5kull melakukan tindak pidana *doxing* terhadap jurnalis yang bersangkutan. *Doxing* yang dilakukan pelaku berupa penyebaran foto pribadi, nama lengkap serta identitas jurnalis tersebut yang disebarluaskan melalui media sosial.

Dalam postingannya pelaku juga menuliskan kalimat yang terkesan merendahkan dan mengancam. Karena *doxing* yang dilakukan pelaku tersebut aktivitas korban sebagai jurnalis yang sedang dijalankan menjadi terganggu, hal ini juga dianggap sebagai bentuk serangan terhadap kebebasan pers. Pada

kasus ini keluarga korban pun turut serta merasakan dampak berupa adanya tekanan sosial dan potensi ancaman yang sifatnya mengintimidasi.

Oleh karena itu maka dalam hukum positif pun sebenarnya larangan *doxing* sudah diatur jelas dan tegas, dimana sebagai warga negara kita dilarang untuk menggunakan data pribadi orang lain tanpa persetujuan untuk melakukan perbuatan melawan hukum karena semua sudah diatur dalam hukum positif. Kemudian dapat diputuskan yang melatar belakangi penulisan ini adalah adanya *gap research* antara *das sollen* dan *das sein*. Dimana peraturan hukum yang sudah ditetapkan dan dibentuk oleh pemerintah fungsi perlindungannya masih belum berjalan dengan maksimal di lingkungan masyarakat. Sehingga dalam kehidupan sehari – hari masih banyak korban *doxing* pada level tertentu yang juga terkena perundungan melalui media sosial, dimana hal ini juga memicu kerusuhan dan amarah yang akhirnya tidak dapat diprediksi dengan tepat.

Penulis tertarik untuk meneliti fenomena *doxing* yang menjadi pokok bahasan deskripsi data perlindungan hukum bagi korbannya, yang disusun dalam skripsi yang berjudul “Perlindungan Hukum Bagi Korban *Doxing* sebagai pencegahan terjadinya Kebocoran Data”. Penelitian ini penting untuk dilakukan guna menganalisis bagaimana perlindungan hukum terhadap korban *doxing* yang diterapkan, serta guna mengkaji lebih lanjut mengenai instrument yang menjadi kendala dalam penerapan perlindungan hukum tersebut.

## **B. Rumusan Masalah**

Rumusan masalah yang akan menjadi pokok bahasan dalam penelitian ini dapat dirumuskan sebagai berikut dengan menggunakan informasi yang telah tersedia pada latar belakang masalah:

1. Bagaimana pengaturan hukum bagi perlindungan korban *doxing*?
2. Apa yang menjadi kendala dalam perlindungan korban dan bagaimana solusi untuk mengatasi situasi tersebut?

## **C. Tujuan Penelitian**

Berikut ini adalah tujuan dari penelitian ini yang didasarkan pada rumusan masalah:

1. Untuk mengetahui apakah peraturan yang sudah dibuat dan ditetapkan dapat menjadi salah satu bentuk pencegahan terhadap kebocoran data pribadi, serta untuk mengetahui bagaimana pengaturan tersebut.
2. Untuk mengkaji kendala yang terjadi dan memberikan solusi yang tepat dan efisien untuk menjalankan peraturan terkait dikemudian waktu.

## **D. Kegunaan Penelitian**

Penelitian ini memiliki sejumlah keuntungan atau aplikasi, termasuk yang berikut ini:

1. Manfaat Teoritis
  - a. Bagi Masyarakat

Pembahasan serta Diharapkan bahwa temuan penyelidikan ini akan memberikan informasi mengenai bagaimana pemakaian sosial

media secara bijak agar tidak menjadi boomerang pada diri sendiri. Penelitian ini juga berguna agar masyarakat mengetahui kualitas peraturan kita dalam penyelesaian dan perlindungan suatu masalah.

b. Bagi Mahasiswa

Sebagai bahan acuan informasi tambahan bagi para calon penulis dalam menulis penulisan selanjutnya.

2. Manfaat Praktis

a. Bagi Masyarakat

Agar masyarakat dapat saling mengingatkan dalam kehidupan sehari – hari bahwa penggunaan sosial media tidak sesederhana kelihatannya, serta masyarakat juga dapat ikut menjaga keseimbangan penggunaan sosial media untuk mengurangi tindakan *doxing* yang dilakukan oleh orang tidak bertanggungjawab.

b. Bagi Mahasiswa

Diharapkan penelitian ini dapat menjadi bahan bacaan atau *literature* bagi mahasiswa dalam penyusunan tugas ataupun dijadikan bahan sebagai materi presentasi pada materi tertentu.

## E. Terminologi

1. Perlindungan

Kata "perlindungan" berasal dari kata bahasa Indonesia "lindung", yang menurut kamus besar berarti "melindungi, mencegah, memelihara, dan membentengi". Sebaliknya, perlindungan berarti menyimpan, melindungi, memelihara, dan melestarikan. Secara umum, perlindungan

adalah tindakan melindungi sesuatu baik itu objek atau kepentingan dari hal-hal yang mengancam atau berbahaya. Perlindungan juga mengacu pada pemberian perlindungan kepada orang yang lebih lemah. Namun dalam pengertian hukum, hukum dapat diartikan sebagai semua tindakan yang disengaja yang dilakukan oleh individu, pemerintah, atau organisasi swasta dengan tujuan melindungi, mengatur, dan memberikan kesejahteraan sesuai dengan hak asasi manusia yang telah ada, sebagaimana digariskan dalam Undang-Undang Nomor 39 Tahun 1999 tentang Hak Asasi Manusia.<sup>12</sup>

## 2. Korban

Korban adalah seseorang yang mengalami kerugian finansial, psikologis, atau fisik akibat tindakan kriminal.<sup>13</sup> Atau bisa juga diartikan bahwa Korban adalah orang yang kehilangan sesuatu akibat suatu kejadian kriminal, dimana kerugian yang didapat bukan hanya tentang kerugian materi namun juga kerugian secara fisik,

## 3. *Doxing*

*Doxing* atau praktik penyebaran informasi pribadi seseorang secara daring atau melalui media sosial yang dilakukan oleh individu yang ceroboh tanpa persetujuan subjek dan untuk alasan jahat.<sup>14</sup> *Doxing* juga termasuk bentuk dari kebocoran data namun *doxing* adaah bentuk

---

<sup>12</sup> Anonym, <http://tesishukum.com/pengertian-perlindungan-hukum/> diakses pada 22 April 2025 pkl. 11.30

<sup>13</sup> Pasal 1 ayat (2) Undang – undang Nomor 13 Tahun 2006 Tentang Perlindungan Saksi dan Korban

<sup>14</sup> Leonardo Latsiano Dade, Caecilia J.J Waha & Nurhikmah Nachrawy, 2024, Kajian Yuridis Tentang Tindak Pidana Penyebaran Data Pribadi Melalui Internet (*Doxing*) Di Indonesia, *Jurnal Fakultas Hukum Universitas Sam Ratulangi Lex Privatum* Vol.13 No. 3, hlm. 3.

kebocoran data yang disengaja yang direncana bukan dikarenakan kesalahan system.

#### 4. Pencegahan

Menurut Bahruddin Lopa (2001), pengertian pencegahan lebih dikenal dengan istilah penanggulangan kejahatan dari sudut pandang hukum. Selain cara preventif, tindakan represif juga dapat digunakan untuk mencegah terjadinya kejahatan. Kamus Besar Bahasa Indonesia mengartikan pencegahan sebagai suatu tata cara, pendekatan, atau tindakan yang menghentikan atau membatasi terjadinya sesuatu. Artinya, pencegahan dapat pula dilakukan dengan cara penanggulangan sebagai upaya awal yang dilakukan agar “hal” yang merugikan tersebut tidak terjadi.

#### **F. Metode Penelitian**

Adapun yang menjadi bagian dari metode penelitian sebagai acuan dalam penulisan yakni sebagai berikut :

##### 1. Metode Pendekatan

Sugiyono berpendapat bahwa metode penelitian adalah pendekatan ilmiah untuk mengumpulkan data untuk aplikasi tertentu. Prosedur, teknik, instrumen, dan desain penelitian semuanya terkait erat dengan metodologi penelitian. Pendekatan penelitian yang dipilih dan desain penelitian harus sesuai. Metode penelitian yang ditentukan juga harus diikuti oleh prosedur, metode, dan instrumen yang digunakan dalam penelitian. Penulis kemudian menggunakan metode pendekatan hukum normatif dalam

penyelidikan ini. Dalam hal ini, penulis ingin memfokuskan pada dasar pengkajian aspek – aspek dalam hukum positif yang berhubungan. Pendekatan yuridis normatif juga mendasar kepada analisisnya terhadap peraturan aturan—aturan yang relevan dengan topik penelitian dan berlaku.

## 2. Spesifikasi Penelitian

Uraian spesifikasi kajian hukum dalam tulisan ini bersifat deskriptif, dengan tujuan memberikan gambaran menyeluruh tentang fenomena masyarakat. Tulisan ini juga memaparkan secara rinci beberapa aspek yang terkait dengan masalah yang diteliti. Dalam artian yang menjadi fokus adalah bagaimana perlindungan korban *doxing*.

## 3. Jenis dan Sumber Data

Sumber data yang digunakan dalam penulisan penelitian ini adalah :

### a. Sumber data primer

Pada penelitian ini yang menjadi sumber primer adalah segala informasi yang berkaitan dengan topik pada Undang – undang Nomor 1 Tahun 2024 Tentang Informasi dan Transaksi Elektronik. Hal ini sesuai dengan studi kepustakaan yang dituliskan pada Judul penelitian. Pendapat individu atau kelompok orang, hasil survei observasi terhadap suatu hal, peristiwa, atau tindakan tertentu, atau hasil pengujian merupakan contoh data primer.

### b. Sumber data sekunder

Melalui tinjauan pustaka dan bacaan, sumber data sekunder untuk penelitian ini dikumpulkan kepustakaan diluar bahan primer yang menjadi acuan untuk memperoleh informasi tambahan guna memperkuat hasil tulisan dalam bentuk ketentuan formal maupun data. Data sekunder dalam penelitian ini dikelompokkan menjadi 3 (tiga) yaitu sebagai berikut :

1) Bahan Hukum Primer, yakni bahan hukum yang mengikat, terdiri atas :

- a) Undang – Undang Dasar Negara Republik Indonesia Tahun 1945
- b) Kitab Undang – undang Hukum Pidana
- c) Undang – undang Nomor 1 Tahun 2024 Tentang Informasi dan Transaksi elektronik, yang secara jelas disebutkan dalam judul penulisan.
- d) Undang – Undang Nomor 19 Tahun 2016 tentang perubahan atas Undang – Undang Nomor 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik yang, sebagai bahan hukum penunjang karena masih ada keterkaitan
- e) Undang – undang Nomor 27 Tahun 2022 Tentang Pelindungan Data Pribadi

2) Bahan Hukum Sekunder, Secara khusus, konten yang seharusnya menjelaskan hukum primer, atau alternatifnya, hukum sekunder, yang merupakan penjelasan lebih menyeluruh tentang hukum

primer, berasal dari materi hukum sekunder pustaka yang berhubungan diantaranya dapat berupa buku – buku, dokumen atau publikasi yang berkaitan dengan masalah atau fenomena yang sedang dikaji, yakni mengenai perlindungan hukum bagi korban *doxing* sebagai pencegahan kebocoran data.

3) Bahan Hukum Tersier, yaitu dokumen hukum, seperti Kamus Hukum atau Kamus Besar Bahasa Indonesia, yang tujuannya memberi arahan dan klarifikasi mengenai bahan hukum primer dan sekunder.

#### 4. Metode Pengumpulan Data

##### a. Pengumpulan Data Primer

Penelitian hukum normatif, yang juga dikenal sebagai penelitian hukum kepustakaan, mengumpulkan data melalui data sekunder dari studi kepustakaan. Hal ini dilakukan dengan mencari peraturan dan buku-buku lain yang relevan dengan masalah yang diteliti. Studi kepustakaan yang didasarkan pada bahan sekunder dikenal sebagai penelitian hukum normatif.<sup>15</sup> Sehingga data yang dikumpulkan murni melalui pencarian kepustakaan yang kemudian dikemas dan dikaji menjadi lebih terperinci dan mudah untuk dipahami.

##### b. Pengumpulan Data Sekunder

Dalam penelitian ini pengumpulan data sekunder tidak jauh berbeda dengan data primer hal ini dikarenakan bahan hukum yang

---

<sup>15</sup> Johannes Supranto, (2003). *Metode Penelitian Hukum dan Statistik*. Rineka Cipta: Jakarta. 2003, hlm. 2.

digunakan juga masih saling bersangkutan sehingga yang membedakan hanyalah porsi atau presentase banyaknya data yang dimasukkan dalam penulisan ini. Tentu saja data primer harus menjadi acuan yang utama sehingga presentase keberadannya lebih banyak dibandingkan dengan yang sekunder maupun tersier.

#### 5. Lokasi dan Subyek Penelitian

Dalam penulisan ini penelitian tidak dilakukan secara langsung di lapangan atau mendatangi instansi secara langsung, melainkan melalui analisis dokumen data primer maupun sekunder yang diperoleh dari situs resmi JDIH Kominfo (Jaringan Dokumentasi dan Informasi Hukum) dan Peraturan BPK RI (Badan Pemeriksa Keuangan Republik Indonesia). Sehingga Lokasi yang dituliskan tidak spesifik namun data serta bahan yang digunakan berasal dari wilayah Indonesia. Kemudian subyek dalam penelitian ini adalah bentuk – bentuk perlindungan yang tertulis dalam peraturan untuk melindungi korban *doxing* yang termasuk dalam korban tidak bijaknya pengguna media sosial.

#### 6. Metode Analisis Data

Data yang diperoleh kemudian diproses dan diatur secara metedis, logis, dan legal sebagai bagian dari pendekatan analisis yang digunakan dalam pemrosesan data dan tidak lupa disusun dalam bentuk deskriptif guna mendapatkan gambaran umum dari data yang didapat dalam penelitian. Gambaran umum tersebut didapatkan melalui analisis dengan menggunakan metode kualitatif. Menurut Lexy Moleong mendefinisikan

Penelitian kualitatif didefinisikan sebagai penelitian yang menggunakan berbagai metode ilmiah dan bertujuan untuk memahami fenomena tentang apa yang dipahami subjek penelitian, seperti aktor, persepsi, motivasi, tindakan, dan sebagainya, secara holistik dan deskriptif dalam bentuk kata-kata dan bahasa dalam konteks alamiah tertentu.<sup>16</sup>

## **G. Sistematika Penulisan**

### **BAB I PENDAHULUAN**

Bagian ini akan memberikan penjelasan tentang latar belakang masalah, konseptualisasi, tujuan penelitian, dan penggunaan Terminologi, Metode Penelitian serta Sistematika penulisan yang tiap bagiannya sudah dijelaskan secara detail.

### **BAB II TINJAUAN PUSTAKA**

Tinjauan umum tentang doxing, perlindungan hukum yang diberikan kepada korban kejahatan ini, dan hubungannya dengan penelitian tentang doktrin Islam semuanya akan dibahas dalam bagian ini.

### **BAB III HASIL PENELITIAN DAN PEMBAHASAN**

Bagian ini akan menjelaskan bagaimana korban tindakan kriminal diberikan perlindungan hukum *doxing*. Yang kemudian difokuskan kepada apa kendala dalam menjalankan fungsi

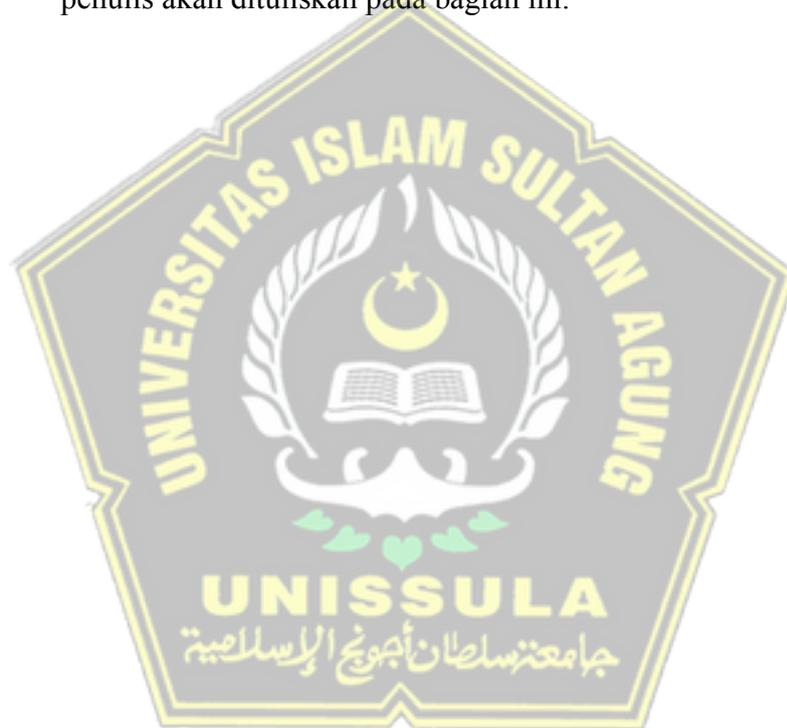
---

<sup>16</sup> Moleong, L. J. (2013). *Metodologi Penelitian Kualitatif*. Bandung: PT. Remaja Rosdakarya.

perlindungan tersebut kepada masyarakat dan juga berisikan solusi dari penulis untuk kendala yang terjadi.

#### **BAB IV PENUTUP**

Kesimpulan dan rekomendasi terkait fenomena yang diangkat penulis akan dituliskan pada bagian ini.



## BAB II

### TINJAUAN PUSTAKA

#### A. Tinjauan Umum Perlindungan Hukum

Istilah “perlindungan” dan “hukum” muncul bersamaan dalam frasa “perlindungan hukum.” Menurut Kamus Besar Bahasa Indonesia, kata “perlindungan” sendiri berarti dalam beberapa unsur salah satunya yakni melindungi yang memiliki makna menutupi, menjaga merawat dalam konteks memelihara dan menyelamatkan dalam bentuk memberi pertolongan serta diartikan membuat diri terlindung atau menggunakan sesuatu yang bertujuan untuk melindungi.<sup>17</sup> Tempat berlindung atau perbuatan atau tindakan untuk melindungi, seperti memberi perlindungan kepada individu yang lemah (rasa aman), merupakan definisi lain dari kata perlindungan yang terdapat dalam Kamus Besar Bahasa Indonesia. Kemudian, menurut Sudikno Mertokusumo, hukum adalah seperangkat aturan atau ketentuan yang bersifat umum dan normatif. Dalam konteks ini, hukum bersifat normatif karena menetapkan apa yang harus dilakukan, apa yang tidak boleh dilakukan, dan bagaimana cara menaati aturan tersebut. Hukum juga berlaku bagi setiap orang tanpa kecuali.

18

Menurut ilmu hukum, perlindungan adalah jenis layanan yang diperlukan dan dilakukan oleh personel keamanan atau penegak hukum dengan tujuan memberikan rasa aman secara fisik dan mental kepada korban

---

<sup>17</sup> Kamus Besar Bahasa Indonesia

<sup>18</sup> Harahap, T. K., Prayuti, Y., Latianingsih, N., Damanik, A., Maheni, T., Farida, I., Muhtar, M. H., & Mustaqim. (2023). PENGANTAR ILMU HUKUM. *Penerbit Tahta Media*. Retrieved from <http://tahtamedia.co.id/index.php/issj/article/view/255>

serta sanksi dari tindakan kejahatan yang berupa ancaman, terror, dan kekerasan dari siapapun dan dengan alasan apapun dimana sanksi ini disediakan sepanjang tahap penyidikan, diterima, dan telah sesuai dengan prosedur pemeriksaan di pengadilan. Proses perlindungan hukum harus dilaksanakan dari dua sumber: pertama, perlindungan hukum yang bersumber dari undang-undang, dan kedua, semua peraturan yang ditetapkan masyarakat, yaitu kesepakatan yang dibuat oleh masyarakat itu sendiri dengan tujuan mengatur perilaku anggota – anggota masyarakat serta mengatur hubungan perilaku antara masyarakat dan pemerintah yang dianggap mewakili masyarakat secara keseluruhan.

Beberapa ahli juga menyatakan bagaimana konsep atau definisi perlindungan hukum bagi masyarakat beberapa diantaranya yakni yang pertama Satjipto Perlindungan hukum, menurut Raharjo, adalah tindakan atau kegiatan yang memberikan perlindungan terhadap hak asasi manusia (HAM) yang dilanggar oleh orang lain. Perlindungan ini diberikan agar masyarakat dapat menikmati semua hak yang diberikan oleh hukum.<sup>19</sup>

Menurut Philipus M. Hadjon perlindungan hukum bagi masyarakat diartikan sebagai tindakan pemerintah yang sifatnya preventif dan represif. Preventif berarti rakyat memiliki kesempatan yang sama untuk mengajukan pendapat atau keberatan (*inspraak*) sebelum keputusan yang dibentuk oleh pemerintah memiliki kekuatan hukum yang sah dan mengikat. Sehingga perlindungan preventif dilakukan dalam upaya mencegah tercapainya

---

<sup>19</sup> Sinaulan, J. (2018). Perlindungan Hukum Terhadap Warga Masyarakat. *Ideas: Jurnal Pendidikan, Sosial, Dan Budaya*, 4(1). Hlm. 81

perdamaian. Meskipun perlindungan hukum yang represif memerlukan pembelaan diberikan setelah terjadinya sengketa, tujuan perlindungan represif yakni guna memulihkan dan menegakkan keadilan melalui pemberian sanksi kepada pihak yang melanggar (pelaku).<sup>20</sup>

Dalam konteks tindak pidana *doxing* perlindungan hukum diatur dalam beberapa peraturan yang mengatur mengenai tindak kejahatan dalam ranah elektronik, yang dapat dirumuskan sebagai berikut:

1. Undang – Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi (UU PDP)
2. Undang – Undang Nomo 1 Tahun 2024 tentang Informasi dan Transaksi Elektronik
3. Undang – Undang Nomor 19 Tahun 2016 tentang Perubahan Atas Undang – Undang Nomor 11 Tahun 2008 tentang informasi dah Transaksi Elektronik
4. Undang – Undang Nomor 23 tahun 2006 tentang Administrasi Kependudukan (UU Aminduk)
5. Peraturan Pemerintah Nomor 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik (PP PSTE)
6. Peraturan Menteri Kominfo Nomor 20 Tahun 2016 tentang Perlindungan Data Pribadi dalam Sistem Elektronik

---

<sup>20</sup> Ibid, hlm 81

## B. Tinjauan Umum Tindak Pidana

### 1. Penjelasan Umum Tindak Pidana

Pada dasarnya, tindak pidana akan selalu berjalan beriringan dengan hukum pidana kedua unsur ini bisa dirumuskan sebagai sebab akibat. Dimana Ketika ada tindak pidana maka pelaku dan pihak lain akan berhadapan dengan hukum pidana. Istilah hukum pidana berasal dari terjemahan bahasa Belanda “*strafrecht*”, yang dapat dibagi menjadi 2 suku kata, yaitu *Straf* yang berarti pidana dan *Recht* yang berarti hukum. Menurut Wirjono Prodjodikoro, istilah hukum pidana telah dipakai sejak penduduk Jepang di Indonesia untuk arti *strafrecht* dari bahasa Belanda, dan untuk membedakannya dengan istilah hukum perdata untuk arti *burgelijkrecht* dari bahasa Belanda.<sup>21</sup>

Dalam Kitab Undang – Undang Hukum Pidana (KUHP) istilah tindak pidana tidak dijelaskan secara langsung yang menyebutkan definisi dari tindak pidana. Istilah tindak pidana sendiri berasal dari terjemahan dari *stafbaarfeit*. Karena dalam KUHP tidak terdapat penjelasan mengenai istilah tersebut, maka biasanya tindak pidana disamakan dengan delik. Delik yang dalam Bahasa Latin yakni disebut *delictum* yang berarti “kesalahan” atau “pelanggaran”. Dalam hukum pidana kata “delik” dipergunakan untuk memberi Gambaran terhadap tindakan yang dilarang oleh hukum yang berlaku dan yang membawa hukuman.

---

<sup>21</sup> Dr. Tofik Yanuar Chandra, S.H., M.H, 2022, *HUKUM PIDANA*, PT. Sangir Multi Usaha, Jakarta, hlm. 19.

Kata tiga suku kata "strafbaatfeit" dalam bahasa Belanda mengacu pada tindakan criminal yakni yang pertama ialah straf yang dapat didefinisikan sebagai pidana dan hukuman, kemudian yang kedua ialah baar yang dimaksudkan sebagai boleh dan dapat, serta Yang terakhir namun tidak kalah pentingnya adalah feit, yang dapat menyiratkan aktivitas, perbuatan, peristiwa, atau pelanggaran.

Menurut Moeljatno, tindak pidana diartikan sebagai suatu perbuatan yang dilarang oleh suatu peraturan perundang-undangan, dan siapa saja yang tidak menaati larangan tersebut dapat diancam dengan pidana tertentu. Oleh karena itu, dapat dikatakan bahwa tindak pidana yang dikenal dengan istilah strafbaarfeit sering kali menggunakan kata delik dalam pengambilan keputusan tentang hukum pidana, sedangkan istilah pidana atau melakukan perbuatan pidana atau tindakan pidana digunakan dalam pembuatan undang-undangan guna mempermudah jalannya peraturan yang berlaku.

## **2. Unsur – Unsur Tindak Pidana**

Setelah memahami penjelasan mengenai beberapa definisi tindak pidana, maka pertanggungjawaban terhadap bentuk tindakan pidana dapat di proses apabila unsur – unsur atau syarat tindak pidana sudah terpenuhi. Tindak pidana atau perbuatan pidana hakekatnya diharuskan memenuhi unsur atau syarat sehingga tindakan tersebut dapat dikategorikan sebagai

tindakan pidana. Maka dengan itu syarat agar suatu perbuatan termasuk dalam tindakan pidana dapat dirumuskan sebagai berikut.<sup>22</sup>

- a. Diharuskan adanya suatu perbuatan, yakni suatu Tindakan atau peristiwa atau tindakan yang dilakukan oleh satu orang individu atau oleh beberapa (kelompok) individu;
- b. Persyaratan berikut harus dipenuhi perbuatan, tindakan, atau kejadian harus sesuai dengan hukum yang tertulis;
- c. perbuatan seseorang harus menunjukkan bahwa mereka telah melakukan "dosa" yang menjadi tanggung jawab mereka;
- d. perbuatan tersebut harus melanggar hukum;
- e. hukum tersebut harus memuat ancaman hukuman.

Simons menegaskan bahwa ada dua kategori faktor yang membentuk suatu tindak pidana: aspek objektif dan subjektif. Menurut Simons, perilaku manusia, hasil nyata dari perilaku tersebut, dan persepsi terhadap suatu keadaan tertentu merupakan komponen dari aspek objektif yang menyertai perbuatan tersebut seperti yang ada dalam Pasal 281 KUHP dimana dalam bunyinya terdapat openbar, atau "di depan umum". Simons melanjutkan dengan mengatakan bahwa ciri subjektif merujuk pada seseorang atau penjahat yang mampu membalas dendam atas pelanggaran (dollar atau culpa). Karena tindakan tersebut harus dilakukan secara tidak

---

<sup>22</sup> Apriani, T. (2019). Konsep Perbuatan Melawan Hukum Dalam Tindak Pidana. *Ganec Swara*, 13(1), 43-49.

benar, hal ini berkaitan dengan hasil tindakan atau situasi di mana tindakan tersebut dilakukan.

Menurut Moeljatno, suatu perbuatan pidana terdiri dari tiga unsur, yaitu perbuatan yang melanggar hukum (syarat materiil), perbuatan yang memenuhi syarat hukum (syarat formil), dan perbuatan yang manusiawi. Dengan demikian, dapat dirumuskan unsur-unsur menurut Moeljatno sebagai berikut:

- a. Perbuatan
- b. Yang dilarang (oleh aturan hukum)
- c. Ancaman pidana (bagi yang melanggar larangan)

Kemudian menurut Schravendijk, tindak pidana terdiri dari perilaku, kegiatan yang melawan hukum, ancaman hukuman tanpa hukuman yang nyata, dan tindakan yang dilakukan oleh orang yang dapat dimintai pertanggungjawaban atau yang melakukan kesalahan. Peraturan hukum hanya memperbolehkan dan melarang kegiatan yang dilakukan oleh manusia. Ancaman sanksi pidana menjadi contoh bahwa tidak semua tindakan benar-benar dihukum. Hukuman pidana yang dijatuhkan disini dapat dimaknai sebagai pada umumnya dijatuhi pidana. Kenyataannya, unsur yang telah dikemukakan oleh para ahli tidak berbeda jauh beberapa pendapat tersebut memiliki persamaan dimana dalam setiap pendapatnya tidak memisahkan antara unsur perbuatan dengan unsur mengenai orangnya.

Buku II KUHP memuat tentang pembentukan tindak pidana tertentu yang termasuk dalam golongan kejahatan, sedangkan Buku III memuat tentang pelanggaran. Demikianlah KUHP merumuskan tindak pidana. Dari definisi KUHP tentang kejahatan tertentu, terlihat bahwa ada 11 unsur tindak pidana, yaitu sebagai berikut:<sup>23</sup>

- a. Unsur tingkah laku
- b. Unsur melawan hukum
- c. Unsur kesalahan
- d. Unsur akibat konstitutif
- e. Unsur keadaan yang menyertai
- f. Unsur syarat tambahan untuk dapatnya dituntut pidana
- g. Unsur syarat tambahan untuk memperberat pidana
- h. Unsur syarat tambahan untuk dapatnya dipidana
- i. Objek unsur hukum tindak pidana
- j. Unsur kualitas subjek hukum pidana
- k. Unsur syarat tambahan untuk memperingan pidana

Sehingga jika ingin disimpulkan maka unsur tindak pidana tidak akan lepas dari apa yang menjadi perbuatan dan siapa yang melakukan perbuatan tersebut yang selanjutnya dapat bertanggungjawab, yang dimana perbuatan tersebut harus mengandung unsur kesalahan yang sudah dirumuskan dalam ketentuan hukum.

---

<sup>23</sup> Adami Chazawi, *Pelajaran Hukum Pidana 1*, (Jakarta: PT. Raja Grafindo, 2007), hlm. 82.

### C. Tinjauan Umum Tentang *Cyber crime*

*Cyber crime* adalah jenis kejahatan kontemporer baru yang menarik perhatian bahkan dari masyarakat global. Volodymyr Golubev menyebutnya sebagai *the new form of anti-social behavior*.<sup>24</sup> *Cyber crime* dianggap sebagai Salah satu aspek buruk teknologi yang sangat mempengaruhi era saat ini. The oxford reference online mendefinisikan *cyber crime as crime committed over the internet*.<sup>25</sup> Kedua pengertian tersebut memiliki hubungan yang sejalan yakni *cyber crime* yang dianggap sebagai bentuk anti sosial yang baru dapat memicu terjadinya kejahatan yang dilakukan melalui internet karena sikap individual yang tinggi.

Selanjutnya beberapa ahli juga mengemukakan pendapatnya mengenai definisi *cyber crime*, beberapa diantaranya yaitu Muladi, menurut Muladi *cyber crime* memiliki cakupan pengertian termasuk dalam tindak pidana yang pengaturannya tercantum dalam peraturan perundang-undangan pidana dan/atau Kitab Undang-Undang Hukum Pidana lainnya yang dimana tindak pidana tersebut menggunakan teknologi komputer sebagai komponen sentral. Selanjutnya menurut Roger Leroy Miller dan Gaylord A. Jentz mengemukakan bahwa *cyber crime* diartikan sebagai kejahatan dalam dunia maya yang kemudian karena lokasi dalam melakukan kejahatan tersebut maka

---

<sup>24</sup> Hadion Wijoyo et al., 2024, *CYBER CRIME*. PT. MAFY MEDIA LITERASI INDONESIA, Sumatera Barat, hal. 1.

<sup>25</sup> Ibid , hlm. 2.

selanjutnya menimbulkan masalah baru dalam penyelidikan dan penuntutan pelaku.

*Cyber crime* muncul sebagai akibat dari komunitas online di dunia maya, *cyber crime* juga memiliki karakteristik yang cukup unik dimana ini menyangkut dalam beberapa hal sebagai berikut:

- a. Luasnya tindak pidana
- b. Jenis tindak pidana
- c. Pelaku tindak pidana
- d. Modus tindak pidana
- e. Jenis kerugian yang diderita

Melalui karakteristik tersebut berdasarkan motif kegiatannya maka *cyber crime* dapat digolongkan dalam beberapa klasifikasi sebagai berikut:

- a. *Cyber crime* Sebagai Tindak Kejahatan Murni

Kejahatan siber murni disini maksudnya adalah kejahatan yang dilakukan hanyalah semata – mata menggunakan internet sebagai sarana kejahatan saja. Atau bisa diartikan bahwa dalam jenis ini teknologi computer dan internet dijadikan saran utama dalam melakukan tindak kejahatan. Biasanya tindak kejahatan ini mengincar keuntungan finansial atau kerusakan system. Contohnya yaitu *carding*, *ransomware*, dan *hacking*.

- b. *Cyber crime* Sebagai Tindak Kejahatan Abu – abu

Pada bagian ini kejahatan siber berada pada area “abu – abu” yang menjadikannya sulit untuk memastikan motivasi di balik perilaku

tersebut dan apakah itu merupakan tindakan criminal tersebut terkadang bukan ditujukan untuk kejahatan. Sebagai contoh yakni tindakan probing atau portscanning, ini merupakan sebutan guna mengumpulkan informasi melalui system yang dituju termasuk dalam sistem operasi yang digunakan. Probing ditujukan untuk memastikan kondisi jaringan sedangkan portscanning ditujukan untuk identifikasi port terbuka serta layanan yang sedang berjalan didalamnya. Sehingga karena keduanya dapat digunakan secara sah dalam konteks menjaga dan evaluasi keamanan, audit jaringan serta penanggulangan, kedua tindakan ini juga dapat memicu tindakan kriminal seperti kejahatan siber.

Selanjutnya yakni jenis *cyber crime* berdasarkan bentuknya dapat digolongkan kedalam dua golongan yakni sebagai berikut:

a. *Cyber crime* Langsung (*Direct Cyber crime*)

*Cyber crime* langsung didefinisikan sebagai suatu tindak kejahatan yang sepeuhnya dilakukan melalui sarana teknologi informasi dan komunikasi tanpa melibatkan kegiatan fisik secara langsung. Contohnya hacking, malware dan phising.

b. *Cyber crime* Tidak Langsung (*Indirect Cyber crime*)

Tindakan ini teknologi informasi hanya sebagai alat pendukung dalam memperluas kejahatan yang sudah ada di dunia nyata. Contohnya scam dan penipuan online, cyberstalking dan cyberbullying, hoaks dan online extortion.

Selanjutnya yakni jenis *cyber crime* berdasarkan sasaran digolongkan sebagai berikut:

a. Againsts Person

Kejahatan jenis ini menyasar orang-orang tertentu atau orang-orang yang memenuhi kriteria dan/atau ciri-ciri kejahatan. Jenis ini biasanya memiliki motif dendam. Contohnya pornografi, *Cyber-trespass* dan *cyberstalking*.

b. Againsts Property

Jenis ini biasa dikenal juga dengan sebutan *cyber crime* penyerangan hak milik: Jenis kejahatan ini dilakukan dengan tujuan mengganggu atau menyerang hak milik orang lain yang memiliki motif untuk menggandakan, mengubah serta memasarkan dengan tujuan guna kepentingan pribadi atau suatu kelompok tertentu ataupun demi keuntungan materi atau non materi. Contohnya seperti *carding*, *forgery data* dan *hijacking*. *Doxing* jenis ini sangat populer dalam dunia seni dikarenakan banyaknya isu – isu mengenai plagiarisme karya yang memicu munculnya *doxing*.

c. Against Government

Pemerintah dimanfaatkan sebagai alat dengan tujuan dalam kejahatan ini yang biasa digunakan adalah terror, kejahatan ini memiliki tujuan khusus yang dilayangkan kepada pemerintah guna mengacaukan sistem pemerintahan atau dampak paling buruknya yaitu dapat menghancurkan suatu negara. Contohnya yakni tindak kejahatan siber terrorism yang

menjadi tindakan mengancam yang melibatkan pembobolan situs web militer atau pemerintah resmi.

#### **D. Tinjauan Umum Tentang *Doxing***

Pada era digital teknologi yang semakin pesat pada saat ini begitu banyak memiliki banyak efek menguntungkan bagi kehidupan, termasuk membuat informasi lebih mudah diperoleh dengan jarak yang sangat jauh sekalipun. Namun pesatnya teknologi ini juga membawa dampak negatif apabila dalam penggunaannya digunakan dengan tidak bijak. Diantara dampak buruk yang bisa terjadi adalah kejahatan siber atau biasanya lebih dikenal dengan istilah *cyber crime*.

Arti kata *doxing* sendiri dalam Black Law Dictionary khususnya pelepasan informasi pribadi tanpa persetujuan untuk tujuan mengintimidasi seseorang, seperti alamat rumah, alamat email, gambar pribadi yang sensitif, riwayat medis, dan sebagainya (Garner, 2019).<sup>26</sup> Kejahatan siber memiliki banyak bentuk dan jenis diantara banyaknya kejahatan siber terdapat empat jenis kejahatan siber yang paling sering ditemukan, empat kejahatan tersebut adalah *phising*, peretasan, *cyberstalking* dan *cyberbullying*.

Perkembangan internet serta media sosial pada era digital seperti ini semakin mempermudah pelaku untuk memperoleh data melalui berbagai sumber, baik melalui digital seperti scraping dan phising maupun dengan memanfaatkan celah dari privasi yang ada dalam *platform* digital. *Doxing*

---

<sup>26</sup> Armando M. Arvy Chico dan Hari Soeskandi, 2023, PERTANGGUNGJAWABAN PIDANA BAGI PARA PELAKU *DOXING* MENURUT UU ITE DAN UU PDP, *Bureaucracy Journal : Indonesia Journal of Law and Social-Political Governance*, Vol. 3. Hlm. 561.

sekarang dianggap sebagai bagian dari fenomena kekerasan digital yang disebut dengan digital vigilantism. Digital Vigilantism termasuk dalam bentuk persekusi atau balas dendam oleh warga sipil melalui kegiatan publikasi data pribadi orang lain.

Namun, dikarenakan semakin berkembangnya digital teknologi maka timbul kejahatan siber jenis baru, salah satu kejahatan siber tersebut adalah *doxing*. *Doxing* mudahnya dipahami dalam definisi sebagai suatu tindakan menyebarkan data dan/atau informasi pribadi seseorang diluar izin dari pihak pemilik data yang bersangkutan dan disebarluaskan yang biasanya disebarluaskan melalui internet. Dalam banyak kasus, *doxing* menimbulkan efek domino seperti pelecehan melalui media sosial, perundungan massal (cyberbullying) hingga korban juga bisa mendapat ancaman fisik secara langsung.

*Doxer* atau pelaku *doxing* melakukan aktivitas *doxing*, yaitu dengan cara mengumpulkan informasi korban sebanyak-banyaknya seperti nama lengkap, tempat dan tanggal lahir, alamat, jenis kelamin, nomor telepon, nama anggota keluarga, dan lain-lain, lalu mempostingnya secara daring.<sup>27</sup> *Doxing* merupakan tindakan yang sangat merugikan korban, baik secara finansial, emosional, bahkan fisik, jika data dan informasi yang disebarluaskan sensitif

---

<sup>27</sup> Nadisa Pratiwi, Skripsi, “Persepsi Mengenai *Doxing* Di Media Sosial Twitter (Studi Deskriptif Kualitatif Pada Mahasiswa Pengguna Twitter di Indonesia)” Bandung: Universitas Pasundan, 2023, hlm. 1.

tentunya korban berpotensi menjadi sasaran bullying oleh netizen sehingga korban akan merasa malu, tertekan, dan stress.<sup>28</sup>

Selanjutnya menurut Professor Mary Anne Frank, mengemukakan bahwa *doxing* memiliki arti “*the definition of doxing is the publik release of an individual’s pri vate, sensitive, or personal information, such as home address, email address, phone number, social security number, and employer contact info, family member’s contact information, photos of the victim’s children and the school they attend*”.<sup>29</sup> Marry Anne Frank menjelaskan bahwa *doxing* merupakan suatu tindakan myebarluaskan informasi pribadi yang sifatnya sensitif dan/atau rahasia seseorang kepada publik tanpa izin. Informasi disini termasuk dalam alamat rumah, alamat e-mail, nomor telepon, informasi yang berkaitan dengan pekerjaan, anggota keluarga dan informasi anggota keluarga terdekat. Jika ditinjau melalui definisi ini maka *doxing* hanya kegiatan menyebarkan data tanpa ada ancaman yang berkelanjutan.

Tindak kejahatan *doxing* Di Indonesia diatur dalam Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi yang lebih jelas disebutkan dalam Pasal 65 Ayat (2) jo Pasal 67 Ayat (2) UU Perlindungan Data Pribadi menjelaskan bahwa setiap orang dilarang secara melawan hukum mengungkapkan data pribadi yang bukan miliknya (milik orang lain). Pasal ini mengungkap larangan mengungkapkan data pribadi milik orang lain. Yang

---

<sup>28</sup> Anissa Nur Fitriani, “5 Alasan Jangan Lakukan *Doxing* di Internet, Langgar Privasi!,” [https://www.idntimes.com/life/inspiration/annisa-nur-fitriani-1/doxing-di-internet-clc2?utm\\_source=whatsapp](https://www.idntimes.com/life/inspiration/annisa-nur-fitriani-1/doxing-di-internet-clc2?utm_source=whatsapp), diakses tanggal 29 April 2025 pk1. 19.55.

<sup>29</sup> Batuhan Kukul, 2023, Personal Data and Personal Safety : Re-Examining The Limits Of Publik Data In The Context Of *Doxing*, *International Data Privacy Law*, Vol.13, No. 3. Hlm. 183.

penting dalam frasa pasal ini yakni adanya frasa “melawan hukum” yang dapat diartikan penyebarluasan data pribadi orang lain ini harus berdampak negatif bagi korban dan dapat sangat merugikan meskipun dalam PDP tidak menjelaskan bagaimana perbedaan bentuk dan tujuan dari *doxing*.

Selanjutnya pengaturan mengenai *doxing* sendiri diatur dalam perundang-undangan yang berkaitan dengan transaksi dan informasi elektronik. Lebih khusus lagi, dalam Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik, Undang-Undang Nomor 1 Tahun 2024 tentang Perubahan Kedua. Pasal 27 ayat 4 Undang-Undang Nomor 11 Tahun 2008 jo Undang-Undang Nomor 19 Tahun 2016 mengatur tentang *doxing*, yaitu melarang seseorang membagikan informasi pribadi orang lain disertai konten tambahan yang mengandung ancaman.<sup>30</sup>

Selanjutnya *doxing* dalam pandangan hukum di Malaysia diatur dalam *Section 130(1) (a) PDPA (Personal Data Protection Act) 2010*, dalam pasal ini terdapat penjelasan mengenai larangan untuk mengungkapkan data pribadi yang dipegang oleh pengguna data. Dalam pasal ini terdapat unsur “tanpa persetujuan pengguna data”. Namun dalam PDPA Malaysia sendiri tidak ada penjelasan secara eksplisit mengenai bagaimana cara dari pelaku *doxing* memperoleh informasi.

Kemudian di negara Singapura aturan mengenai *doxing* diatur dalam PDPA 2012 mengenai Pengungkapan Data Pribadi tanpa Izin. Hal ini termuat dalam *section 48D (1)*. *Doxing* dalam pasal ini menjelaskan bahwa pelakunya

---

<sup>30</sup> Armando M. Arvy Chico dan Hari Soeskandi, *Op Cit.*, hal 563

adalah organisasi. Jika terjadi *disclosure data* yang dilakukan dengan cara tidak sah maka sanksi yang diberikan adalah pada *section 48* PDPA. *Disclosure data* merupakan pengungkapan data atau Tindakan membuka informasi kepada pihak lain baik secara sah maupun tidak sah. *Disclosure data* juga ada beberapa jenis yakni *voluntary disclosure*, *involuntary disclosure*, *legal disclosure* dan *accidental disclosure*. *Voluntary disclosure* atau pengungkapan sukarela merupakan kegiatan mengungkapkan data yang dilakukan atas izin pemilik data, contohnya seorang pengguna yang menyetujui syarat dan ketentuan suatu aplikasi.

Kemudian *involuntary disclosure* diartikan sebagai pengungkapan tidak sukarela maksudnya tindakan ini dilakukan tanpa sepengetahuan atau persetujuan pemilik data, tindakan ini seperti saat data dibocorkan oleh peretas (*data breach*). Selanjutnya *legal disclosure* yakni pengungkapan berdasarkan hukum dimana pada saat melakukan Tindakan ini harus didasarkan atas perintah hukum atau peraturan, seperti permintaan data yang digunakan dalam proses peradilan. Yang terakhir yakni *accidental disclosure* yang diartikan sebagai pengungkapan tidak sengaja yang berarti pengungkapan data murni disebabkan oleh kesalahan manusia atau sistem, misalnya seperti kesalahan dalam pengiriman e-mail atau system keamanan yang digunakan lemah.

Di Singapura selain pada PDPA yang sudah dijelaskan *doxing* juga dimuat dalam Protection Harasement Act 2014 (POHA) atau bisa disebut dengan Undang – Undang Perlindungan dari Pelecehan. *Doxing* lebih lanjut

diatur dalam section 3 (1) (c) POHA 2014 yang mengatur mengenai publikasi informasi identitas orang yang dapat menyebabkan orang mengalami pelecehan, kekhawatiran atau kesusahan.

Dalam peraturan ini disebutkan ada 3 jenis *doxing* yang pertama terdapat pada pasal 3 yang memuat mengenai tindakan mempublikasi data atau informasi pribadi yang mana Tindakan tersebut mengarah pada ranah pelecehan, kegelisahan, atau kesusahan yang menyebabkan orang mengalami pelecehan, kecemasan atau tekanan. Kemudian yang kedua paada pasal 5 *doxing* diartikan sebagai penyebaran data atau informasi yang menyebabkan korban merasa takut dikarenakan tindak kejahatan diikuti dengan ancaman kekerasan. Dan yang terakhir juga terdapat dalam pasal 5 dimana tindakan *doxing* dilakukan dengan tujuan memudahkan terjadinya kejahatan.

Tindak kejahatan *doxing* tentunya memiliki dampak yang sangat merugikan bagi korban, selanjutnya dampak *doxing* dapat dirumuskan sebagai berikut:

### **1. Dampak psikologis**

Tindak kejahatan *doxing* seringkali menimbulkan trauma, kecemasan, stress serta rasa takut yang berlebihan terhadap korban. Hal ini terjadi dikarenakan *doxing* seringkali dibarengi dengan adanya ancaman kekerasan dan/atau pelecehan yang mana hal ini membuat korban merasa tidak aman bahkan ketika ia berada dalam lingkungan pribadinya.

### **2. Dampak Sosial**

Kejahatan *doxing* juga dapat menyebabkan korban mengalami kerusakan reputasi, baik secara pribadi maupun profesional. Informasi atau data yang disebarluaskan terutama apabila *doxing* tersebut ditambah dengan informasi tambahan yang tidak sesuai fakta (hoaks) maka dengan hal ini dapat memicu perundungan, pengucilan sosial, dan bahkan memicu kekerasan fisik dari pihak yang terprovokasi.

### **3. Dampak Ekonomi dan Karier**

Penyebaran data pribadi atau tindakan *doxing* ini dapat berujung pada pemutusan hubungan kerja, kehilangan peluang bisnis bahkan kebangkrutan juga bisa saja terjadi. *Doxing* juga dapat membuat suatu perusahaan atau usaha kehilangan kepercayaan publik sehingga perusahaan tersebut mengalami penurunan pendapatan. Terutama pada era turunnya nilai mata uang menjadikan perekonomian menjadi lebih sensitif.

### **4. Dampak hukum**

Terjadinya tindak pidana *doxing* juga berhubungan dengan dampak secara hukum baik bagi pelaku maupun korban, kedua pihak sangat dimungkinkan untuk terlibat dalam proses hukum. Pihak korban dapat melaporkan pelaku atas pelanggaran privasi yang dilakukan pelaku. Sedangkan pelaku harus memenuhi panggilan ketika laporan sudah masuk dalam pengadilan.

Sehingga *doxing* disini dapat didefinisikan sebagai segala jenis tindakan menyebarluaskan data pribadi milik orang lain tanpa sepengetahuan

atau persetujuan pemiliknya, yang dapat menimbulkan kerugian materiil maupun non-materiil sebagai akibat dari perbuatan pemiliknya.

#### **E. Pengertian Data Pribadi**

Berdasarkan Pasal 1 ayat (1) Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi, data pribadi adalah setiap informasi yang dapat digunakan untuk mengidentifikasi seseorang, digunakan untuk mengidentifikasi seseorang secara terpisah, atau digabungkan dengan informasi lain yang dilakukan secara langsung atau tidak langsung melalui sistem informasi elektronik dan/atau nonelektronik.

*Doxing* juga berkaitan dengan Undang-undang ini mencakup ketentuan untuk perlindungan data pribadi diatur apa saja yang menjadi data pribadi yang kedepannya ada kemungkinan menjadi target tindak pidana *doxing*. Undang – undang mengenai perlindungan data pribadi diatur dalam Undang – Undang Nomor 27 Tahun 2022 Tentang Perlindungan Data Pribadi. Ruang lingkup UU PDP (undang – undang perlindungan data pribadi) mencakup dua sektor yaitu sektor privat dan sektor publik, dimana sektor privat mencakup perusahaan dan individu, baik sebagai badan hukum maupun non-hukum. Selain itu, mencakup pula pemerintah di sektor publik.

Dalam Undang – Undang PDP pasal 4 ayat (1) dirumuskan bahwa:

Data pribadi terdiri atas:

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

Yang selanjutnya diperluas jenisnya pada pasal 4 ayat (2) dan (3) yang berbunyi:

(2) Data Pribadi yang bersifat spesifik sebagaimana dimaksud pada ayat (1)

huruf a meliputi:

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

(3) Data Pribadi yang bersifat umum sebagaimana dimaksud pada ayat (1)

huruf b meliputi:

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

## **F. Perlindungan Data Pribadi Dalam Perspektif Islam**

Islam sebagai ajaran yang memuat ilmu – ilmu mengenai akidah ehidupan sudah telah lama menekankan betapa pentingnya privasi dan perlindungan data pribadi. Al-Quran dan Hadits memuat banyak hukum yang berkaitan dengan privasi; Banyak ayat menyatakan bahwa melindungi dan menjaga privasi seseorang tidak hanya benar secara moral tetapi juga dilindungi oleh hukum Islam.

Islam mengajarkan bahwa maqashid syariah mencakup perlindungan data pribadi. Tujuan syariah, yang dikenal sebagai maqashid syariah, adalah untuk menjaga harta, keturunan, jiwa, akal, dan agama. Dalam pandangan ini data pribadi dianggap sebagai bagian dari hifdzul ‘irdh (perawatan kehormatan) dan hifdzul mal (perawatan harta). Berhubungan dengan *doxing* yakni apabila penyalahgunaan atau kebocoran data pribadi sangat bertentangan dengan prinsip – prinsip syariah.

Prinsip – prinsip syariah yang dimaksud disini yakni yang pertama Hifdzul ‘Irdh yang diartikan sebagai menjaga kehormatan, maksudnya yakni pada saat ada data pribadi yang bocor lalu digunakan untuk melakukan tidak pidana pencemaran nama baik, fitnah atau manipulasi opini publik, sebagai warga muslim perlu mengingat untuk selalu menjaga kehormatan seseorang supaya tidak merugikan atau dirugikan terhadap orang lain.

Yang kedua yaitu Hifdzun Nafs yang diartikan sebagai menjaga jiwa, hal ini berhubungan dengan *doxing* karena apabila Islam mengajarkan bahwa memastikan keselamatan hidup adalah hak mendasar yang harus dijunjung

tinggi, karena informasi pribadi dapat menimbulkan risiko fisik dan psikologis.

Selanjutnya yang ketiga ada yang disebut Hifdzul Mal atau bisa dikatakan sebagai menjaga harta, dalam tindak kejahatan *doxing* hal ini menjerumus pada informasi keuangan yang dicuri yang dimaksudkan untuk digunakan dalam transaksi daring guna melakukan kejahatan seperti pencurian identitas, peretasan akun, dan/atau skimming. Menurut ajaran Islam, harta benda harus dilindungi dari tindakan yang merugikan seperti pencurian dan kecelakaan, sehingga tidak seharusnya data apapun yang berhubungan dengan transaksi online disebarluaskan tanpa persetujuan pihak yang memiliki data.

Dalam Islam, sebagai umat muslim memiliki sifat Amanah adalah kewajiban moral. Salah satu hadits menjelaskan bahwa Barangsiapa tidak mempunyai kualitas keandalan, maka ia tidak dapat beriman, dan barangsiapa tidak dapat memenuhi komitmennya, maka ia tidak dapat beragama. Hal ini berkaitan mengenai bagaimana kita sebagai seorang muslim mampu menjaga privasi atau dalam konteks ini yakni data pribadi seorang muslim lain sehingga tidak terjadi hal yang tidak diinginkan dikemudian hari. Hadits ini juga mempertegas bahwa seseorang yang sudah diberi kewenangan untuk mengelola atau diberi akses untuk membuka data tersebut harus mampu menjaga dan tidak boleh menyalahgunakannya.

Selanjutnya dijelaskan dalam Al-Quran Surah An-Nur yang menjelaskan mengenai perlindungan privasi yang berbunyi:

لَعَلَّكُمْ لَكُمْ خَيْرٌ ذَلِكَمْ أَهْلِيهَا عَلَىٰ وَتُسَلِّمُوا تَسْلِيمًا حَتَّىٰ بُيُوتِكُمْ غَيْرَ بِيُوتِنَا تَدْخُلُوا لَا أَمْنُوا الَّذِينَ يَأْتِيهَا

○ ٢٧ تَذَكَّرُونَ

Artinya : *Hai orang-orang yang beriman, janganlah sekali-kali memasuki rumah orang lain kecuali meminta izin terlebih dahulu dan mengucapkan salam kepada penghuninya. Karena itu, lebih bijaksana bagimu untuk menempuh pendidikan. (QS An-Nur [24]:27).*<sup>31</sup>

Seorang ahli tafsir yang bernama Ibnu Asyur menjelaskan dalam tafsirannya bahwa rumah dapat dimaksudkan sebagai tempat paling pribadi bagi seseorang. Pada ayat tersebut menjelaskan bahwa muslim tidak bisa memasuki "rumah" orang lain tanpa persetujuan mereka, hal ini berhubungan dengan data pribadi atau hal apapun yang sifatnya pribadi tidak boleh diakses atau digunakan tanpa atas izin pemiliknya.

Selain itu ada hadits yang membahas mengenai perlindungan rahasia dan informasi pribadi salah satu hadits tersebut yakni sebagai berikut:

إِلَىٰ فَبِعَنِّي عَلَيْنَا فَسَلَّمَ قَالَ الْعُلَمَانُ مَعَ الْعَبِّ وَأَنَا وَسَلَّمْ عَلَيْهِ اللَّهُ صَلَّى اللَّهُ رَسُولُ عَلِيٍّ أَتَىٰ قَالَ أَنَسٌ عَنْ  
لِحَاجَةٍ وَسَلَّمْ عَلَيْهِ اللَّهُ صَلَّى اللَّهُ رَسُولُ بَعَثَنِي قُلْتُ سَكَحَبَ مَا قَالَتْ جِئْتُ فَلَمَّا أُمِّي عَلَىٰ فَأَبْطَأْتُ حَاجَةً  
لَوْ وَاللَّهِ أَنَسٌ قَالَ أَحَدًا وَسَلَّمْ عَلَيْهِ اللَّهُ صَلَّى اللَّهُ رَسُولُ بِسِرِّ تُحَدِّثَنَّ لَا قَالَتْ سِرٌّ إِنَّهَا قُلْتُ حَاجَتُهُ مَا قَالَتْ  
تَأْبِتُ يَا لِحَدَّثْتُكَ أَحَدًا بِهِ حَدَّثْتُ

Artinya : Menurut Anas bin Malik, ia pernah diutus oleh Rasulullah SAW untuk mengemban suatu misi. Menanggapi pertanyaan ibunya mengenai misi tersebut, Anas berkata, "Itu rahasia." Kemudian

<sup>31</sup> <https://quran.nu.or.id/an-nur/27> diakses 6 mei 2025 pkl 22.15

ibunya memohon, "Jangan kau ungkapkan kepada siapa pun rahasia Rasulullah SAW." (HR Muslim no. 4533).<sup>32</sup>

Penafsiran hadits tersebut menunjukkan bahwa ilmu pengetahuan itu terpelihara bagi umat muslim merupakan amanah yang harus dijaga, terutama pada era digital seperti sekarang, informasi yang bersifat pribadi dan/atau sensitif seperti nomor ktp atau alamat hingga riwayat transaksi sebaik – baiknya disimpan untuk diri sendiri atau dirahasiakan dengan tujuan tidak terjadi penyalahgunaan data oleh pihak yang tidak bertanggungjawab.

### **BAB III**

#### **HASIL PENELITIAN DAN PEMBAHASAN**

##### **A. Perlindungan Hukum Bagi Korban *Doxing* Sebagai Pencegahan Kebocoran Data**

###### **1. Perlindungan Hukum Bagi Korban *Doxing***

Hukum mempunyai fungsi sebagai pelindung dalam kepentingan manusia dalam bermasyarakat dan bernegara, hal tersebut ditujukan supaya kepentingan masyarakat terlindungi, yang perlu diingat yakni hukum harus dilaksanakan secara professional dan dilaksanakan menurut ketentuan yang sudah ditetapkan dan disepakati. Pelaksanaan hukum harus dilaksanakan dengan normal (sebagaimana mestinya), damai seta tertib. Adanya perlindungan hukum rasanya diperlukan masyarakat dikarenakan sangat penting dan secara signifikan mempengaruhi keadilan bagi masyarakat secara keseluruhan.

---

<sup>32</sup> Anonym, "Menjaga Data Pribadi dalam Perspektif Islam: Prinsip dan Tindakan",

Dalam era digital yang sangat berkembang pesat, penyebaran informasi dan data pribadi tanpa izin pemilik data melalui media elektronik yang biasa dikenal dengan istilah *doxing*. *Doxing* dianggap sebagai ancaman yang cukup serius terhadap privasi seseorang. *Doxing* tidak hanya sekedar kegiatan semata – mata membuka identitas seseorang tetapi dapat memicu berbagai bentuk ancaman dan tindak kejahatan lainnya seperti intimidasi, pelecehan hingga kekerasan secara fisik.

Tindak kejahatan ini biasanya berbasis online atau daring melalui media sosial, hal ini menyebabkan penyebaran informasi berlangsung sangat cepat dengan cakupan yang cukup luas. Selain itu beberapa pengguna media sosial juga tidak sering yang sadar bahwa mereka sedang melakukan tindak pidana kejahatan siber dalam bentuk *doxing*. Dalam permasalahan ini maka dapat memunculkan masalah yang berkelanjutan bagi korban. Karena penderita dapat menderita kerugian materiil disamping kerugian immateriil.

Kerugian immaterial korban *doxing* sangat jelas dimana korban merasakan penderitaan karena data yang bocor diluar kendalinya. Hal tersebut menyebabkan beberapa pihak dengan mudah mengakses datanya dan dapat digunakan oleh orang lain secara bebas.

Sedangkan kerugian korban secara materiil dapat berupa kehilangan pekerjaan yang kemudian korban menjadi kehilangan penghasilannya. Oleh karena itu tindak pidana *doxing* perlu dikaji lebih lanjut mengenai bagaimana perlindungan hukum bagi korbannya. Yang

menjadi titik fokusnya yakni karena semua korban kejahatan atau korban tindak pidana berhak atas perlindungan hukumnya atau semua orang berhak mendapatkan perlindungan hukum.

Kemajuan teknologi informasi yang pesat telah mengakibatkan banyaknya pergantian pola hidup dalam keseharian manusia dalam berbagai aspek yang terjadi secara langsung sudah mempengaruhi munculnya jenis – jenis perbuatan hukum yang belum pernah terjadi sebelumnya, pemakaian dan pengaplikasian teknologi informasi memicu banyak tindak kejahatan siber. Setelah memahami bagaimana konsep mengenai *doxing* yang menjadi fokus selanjutnya adalahh apa saja kemungkinan yang dapat terjadi jika *doxing* terjadi pada seseorang.

*Doxing* dalam beberapa tahun menduduki peringkat yang cukup tinggi dalam konteks banyaknya jumlah kasus yang terjadi. Beberapa kemungkinan pada korban *doxing* juga beragam salah satunya korban *doxing* dapat seringkali mendapat ancaman dengan dibarengi oleh tindakan *doxing* oleh pelaku. Pada beberapa kasus *doxing* yang terjadi yang menjadi latar belakang atau alasan pelaku melakukan hal tersebut terkesan tidak begitu jauh yakni adanya perbedaan pendapat terhadap suatu unggahan pada *platform* media online atau media sosial.

Pada tahun 2024 diketahui jumlah Di Indonesia, sekitar 220 juta orang memanfaatkan media sosial. aktif dalam penggunaan media sosial, angka ini tentu saja tergolong banyak dan tinggi. Angka tersebut menunjukkan bahwa media sosial dalam penggunaanya sangat signifikan di

kalangan masyarakat Indonesia. Kelompok pengguna *platform* digital berdasarkan usianya tercatat pada beberapa kelompok. Kelompok usia 18 hingga 34 tahun sangat mendominasi penggunaan media sosial yang jika diubah dalam persentase angka presentasinya sebesar 65% dari total pengguna. Selanjutnya Perempuan dalam kurun usia 18 hingga 34 tahun tercatat lebih aktif menggunakan sosial media jika dibandingkan laki – laki, terutama pada penggunaan media sosial di *platform* seperti Instagram dan TikTok.

Selanjutnya *platform* yang paling sering digunakan oleh pengguna di Indonesia yakni aplikasi WhatsApp dengan angka presentase 90,9% dengan kelompok usia pengguna di kisaran 16 hingga 64 tahun yang menggunakan aplikasi tersebut setiap bulannya. Selanjutnya diikuti oleh Instagram dengan angka persentase 85,3% dan Facebook menyusul dengan angka persentase 81,6%. Pada era sekarang TikTok mengalami pertumbuhan yang sangat pesat, dengan jumlah pengguna mencapai angka 157,6 juta pengguna pada juli 2024, dengan adanya hal ini menjadikan Indonesia menjadi negara dengan jumlah pengguna TikTok terbesar di dunia.

Dengan angka pengguna internet yang sangat tinggi seperti yang sudah tertera dengan ini maka media sosial bukan hanya sekedar menjadi wadah untuk saling berinteraksi namun juga sebagai wadah untuk mendapat informasi yang terkadang keaslian dan keabsahannya masih perlu dipertanyakan. Melalui tingginya angka persentase pengguna media

sosial juga dapat memicu terjadinya kejahatan siber seperti *doxing*. Meskipun kegunaan penggunaan internet untuk transaksi elektronik sangat besar karena cepat dan mudah, belum lagi kompleksitas dalam melakukan hubungan global yang dengan menggunakan internet bisa dilakukan tanpa adanya batasan lokasi dan waktu. Meskipun begitu tidak menutup kemungkinan bahwa *doxing* akan tetap ada.

*Doxing* berasal dari kata “dox” yang merupakan sinonim dari “documents” yang merujuk pada kegiatan mengumpulkan dan selanjutnya menyebarkan informasi seseorang yang dilakukan secara daring dan tanpa seizin pemilik informasi tersebut. Informasi yang dibagikan biasanya berupa informasi yang sensitif dan sifatnya pribadi seperti nama lengkap, alamat, nomor telepon, id personal, foto hingga data keluarga hingga data orang – orang terdekat dari korban.

Tujuan pelaku *doxing* atau yang biasa disebut doxer melakukan *doxing* juga sangat beragam salah satunya yakni doxer melakukan tindak kejahatan untuk merusak reputasi korban, melakukan intimidasi dan bahkan *doxing* juga dapat ditujukan untuk melakukan ancaman fisik yang ditujukan kepada individu dan/atau orang – orang terdekat individu tersebut yang menjadi target.

Selain memiliki tujuan yang tidak baik doxer dalam menjalankan aksinya juga memiliki motivasi yang sangat beragam. Beberapa diantara mereka melakukan *doxing* dengan motivasi untuk balas dendam terhadap individu yang ditargetkan dengan alasan adanya perbedaan pendapat.

Selain itu kejahatan dalam bentuk *doxing* ini juga dipergunakan untuk tujuan intimidasi. Pemerasan atau hanya sekedar merusak reputasi atau personal branding target tersebut di dunia maya. Fenomena seperti ini sering terjadi pada komunitas daring (dilakukan melalui internet) yang menjadikan pelaku untuk tetap bersifat anonym sehingga korban menjadi lebih mudah untuk ditargetkan pada serangan tersebut.

Menurut data yang disajikan oleh SAFEnet dalam periode 2017 – 2020 angka pada kasus *doxing* terus meningkat, meningkatnya angka kasus *doxing* seperti ini tentu saja harus menjadi perhatian terlebih lagi pada tahun 2020 merupakan jumlah terbanyak dalam periode 2017 – 2020. Bahkan sebagaimana kita ketahui pada tahun 2020 Indonesia dilanda virus Covid-19 namun ditengah menyebarkan virus tersebut *doxing* kembali menjumpai beberapa aktivis dan jurnalis.

Pada 6 Januari 2020 editor Kompas.com yang bernama Jessi Carina menjadi korban *doxing*. Ia dikaitkan dengan pemberitaan pada hari sebelumnya yang dimuat dalam Kompas.com dengan judul “Anies Kerja Bakti Saat Hujan di Kelurahan Makassar, Warga: gubernur DKI Rasa Presiden”. Pada kasus yang menimpa Jessi *doxing* yang dilakukan pelaku yakni diunggahkannya foto pernikahan Jessi yang disandingkan dengan potongan dari berita tersebut. Terjadinya *doxing* pada jurnalis Kompas.com ini di latar belakang karena adanya perbedaan kubu pendukung antara yang disebutkan dalam pemberitaan dengan presiden yang saat itu menjabat yakni Joko Widodo.

Selanjutnya pada 26 Mei 2020 *doxing* menimpa seorang jurnalis Detik.com yang bernama Isal Mawardi. Data pribadi jurnalis tersebut tersebar yang disertai dengan opini menyerang jurnalis tersebut. Serangan tersebut menurut keterangan yang ada berawal Ketika sang jurnalis menuliskan suatu tulisan mengenai rencana Joko Widodo yang disebutkan akan membangun sebuah mal di sekitar wilayah Bekasi di Tengah pandemi Covid-19. Dalam kasus Isal ia juga mendapatkan ancaman berupa pembunuhan yang didapatkan melalui WhatsApp. Yang bersangkutan bahkan didatangi oleh banyak ojek online yang membawa makanan yang isal sendiri mengaku tidak melakukan pemesanan. Kasus Isal berlanjut hingga salah satu pelaku *doxing* tertangkap. Pelaku tersebut mengunggah beberapa hasil ttangkapan layer yang dijadikan jejak digital oleh pelaku untuk kemudia dicari kesalahannya, yang membuat geram yakni kesalahan yang dicari oleh pelaku tidak ada hubungannya dengan berita yang sedang dipersoalkan.

Kasus selanjutnya juga menimpa seorang jurnalis yang berasal dari liputan6.com yang bernama Cakrayuri Nuralam. Kasus ini terjadi pada 11 September 2020 korban menyadari ia sedang menjadi sasaran *doxing* melalui beberapa akun Instagram yang mencantumkan tautan yang mana tautan tersebut ketika di akses maka akan diarahkan kepada alamat rumah, foto keluarga bahkan termasuk foto jurnalis ketika yang bersangkutan masih bayi. Lata belakang dari kasus ini yaitu terpublikasinya Penegasan bahwa Arteria Dahlan, politikus PDI

Perjuangan, adalah cucu Bachtaroeddin, pendiri PKI di Sumatera Barat, diperkuat oleh artikel periksa fakta ini.

Melalui data mengenai beberapa kasus *doxing* di Indonesia maka penerapan dalam perlindungan hukum yang terhadap korban *doxing* harus dipahami. Ketika seseorang mengalami atau menjadi korban *doxing* apa yang harus mereka lakukan, dengan begitu masyarakat harus mengetahui pengaturan mengenai *doxing* di Indonesia seperti apa terutama perlindungannya kepada korban yang sesuai dengan Undang – undang Nomor 1 Tahun 2024 tentang Perubahan Kedua Atas Undang – undang Nomor 8 Tahun 2011.

Banyaknya kejahatan di media sosial membuat pemerintah yang pada akhirnya melahirkan peraturan guna mengikat masyarakat untuk tidak melakukan kejahatan di era digital teknologi. Peraturan ini juga dirumuskan sebagai bentuk perlindungan terhadap masyarakat. Pengaturan mengenai *doxing* sendiri diatur dalam Undang-Undang Informasi dan Transaksi Elektronik. Lebih khusus lagi, Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik sebagaimana telah diubah dengan Undang-Undang Nomor 1 Tahun 2024 tentang Perubahan Kedua.

*Doxing* Berdasarkan Undang-Undang No. 19 Tahun 2016 dan Pasal 27 ayat 4 Undang-Undang No. 11 Tahun 2008, dilarang bagi siapa pun untuk membagikan informasi pribadi orang lain beserta konten

tambahan yang membahayakan.<sup>33</sup> Dalam pasal tersebut yang dimaksud dengan mendistribusikan yakni ketika data informasi tersebut dikirimkan dan/atau disebarakan kepada banyak individu atau pihak, yang dilakukan melalui sistem elektronik.

Unsur didalam pasal 27 yang dianggap sebagai kesalahan (kejahatan *doxing*) yakni sebagai berikut:

- a. Setiap orang
- b. Melawan hukum
- c. Mendistribusikan dokumen elektronik
- d. Berisi muatan ancaman

Pasal 27 tersebut memunculkan uraian baru yang tertulis dalam pasal 27 ayat (3) Undang – undang Nomor 19 Tahun 2016 yang dirumuskan sebagai berikut:

- a. Setiap orang
- b. Melawan hukum
- c. Menyerang kehormatan seseorang
- d. Menuduhkan sesuatu untuk diketahui umum
- e. Dalam bentuk elektronik dan/atau dokumen elektronik
- f. Dilakukan secara sistem elektronik

Pengaturan perbuatan *doxing* selain diatur dalam dalam Pernyataan “setiap penggunaan informasi yang dilakukan melalui media elektronik mengenai data pribadi seseorang harus dilakukan dengan persetujuan

---

<sup>33</sup> Armando M. Arvy Chico dan Hari Soeskandi, *Op Cit.*, hal 563

orang atau pihak yang bersangkutan” ditegaskan dalam Pasal 26 ayat (1) UU ITE. UU ITE telah mengatur perilaku apa saja yang termasuk dalam lingkup tindak pidana di bidang ITE, serta bagaimana perilaku tersebut didefinisikan sebagai perbuatan jahat dan bagaimana perilaku tersebut menyerang berbagai kepentingan hukum melalui rumusan delik pidana tertentu.

Juga diatur dalam peraturan lain mengenai perlindungan korban khususnya dalam kasus tindak pidana *doxing* dapat ditemukan dalam Pelepasan dan akses tidak sah terhadap informasi pribadi diatur dalam Undang-Undang Nomor 19 Tahun 2016 tentang Informasi dan Transaksi Elektronik (ITE) yang secara rinci diatur dalam Pasal 27 ayat (1) dan Pasal 32 ayat (2). Selain itu, perlindungan bagi korban kejahatan digital dapat dibuka melalui Peraturan Komisi Informasi dan dengan bantuan Lembaga Perlindungan Saksi dan Korban (LPSK).

Sesuai dengan Undang-Undang Nomor 31 Tahun 2014 tentang Perubahan Atas Undang-Undang Nomor 13 Tahun 2006 tentang Perlindungan Saksi dan Korban yang tercantum dalam Pasal 5 ayat (1), korban dan saksi mempunyai hak-hak sebagai berikut dalam situasi tertentu dan ketika membahayakan untuk terhindar dari kejahatan teknologi:

- a. dilindungi dari ancaman terhadap barang bukti yang telah, akan, atau sedang diajukan, dan memperoleh perlindungan terhadap keselamatan pribadi, keluarga, dan harta bendanya

- b. ikut serta dalam memilih dan memutuskan jenis bantuan keamanan dan perlindungan;
- c. memberikan keterangan secara bebas;
- d. diberi penerjemah; bebas dari pertanyaan yang menjerat;
- e. mendapat informasi perkembangan kasus; mengenai
- f. mendapat informasi mengenai putusan pengadilan;
- g. mendapat informasi dalam hal terpidana dibebaskan;
- h. dirahasiakan identitasnya;
- i. mendapat identitas baru;
- j. mendapat tempat kediaman sementara;
- k. mendapat tempat kediaman baru;
- l. memperoleh penggantian biaya transportasi sesuai dengan kebutuhan;
- m. mendapat nasihat hukum;
- n. memperoleh bantuan biaya hidup sementara sampai batas waktu perlindungan berakhir; dan/atau
- o. mendapat pendampingan.

Dalam Undang – Undang ITE dirumuskan dalam pasal 26 ayat (1) dan (2) mengenai bahwa adanya larangan mengenai penyebaran informasi elektronik milik pihak lain baik disengaja maupun tidak disengaja Dapat membahayakan orang lain. Hukuman bagi pelaku atau doxer dapat berupa denda paling banyak Rp. 750.000.000,00 (tujuh ratus lima puluh juta rupiah) atau pidana penjara paling lama 4 (empat) tahun. Pasal 45B mengatur hal ini namun pada pasal ini unsur kesalahan yang sesuai yakni

pada pasal 29 yang mana *doxing* juga disertai dengan ancaman kekerasan dan/atau menakut-nakuti.

Selain daripada pengaturan mengenai penyebaran data seperti apa yang disebutkan dalam Pasal 26 ayat (1), pasal ini juga secara tidak langsung memberikan hak kepada korban untuk melakukan pengajuan gugatan atas kerugian yang dialaminya akibat penyalahgunaan data pribadi mereka sebagai korban. Hal tersebut menunjukkan bahwa Undang – Undang ITE bukan hanya menjadi wadah untuk mengatur sanksi pidana, melainkan juga sebagai ruang untuk korban dalam memperoleh ganti rugi secara hukum.

Maknanya dalam perbaikan atau revisi atau perubahan undang – undang ITE tersebut telah dipersempit hal ini akhirnya mempermudah kriminalitas pelaku *doxing*; peraturan ini pernah merujuk pada Kitab Undang-Undang Hukum Pidana. Jika tindakan tersebut melibatkan kekerasan atau ancaman, pelaku *doxing* dapat menghadapi hukuman pidana. Misalnya, jika *doxing* dilakukan dengan disertai ancaman fisik di dunia nyata, pelaku dapat dikenakan Pasal 482 Kitab Undang-Undang Hukum Pidana (UU Nomor 1 Tahun 2023), yang menyatakan bahwa ancaman kekerasan memiliki ancaman hukuman maksimal 9 (sembilan) tahun penjara.

*Doxing* dapat berhubungan pula dengan KUHP pada Pasal 513 yang berbunyi: “Barangsiapa Menggunakan atau membiarkan digunakannya barang milik orang lain yang berada dalam penguasaannya

karena hubungan kerja atau profesinya untuk keperluan lain daripada keperluan pemiliknya, dipidana dengan pidana kurungan paling lama enam hari atau denda paling banyak Rp25.000.000.000,00 (dua puluh lima rupiah)”.<sup>34</sup> Maka dengan itu semua orang dilarang untuk menggunakan barang yang termasuk didalamnya informasi pribadi dengan alasan apapun dan tanpa persetujuan pihak yang bersangkutan, sehingga pelaku *doxing* dapat dikenakan hukuman melalui unsur undang – undang ITE maupun KUHP.

Agar data tersebut tampak nyata, UU ITE juga mengatur tentang pembuatan, perubahan, penghapusan, dan pemusnahan dokumen dan/atau informasi elektronik. Pasal 35 UU ITE mengatur hal tersebut. Dalam konteks *doxing* hal ini berhubungan dengan tindakan pelaku yang mengunggah data pribadi korban dimana seolah – olah korban sendiri yang mengunggahnya melalui akun sosial media lain. Sanksi dalam unsur pasal 35 diperjelas Sesuai dengan Pasal 51 ayat (1), setiap orang yang memenuhi persyaratan sebagaimana dimaksud dalam Pasal 35 dipidana dengan pidana penjara paling lama 12 tahun dan/atau denda paling banyak Rp12.000.000.000,00 (dua belas miliar rupiah).

Peraturan perlindungan data pribadi tahun 2022 yang kemudian dituangkan dalam Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi, semakin meningkatkan perlindungan bagi korban permasalahan terkait data pribadi. Setiap orang yang dengan

---

<sup>34</sup> Prof. Moeljatno, S.H., 2018, *KITAB UNDANG – UNDANG HUKUM PIDANA*, PT. Bumi Aksara, Jakarta, hal. 186.

sengaja dan melawan hukum memperoleh atau mengumpulkan data pribadi yang bukan miliknya dengan maksud dan tujuan menguntungkan diri sendiri atau pihak lain, dan akibatnya menimbulkan kerugian bagi korban atau subjek data pribadi yang diambil, diancam dengan pidana penjara paling lama lima tahun dan/atau denda paling banyak Rp5.000.000.000,00 (lima miliar rupiah), sesuai Pasal 67 ayat (1) UU PDP.

Pemberat pidana terhadap pelaku *doxing* dapat dikenakan apabila tindakan tersebut memuat kekerasan atau ancaman, sebagai contoh ketika pelaku melakukan *doxing* yang kemudian disertai ancaman secara fisik didunia nyata maka pelaku bisa dikenakan pasal 482 KUHP (Undang – Undang Nomor 1 Tahun 2023) yang menjelaskan bahwa adanya ancaman dengan kekerasan bagi pelakunya akan dipidana penjara paling lama 9 (sembilan) tahun. Maknanya dalam perbaikan atau revisi atau perubahan undang – undang ITE tersebut telah dipersempit hal ini akhirnya mempermudah pembedaan bagi pelaku *doxing* yang sebelumnya undang – undang ini merujuk kepada KUHP.

*Doxing* juga berkaitan dengan undang – undang perlindungan data pribadi yang mana pada undang – undang ini diatur apa saja yang menjadi data pribadi yang kedepannya ada kemungkinan untuk menjadi target tindak pidana *doxing*. Undang – undang mengenai perlindungan data pribadi diatur dalam Undang – Undang Nomor 27 Tahun 2022 Tentang Perlindungan Data Pribadi. Ruang lingkup UU PDP (undang – undang

perlindungan data pribadi) mencakup dua sektor yaitu sektor privat dan sektor publik, dimana sektor privat mencakup perusahaan dan individu, baik sebagai badan hukum maupun non-hukum. Selain itu, mencakup pula pemerintah di sektor publik.

Menurut Pasal 4 ayat (1) UU Perlindungan Data Pribadi, terdapat dua kategori data pribadi, yaitu data pribadi khusus dan data pribadi umum. Kemudian, ayat (2) lebih jelas menyebutkan bahwa data pribadi khusus meliputi informasi tentang kesehatan, biometrik, genetika, riwayat kriminal, anak, informasi pribadi, dan/atau data lain yang sesuai dengan ketentuan perundang-undangan. Selanjutnya, informasi pribadi umum selanjutnya diperjelas dalam ayat (3) yang menjelaskan bahwa Nama lengkap, jenis kelamin, kewarganegaraan, agama, status perkawinan, dan/atau informasi pribadi lainnya yang, jika digabungkan, dapat digunakan untuk mengidentifikasi seseorang adalah contoh data pribadi umum.

Pelaku doxing dapat dikenakan hukuman pidana berdasarkan Pasal XIV KETENTUAN PIDANA UU PDP, khususnya Pasal 67 ayat 1 dan 2. Orang yang mengumpulkan informasi pribadi orang lain dan membocorkan informasi yang bukan miliknya disebut sebagai pelaku dalam pasal ini. Definisi kalimat ini adalah *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.<sup>35</sup>

Sehingga dengan begini sanksi yang diberikan pada pelaku *doxing* menurut peraturannya harus disesuaikan dengan apa yang menyertai tindakan *doxing* tersebut, apakah *doxing* disertai dengan muatan ancaman, atautkah *doxing* disertai dengan muatan yang melanggar asusila, atau *doxing* yang disertai dengan muatan perjudian, kemudian bisa juga dikarenakan *doxing* dilakukan dengan muatan penghinaan dan/atau pencemaran nama baik bahkan *doxing* disertai dengan muatan pemerasan atau pengancaman.

## **2. Perlindungan Hukum Korban *Doxing* Sebagai Pencegahan Kebocoran Data Pribadi**

Dalam penegakkan hukum aparat hukum termasuk didalamnya polisi menjadi faktor penentu dalam keberhasilan penegakan hukum. Maka dari itu setiap tahapan dalam proses penegakan hukum harus dilaksanakan sebaik – baiknya bagaimana dan sesuai dengan peraturan yang sudah ditetapkan. Aparat negara harus menjalankan tugasnya sesuai dengan ketentuan dan peraturan yang sedang berlaku yang mana hal tersebut bertujuan untuk mewujudkan tujuan hukum.

Sedangkan polisi berperan sebagai penegak keadilan hukum dan pelayan masyarakat yang mana dalam posisi seperti ini diharuskan

---

<sup>35</sup> Armando M. Arvy Chico dan Hari Soeskandi, *Op Cit.*, hal 566-567.

menghormati hukum dan HAM (Hak Asasi Manusia) serta sebagai penegak hukum harus taat pada kode etik profesi mereka. Namun terkadang beberapa oknum kepolisian tidak menjalankan kode etiknya sehingga korban *doxing* kurang yakin untuk melakukan pelaporan ke pihak kepolisian. LPSK sebagai Lembaga perlindungan korban juga memiliki peran yang penting dalam penanganan kasus *doxing*.

LPSK juga memberikan perlindungan hukum bagi korban *doxing* dalam bentuk safehouse, kemudian memberikan konseling psikologis yang diperlukan, hal tersebut dikarenakan *doxing* atau serangan digital dalam bentuk lain pasti akan menimbulkan trauma secara psikologis pada korban. Selain itu LPSK sebagai lembaga perlindungan terhadap korban juga memfasilitasi mengenai isu-isu terkait dengan organisasi termasuk dalam isu keamanan digital yang mana hal tersebut sangatlah berguna bagi warga negara terutama dalam era teknologi seperti pada masa sekarang ini.

Selain LPSK yang dapat menangani aduan terkait kejahatan siber korban juga dapat membuat aduan kepada Kominfo. Kominfo mendorong korban kejahatan siber untuk membuat pelaporan melalui layanan yang dikelola oleh Kominfo yang dapat diakses melalui [audankonten.id](http://audankonten.id) yang mana situs tersebut merupakan bentuk pelayanan dari Kominfo. Ini merupakan situs fasilitas situs/website, URL, akun media sosial yang aplikasi mobile dalam bentuk perangkat lunak yang mana hal tersebut memenuhi kriteria atau standar sebagai informasi dan/atau dokumen elektronik yang memiliki unsur muatan negatif sesuai dengan peraturan

perundang – undangan. Para korban *doxing* dapat membuat laporan terhadap akun – akun yang melakukan penyebaran terhadap informasi pribadi milik korban.

Selanjutnya Badan Siber dan Sandi Negara (BSSN) mempunyai beberapa layanan publik yang dimanfaatkan sebagai upaya perlindungan di ruang siber. Bagi kasus dalam bentuk *doxing* atau terror siber atau web defacement baik yang sifatnya perorangan atau organisasi. Korban yang mengalami tindak kejahatan dapat mengandalkan layanan publik yang dimiliki oleh BSSN dan dikelola oleh Direktorat Operasi Keamanan Siber yang berpusat pada Pusat Kontak Siber.

Selain daripada BSSN, BIN (Badan Intelijen Negara) juga memiliki bentuk layanan publik yang bergerak dalam bidang siber yang bernama layanan security assessment yang mana layanan tersebut dikelola oleh Deputi Bidang Intelijen Siber BIN atau Deputi IV. Layanan tersebut berfokus pada penanganan kasus web defacement yang terjadi apabila menyerang situs milik pemerintah dan layanan ini tidak berlaku bagi kasus – kasus kejahatan siber yang menyerang perorangan termasuk dalam *doxing* dan terror siber.

Di Indonesia yang memiliki tanggungjawab untuk melaksanakan perlindungan hukum dan rasa aman dalam ruang siber adalah Bareskrim Polri. Sejumlah kasus web defacement telah ditangani oleh pihak keberhasilan dengan hasil yang memuaskan hingga pelaku tertangkap, salah satunya yakni penangkapan pelaku dalam kasus peretasan *web*

Seskab. Yang menjadi catatan terbesar dalam aspek penegak hukum di Indonesia yaitu belum diaturnya *doxing* secara spesifik dalam aturan dan norma hukum.

Dalam Pasal 60 UU PDP pencegahan kebocoran data pribadi dapat diatasi dengan beberapa beberapa diantaranya yaitu dengan melakukan pemeriksaan serta penelusuran atas laporan, pengaduan, dan/atau hasil pengawasan terhadap adanya dugaan terjadinya pelanggaran perlindungan data pribadi. Korban juga dapat memanggil para ahli jika dibutuhkan dengan maksud untuk menelusuri lebih lanjut mengenai dugaan tersebut. Bahkan korban juga dapat meminta bantuan hukum kepada kejaksaan dalam proses penyelesaian sengketa dalam pelanggaran Perlindungan Data Pribadi.

Namun meskipun *doxing* belum diatur secara eksplisit dalam UU ITE karena *doxing* merupakan salah satu tindak kejahatan siber yang merampas hak atas privasi individu, maka daripada itu pengaturan hukum mengenai *doxing* menjadi salah satu langkah untuk mencegah terjadinya kebocoran data pribadi. Oleh sebab itu perlindungan hukum bagi korban *doxing* mekanisme atau langkah yang integral dari pencegahan kebocoran data pribadi.

## **B. Kendala Dan Solusi Dalam Menjalankan Perlindungan Korban *Doxing***

Tindak pidana *doxing* yang mana mencakup penyebaran data pribadi seseorang tanpa izin dianggap sebagai permasalahan yang serius karena dianggap melanggar hak privasi dan keamanan individu. Sehingga hal ini

perlu menjadi perhatian pemerintah menerapkan peraturan mengenai perlindungan data pribadi. Salah satu hal yang menjadi kendala yakni berasal yang masyarakatnya sendiri yang mana masyarakat memiliki pemahaman yang kurang mengenai bagaimana pentingnya perlindungan terhadap data pribadi.

Banyak dari individu dalam masyarakat terutama masyarakat yang berada di daerah terpencil yang mana mereka masih belum memiliki kesadaran terkait hak – hak mereka mengenai data pribadi serta cenderung memberikan informasi pribadi mereka tanpa dipikirkan secara matang terlebih dahulu. Hal ini juga disebabkan Pendidikan yang tidak merata sehingga pihak – pihak yang kurang nilai – nilai pendidikannya akan cenderung mudah untuk dirampas datanya dan digunakan secara tidak bijaksana oleh pelaku kejahatan.

Hal tersebut juga menjadikan mereka rentan terhadap serangan kejahatan seperti *doxing* dikarenakan kurangnya pengetahuan mengenai langkah – langkah perlindungan yang harus dilakukan sebagai bentuk dari pertahanan diri. Selain dari sisi pendidikan yang masih belum merata kendala selanjutnya yakni terdapat pada infrastruktur hukum serta kelembagaan yang sampai saat ini belum memadai juga menjadi hambatan. Pada kenyataannya meskipun Undang – Undang Perlindungan Data Pribadi sudah dirumuskan dan disahkan, namun pengawasan dan penegakkan hukum mengenai pelanggaran data pribadi masih sangat terbatas. Komisi yang khusus dibentuk untuk menampung kasus – kasus kejahatan yang berhubungan dengan data pribadi KPDP (Komisi Perlindungan Data Pribadi) masih belum memiliki

kapasitas dan ruang yang memadai guna melakukan pemantauan dan penegakkan hukum yang efektif.

Beberapa kendala lain dapat dikelompokkan dalam berdasarkan subjeknya, subjek – subjek tersebut memiliki bagian masing – masing dalam menjadi kendala, maka dapat dikelompokkan sebagai berikut:

### **1. Pemerintah**

Meskipun pemerintah telah menetapkan regulasi guna melindungi hak privasi warganya dengan membentuk Undang – Undang Mengenai Informasi dan Transaksi Elektronik serta Undang – Undang tentang Perlindungan Data Pribadi dalam hal ini masih terdapat kekurangan terkait dengan perlindungan pada pemilik data atau biasa kita sebut dengan korban oleh pihak lain yang ingin mendapatkan keuntungan pribadi. Hal ini berhubungan dengan masih kurangnya perlindungan kepada korban terhadap pelaku.

Guna mengatasi permasalahan ini, dirasa perlunya ada perbaikan dan peninjauan berkala terhadap regulasi tersebut yang tercermin dalam Undang – Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi. Dalam frasa pasal demi pasal pada undang – undang ini menetapkan suatu kewajiban bagi prosessor data pribadi tersebut untuk izin kepada pemilik sehingga ketika melakukan pemrosesan data sudah atas izin pihak yang bersangkutan, undang – undang ini juga melarang secara tegas perolehan, pengungkapan, dan penggunaan data informasi

yang sifatnya pribadi yang mana data tersebut bukan miliknya tanpa seizin pemilik.

Selanjutnya pemerintah juga harus secara tegas dalam menetapkan tindak lanjut atas pelanggaran yang menyerang data pribadi. Meskipun begitu dengan dibetuknya undang – undang tersebut setiaknya pemerintah sudah menunjukkan komitmennya dan kepeduliannya terhadap hak – hak warga negaranya.

## **2. Pemilik data pribadi**

Pemilik data pribadi harus membatasi akses siapa saja yang deapat mengakses data pribadinya, atau dengan kata lain pemilik data harus bisa memilah pemegang data pribadi miliknya. Yang menjadi kendala selanjutnya yakni kurangnya keaktifan dari para pemegang data dalam melindungi data melalui langkah teknis operasional dan kurangnya memperhatikan risiko kebocoran data. Sehingga guna memperkuat perlindungan data juga semua harus bernagkat dari diri sendiri dalam kepedulian terhadap pemeliharaan data pribadi.

## **3. Aparat penegak hukum**

Kurangnya perhatian dari aparat penegak hukum juga menjadi kendala yang harus diperhatikan lagi. Aparat penegak hukum belum optimal dalam menindak pelanggaran tersebut, terutama dalam kasus *doxing* yang disebabkan karena kurangnya sosialisasi serta pengetahuan di bidang terkait. Sehingga banyak kasus *doxing* yang mana pelakunya tidak mendapatkan sanksi.

#### 4. Masyarakat

Kendala selanjutnya berasal dari masyarakat yang mana kesadaran masyarakat merupakan factor yang paling penting dalam menjaga keamanan data pribadi. Dalam hal ini kesadaran masyarakat yang kurang memiliki kesadaran serta pemahaman serta penilaian dalam hukum yang menjadi nilai – nilai penting dari fungsi hukum.

Kurangnya perlindungan hukum yang didalamnya masih terdapat keterbatasan dalam peraturannya terutama mengenai *doxing* yang masih belum diatur secara eksplisit dalam perundang – undangan. Hal ini menyebabkan terjadinya ketidakpastian hukum dalam penanganan kasus *doxing*. Karena pengertian *doxing* yang diraa masih cukup luas dan belum ada standar bagaimana *doxing* pada umumnya atau minimal seperti apa yang bisa dikatakan sebagai *doxing*.

Selanjutnya dalam kesiapan aparat penegak hukum yang masih banyak dalam kondisi belum siap dalam menangani kasus kejahatan siber *doxing*. Hal ini juga perlu diperhatikan serta ditingkatkan kapasitas aparat penegak hukum dalam menangani kasus *doxing*. Kendala berikutnya berkaitan dengan peningkatan serangan kasus *doxing* yang menunjukkan bahwa tren serangan siber dapat mendelegitimasi serta membuat jurnalis tidak dipercaya oleh publik, karena wartawan dan/atau jurnalis menduduki persentase terbesar yakni sebesar 56% sebagai sasaran *doxing* oleh doxer.

Kendala yang menjadi factor penghambat juga berasal dari kompleksitas regulasi yang adaa. Undang – undang Perlindungan Data Pribadi

memiliki ketentuan yang kompleks sehingga dalam memahami frasa yang ada dalam undang – undang tersebut harus dilakukan secara mendalam yang harus diterapkan dengan benar. Selain individu bahkan perusahaan sering kali mengalami kesulitan dalam memahami dan apalagi mematuhi regulasi tersebut yang menjadikan meningkatnya pelanggaran terhadap data pribadi.

Penegakan hukum dalam fungsi melindungi warga negara juga menghadapi hambatan yang cukup signifikan. Dalam peraturan yang sudah dibentuk terdapat ambiguitas dalam pasal – pasal pada Undang – Undang Informasi dan Transaksi Elektronik serta dalam Undang – Undang Perlindungan Data Pribadi, yang dianggap terlalu luas sehingga menjadikan beberapa pasal tersebut menjadi multitafsir, seperti pasal – pasal yang membahas mengenai pencemaran nama baik serta ujaran kebencian yang mana untuk minimal unsur yang dapat dikategorikan sebagai pencemaran nama baik tidak diatur secara jelas standarnya seperti apa.

Pada kenyataannya antara peraturan perundang – undangan dengan sebagaimana yang terjadi dilapangan terdapat dua sisi yang malah berlawanan terkait dengan *doxing*. Sisi pertama mengenai Pasal 31 Undang – Undang Nomor 19 Tahun 2016 tentang Informasi dan Transaksi Elektronik yang mengatur mengenai bahwa apabila seseorang yang telah melakukan intersepsi atau penyadapan yang dilakukan pada informasi orang lain yang bukan miliknya serta menyebarkan tanpa izin si pemilik maka tindakan tersebut merupakan termasuk dalam bentuk kejahatan siber.

Selanjutnya sisi yang kedua yakni yang menjadi fokusnya adalah dalam Pasal 67 ayat (2) Undang – Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi yang menjelaskan dan mengatur mengenai bagi siapapun yang melakukan penyebaran data pribadi orang lain tanpa seizin pemilik informasi maka dapat dikenakan sanksi berupa pidana penjara paling lama 4 (empat) tahun dan/atau pidana denda dengan nominal paling banyak sebesar Rp 4.000.000.000,00 (empat miliar rupiah).

Rumusan norma yang terdapat dalam Pasal 67 ayat (2) Undang – Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi, masyarakat merasa hal tersebut dapat memiliki potensi terbungkamnya partisipasi publik dalam hal pengawasan terhadap kebijakan pemerintah atau pejabat publik, dengan mengeluarkan alibi bahwa tindakan tersebut adalah pencemaran nama baik. Dengan demikian publik menjadi takut dalam mengemukakan pendapat dan bersuara di lingkungan publik karena khawatir akan dibawa ke jalur hukum.

Dibungkamnya pendapat dan tidak bebasnya berpendapat membuat banyak masyarakat yang akhirnya acuh tak acuh dengan apa yang terjadi dalam pemerintahan. Masyarakat takut akan dijadikan sasaran oleh doxer sehingga memilih untuk diam dalam keadaan apapun. Doxer pun paling banyak menargetkan sasaran yang latar belakangnya berbeda pendapat dengan dia. Apabila selanjutnya kita yang dijadikan sasaran dan menjadi korban *doxing* maka kita dapat melaporkan kepada yang bertanggungjawab.

Yang menjadi ketakutan masyarakat yaitu masyarakat takut akan dijadikan sasaran oleh doxer sehingga memilih untuk diam dalam keadaan apapun. Doxer pun paling banyak menargetkan sasaran yang latar belakangnya berbeda pendapat dengan dia. Apabila selanjutnya kita yang dijadikan sasaran dan menjadi korban *doxing* maka kita dapat melaporkan kepada yang bertanggungjawab. Hal tersebut disebabkan karena kurangnya perlindungan hukum yang didalamnya masih terdapat keterbatasan dalam peraturannya terutama mengenai *doxing* yang masih belum diatur secara eksplisit dalam perundang – undangan. Hal ini menyebabkan terjadinya ketidakpastian hukum dalam penanganan kasus *doxing*. Karena pengertian *doxing* yang diraa masih cukup luas dan belum ada standar bagaimana *doxing* pada umumnya atau minimal seperti apa yang bisa dikatakan sebagai *doxing*.

Sebagai solusi yang dapat diberikan beberapa diantaranya harus dimulai dari diri sendiri pemilik data yakni dengan cara memeriksa dan mengelola data pribadi secara mandiri yang tersebar di internet. Dapat dilakukan dengan cara memahami *platform* media sosial yang akan digunakan, baca terlebih dahulu kebijakan privasi serta ketentuan layanan aplikasi terkait sebelum pengguna “accept” untuk masuk lebih lanjut dalam aplikasi. Selanjutnya tinjau informasi apa saja yang tersedia mengenai pengguna dan lakukan rekapan atau notulensi dalam bentuk apapun mengenai situs – situs informasi disimpan. Apabila sudah terjadi segera ambil langkah untuk menghapus informasi yang menurut pengguna tidak aman apabila diketahui oleh khalayak umum seperti alamat rumah dan foto keluarga. Yang paling

utama untuk tetap menjaga data pribadi tetap aman yakni menghindari mengunggah KTP, tiket, foto rumah dan/atau segala jenis foto yang dapat memicu tindak kejahatan siber seperti *doxing*.

Sebagai korban dapat melakukan perlawanan melalui Langkah advokasi, apabila pelaku *doxing* mengungkapkan alamat rumah dan karena itu mengancam keselamatan korban dan keluarga maka korban disarankan untuk berpindah sementara ke tempat atau lokasi yang lebih aman hingga serangan tersebut mereda. Selanjutnya korban dapat melakukan pengaduan terhadap pelaku serta dianjurkan untuk blokir akun pelaku hal ini dikarenakan supaya memberikan rasa supaya pelaku kesal dan tidak berlanjut karena merasa diabaikan oleh korban.

Sebelum melaporkan kasus *doxing* atau kasus kejahatan siber lainnya kepada penegak hukum, sebaiknya Masyarakat melakukan beberapa cara yaitu yang pertama simpan e-mail, kemudian pesan serta komunikasi lain yang dapat dijadikan bukti. Yang menjadi penting yakni bahwa bukti tersebut jangan sampai berubah dengan cara apapun, laporan tersebut tentu saja harus dilaporkan kepada penegak hukum setempat supaya selanjutnya penegak hukum dapat melakukan penyelidikan lebih lanjut.

Yang menjadi Solusi utama dalam penerapan peraturan perlindungan korban *doxing* yaitu dengan cara memperkuat landasan hukum agar selanjutnya dapat diatur secara spesifik mengenai praktik *doxing* sebagai tindak pidana. Pada saat seperti ini, regulasi yang berada di Indonesia ada yang namanya undang – undang ITE yang mana tidak menyebutkan istilah

*doxing* secara langsung, sehingga revisi atau pembentukan perundang – undangan supaya meningkatnya kekuatan mengikat suatu peraturan dan jelas tindak pidanya apa.

Selain daripada penguatan regulasi, Solusi lain yang dapat diberikan yaitu peningkatan kapasitas serta melakukan pelatihan bagi penegak hukum dalam penanganannya mengatasi penyebaran data digital seperti *doxing*. Hal ini juga dikarenakan banyaknya kasus *doxing* yang berujung tanpa penyelesaian atau bahkan tidak dipermasalahkan sama saja.

Oleh sebab itu, pelatihan secara rutin dan berkelanjutan mengenai forensik digital serta alam kaitannya penelusuran jejak siber serta dalam kaitannya mengenai prosedur atau tata cara penyelidikan yang sesuai dengan hak asasi manusia (HAM). Dengan begitu makan akan meminimalisir tindak pidana kejahatan siber dan individu juga merasa lebih aman dan nyaman dalam menggunakan media sosial.

Solusi selanjutnya yakni melakukan pembangunan atau peningkatan terhadap system perlindungan terhadap korban secara inklusif dan mudah diakses. Tidak dapat dipungkiri sekarang masyarakat cenderung malas melakukan suati kegiatan yang padahal tindakan tersebut juga demi melindungi individu atau kelompok tersebut. Seperti yang kita ketahui bahwa pemerintah sudah menyediakan langganan dengan membentuk beberapa lembaga terkait yang relevan pada bidang yang sedang dibicarakan.

Lembaga tersebut antara lain yaitu Komnas HAM, Kominfo dan LPSK (Lembaga Perlindungan Saksi dan Korban). Lembaga – lembaga

tersebut dilengkapi dengan layanan yang harusnya memiliki fitur pelaporan cepat tanggap, kemudian seharusnya dianggarkan untuk bantuan hukum gratis serta konseling bagi korban yang mengalami trauma yang berkelanjutan. Dalam membenahi apa yang kurang dari perlindungan yang sudah ada, seharusnya juga memikirkan jangka panjang mengenai apa saja kemungkinan – kemungkinan yang dapat terjadi di masa depan, termasuk dalam relokasi digital (penggantian identitas daring atau online).

Selanjutnya yang dapat dilakukan juga melakukan edukasi kepada publik mengenai pentingnya privasi data dan bahaya dari *doxing* juga merupakan bentuk Langkah preventif yang cukup penting. Masyarakat seringkali tidak sadar bahwa yang mereka lakukan dalam bermain media sosial dapat memancing pelaku *doxing*. Selain itu masyarakat juga cenderung abai dengan hukum yang ada, merasa tidak perlu berlebihan menghadapi suatu permasalahan dan tidak sadar bahwa membagikan informasi pribadi secara cuma – cuma tanpa izin pemilik informasi berpotensi memiliki konsekuensi hukum dan etis yang cukup serius.

Mengadakan kampanye literasi digital yang didukung oleh pemerintah sebagai bukti peran pemerintah dalam meningkatkan kualitas pola pikir masyarakat mengenai bagaimana resiko dalam penggunaan media sosial terutama pada masyarakat yang sudah dewasa dan menjadi orang tua yang merasa selalu benar dengan apapun yang dilakukannya. Literasi digital juga didukung oleh lembaga swadaya masyarakat dan juga *platform*, yang mana hal ini dirasa harus lebih gencar dilakukan khususnya dikalangan anak muda

yang masih dibawah umur namun sudah mendapat kebebasan untuk bermain sosial media.

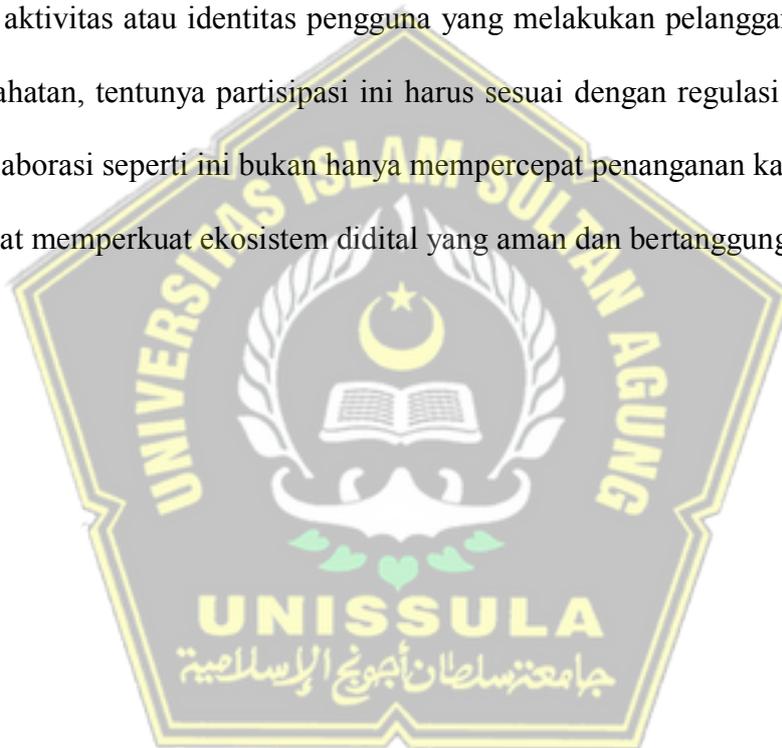
Literasi digital yang ditujukan khususnya untuk anak – anak ini bertujuan guna menanamkan pola pikir mengenai kesadaran pentingnya untuk tidak terlalu mengumbar informasi pribadi miliknya, milik keluarganya bahkan milik orang terdekatnya dalam unggahannya di media sosial. Dengan penanaman pola pikir seperti ini diharapkan masyarakat semakin memiliki rasa kewaspadaan terhadap diri sendiri dan akan lebih baik apabila masyarakat yang sudah memiliki kesadaran juga turut mengingatkan orang – orang disekitarnya supaya lebih waspada dan peka terhadap lingkungan sekitar.

Dengan meningkatnya kesadaran masyarakat, yang diharapkan adalah potensial pelaku sebelum untuk menjalankan aksi kejahatannya, pelaku berfikir dua kali untuk menjalankan aksinya selain itu korban juga akan mengetahui dan memahami langkah apa yang seharusnya diambil ketika mereka menjadi sasaran oleh doxer. Sehingga meskipun sudah ditargetkan korban dapat mengambil Tindakan cepat guna meminimalisir tindak kejahatan yang nantinya bisa saja berkelanjutan.

Kemudian yang terakhir yakni pentingnya mengadakan kolaborasi antara pemerintah dengan *platform* digital yang mana inilah yang menjadi elemen kunci dalam mencegah serta menangani kasus *doxing*. *Platform* seperti Facebook, Instagram dan X (Twitter) yang memiliki induk perusahaan seharusnya memiliki mekanisme pelaporan mengenai konten *doxing* atau dugaan konten yang mengarah ke *doxing* yang cepat dan efektif, serta harus

memiliki tanggung jawab dalam penghapusan konten tersebut yang harus dilakukan dengan segera sebelum menimbulkan dampak yang lebih besar terhadap korban.

Pemerintah dapat mendorong *platform – platform* seperti ini menggunakan kekuasaannya untuk ikut serta dalam partisipasi penyelidikan dalam kasus *doxing*, contoh partisipasinya yakni dengan cara menyerahkan log aktivitas atau identitas pengguna yang melakukan pelanggaran dan tindak kejahatan, tentunya partisipasi ini harus sesuai dengan regulasi yang berlaku. Kolaborasi seperti ini bukan hanya mempercepat penanganan kasus tetapi juga dapat memperkuat ekosistem digital yang aman dan bertanggungjawab.<sup>36</sup>



---

<sup>36</sup> Internet Watch Foundation, 2021, “Combating *Doxing* through *Platform* Cooperation”. IWF R.

## **BAB IV**

### **PENUTUP**

#### **A. Kesimpulan**

Berdasarkan penelitian maka selanjutnya dapat disimpulkan bahwa:

1. Perlindungan hukum bagi korban *doxing* sebagai pencegahan terjadinya kebocoran data penting dikarenakan *doxing* sangat mengancam privasi setiap individu. Pengaturan perbuatan *doxing* selain diatur dalam dalam Pasal 26 ayat (1) Undang – Undang ITE dalam frasanya yang menegaskan bahwa dalam setiap penggunaan informasi yang dilakukan melalui media elektronik yang menyangkut data pribadi seseorang. Tindak pidana *doxing* dapat ditemukan dalam Undang – Undang Nomor 19 Tahun 2016 Tentang Informasi dan Transaksi Elektronik (ITE), yang khususnya dijelaskan pada Pasal 27 ayat (1) dan Pasal 32 ayat (2), yang mana pasal tersebut mengatur mengenai distribusi dan akses illegal terhadap informasi pribadi. *Doxing* juga berkaitan dengan undang – undang perlindungan data pribadi yang mana pada undang – undang ini diatur apa saja yang menjadi data pribadi yang kedepannya ada kemungkinan untuk menjadi target tindak pidana *doxing*. Oleh karena itu pengaturan perlindungan korban *doxing* menjadi bagian yang integral untuk pencegahan terjadinya kebocoran data.
2. Kendala utama dalam menjalankan perlindungan terhadap korban adalah dari masing – masing individu masyarakat. Pengetahuan yang kurang terhadap istilah *doxing* membuka kemungkinan kasus akan semakin

bertambah banyak yang menyebabkan pihak yang berwenang mengalami kewalahan sehingga jalannya peradilan kurang maksimal. Penting untuk melakukan penanaman terhadap bahaya doxing sejak dini. Dengan penanaman pola pikir seperti ini diharapkan masyarakat semakin memiliki rasa kewaspadaan terhadap diri sendiri dan akan lebih baik apabila masyarakat yang sudah memiliki kesadaran juga turut mengingatkan orang – orang disekitarnya supaya lebih waspada dan peka terhadap lingkungan sekitar. Dengan meningkatnya kesadaran masyarakat, yang diharapkan adalah potensial pelaku sebelum untuk menjalankan aksi kejahatannya, pelaku berfikir dua kali untuk menjalankan aksinya selain itu korban juga akan mengetahui dan memahami langkah apa yang seharusnya diambil ketika mereka menjadi sasaran.

## **B. Saran**

### **1. Bagi Pemerintah**

- a) Seharusnya pengaturan mengenai kejahatan siber akan jauh lebih baik apabila diperkuat mengingat angka persentase kasus kejahatan siber yang sangat tinggi. Selain itu pemerintah harus paham terhadap risiko yang akan muncul apabila kejahatan siber semakin banyak dan merajalela di Indonesia.
- b) Pemerintah juga dapat mengajak anak muda yang paham terkait dengan teknologi terutama dalam bidang hacking sehingga keamanan mengenai data yang tersimpan secara digital pada pemerintah jadi lebih aman.

## 2. Bagi Masyarakat

Harus diberikan sosialisasi mengenai bahaya *doxing* bagi korbannya apabila ada pelaku yang masih berkeliaran. Pelaku harus diberikan pembelajaran atau teori yang dapat merubah pola pikirnya supaya menjadi pribadi yang lebih baik. Banyak kendala yang dihadapi namun banyak juga pilihan solusi yang dapat di implementasi. Semestinya dengan adanya beberapa solusi yang sudah ditawarkan pemerintah bersama dengan masyarakat bersama sama membangun Indonesia menjadi negara yang aman dan nyaman bagi pengguna media sosial.



## DAFTAR PUSTAKA

### A. Al – Quran dan Hadis

Q.S AL – HUJURAT AYAT 11

Al-Ghazali, 2018 M/1439 H-1440 H: III/137

### B. Buku

Adami Chazawi, 2007, *Pelajaran Hukum Pidana 1*, PT. Raja Grafindo, Jakarta.

Barda Nawawi Arief, 2011, *Bunga Rampai Kebijakan Hukum Pidana: Perkembangan Penyusunan Konsep KUHP Baru*, Kencana, Jakarta.

Tofik Yanuar Chandra, 2022, *Hukum Pidana*, PT. Sangir Multi Usaha, Jakarta.

Idik Saeful Bahri, *Cyber Crime Dalam Sorotan Hukum Pidana*, Edisi 2023.

Ismu Gunadi dan Jonaedi Efendi, 2014, *Hukum Pidana*, Kencana, Jakarta.

Ismu Gunadi, dan Jonaedi Efendi, 2014, *Cepat & Mudah Memahami Hukum Pidana*, Kencana, Jakarta.

Johanes Supranto, 2003, *Metode Penelitian Hukum dan Statistik*, Rineka Cipta, Jakarta.

Kementerian Komunikasi dan Informatika (Kominfo), 2022, *Strategi nasional literasi digital 2021–2024*. Kementerian Komunikasi dan Informatika Republik Indonesia.

Lili Rasjidi & I.B. Wyasa Putra, 2006, *Hukum sebagai Sistem: Kajian Teoretis*, Remaja Rosdakarya, Bandung.

Mahrus Ali, 2015, *Dasar-Dasar Hukum Pidana Cet ke 3*, Sinar Grafika, Jakarta.

Maskun, 2013, *Kejahatan Siber Cyber crime Suatu Pengantar*, Kencana Jakarta.

Moeljatno, 1993, *Asas-asas Hukum Pidana*, Rineka Cipta, Jakarta.

Moleong, L. J., 2013, *Metodologi Penelitian Kualitatif*, PT. Remaja Rosdakarya, Bandung.

*Oxford British and World English Dictionary*.

Prof. Moeljatno, 2018, *Kitab Undang – Undang Hukum Pidana*, PT. Bumi Aksara, Jakarta.

Seva Maya Sari, 2022, *Buku Ajar FIQH JINAYAH*, Universitas Islam Negeri Sumatera Utara.

Soerjono Soekanto dan Sri Mamudji, 2001, *Penelitian Hukum Normatif Suatu Tinjauan Singkat*, PT Raja Grafindo Persada, Jakarta.

### **C. Perundang – undangan**

Undang – undang Dasar Negara Republik Indonesia Tahun 1945

Kitab Undang – undang Hukum Pidana

Undang – Undang Nomor 1 Tahun 2024 Tentang Perubahan Atas Undang – Undang Nomor 19 Tahun 2016 Tentang Informasi dan Transaksi Elektronik

Undang – undang Nomor 27 Tahun 2022 Tentang Pelindungan Data Pribadi

Undang – undang Nomor 19 Tahun 2016 Tentang Perubahan Atas Undang – undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik.

Undang – Undang Nomor 13 Tahun 2006 Tentang Perlindungan Saksi dan Korban

### **D. Jurnal dan Karya Tulis Ilmiah**

Armando M. Arvy C. dan Hari Soeskandi, 2023, PERTANGGUNGJAWABAN PIDANA BAGI PARA PELAKU DOXING MENURUT UU ITE DAN UU PDP, *Bureaucracy Journal : Indonesia Journal of Law and Social-Political Governance*, Vol. 3.

Batuhan Kukul, 2023, Personal Data and Personal Safety : Re-Examining The Limits Of Public Data In The Context Of Doxing, *International Data Privacy Law*, Vol.13, No. 3.

- Damayanti, D. et al.trans. 2024. Perspektif Hukum Islam Terhadap Perlindungan Data Pribadi Di Era Digital. *al-Battar: Jurnal Pamungkas Hukum* . 1, 3 (Dec. 2024), 151–163.
- Douglas, David M, ‘*Doxing: A Conceptual Analysis*’, *Ethics and Information Technology*, 18 (3), 2016
- Eckert, S. and Metzger-Riftkin, J. (2020). Doxxing. In *The International Encyclopedia of Gender, Media, and Communication* (eds K. Ross, I. Bachmann, V. Cardo, S. Moorti and M. Scarcelli). <https://doi.org/10.1002/9781119429128.iegmc009>
- Jeane Neltje Saly dan Lubna Tabriz Sulthanah, 2023, Pelindungan Data Pribadi dalam Tindakan Doxing Berdasarkan Undaqqng – Undang Nomor 27 Tahun 2022, *Jurnal Kewarganegaraan*, Vol. 7, No. 2.
- Internet Watch Foundation. (2021). *Combating doxing through platform cooperation. IWF Reports*.
- Ketaren, E. (2017). CYBERCRIME, CYBER SPACE, DAN CYBER LAW. *Jurnal TIMES*, 5(2), 35–42. <https://doi.org/10.51351/jtm.5.2.2016556>
- Leonardo Latsiano Dade, Caecilia J.J Waha & Nurhikmah Nachrawy, 2024, KAJIAN YURIDIS TENTANG TINDAK PIDANA PENYEBARAN DATA PRIBADI MELALUI INTERNET (DOXING) DI INDONESIA, *Jurnal Fakultas Hukum Universitas Sam Ratulangi Lex Privatum* Vol.13 No. 3.
- Lianthy Nathania Paat, 2020, KAJIAN HUKUM TERHADAP CYBER BULLYING BERDASARKAN UNDANG – UNDANG NOMOR 19 TAHUN 2016, *Journal Lex Crimen*, Vol. IX, No. 1.
- Mengtong Chen, Anne Shann Yue Cheung and Ko Ling Chan, 2019, Doxing : What Adolescents Look For and Their Intentions, *International Journal of Environmental Research Public Health*, 16, 218.
- Nyman, M. (2021). Legal frameworks addressing doxing in the European Union. *European, Journal of Law and Technology*.
- Permata Ayunda P. dan Lucky Nurhayanto, 2024, Perspektif Perilaku Doxing Sebagai Bentuk Cancel Culture pada Pengguna Media Sosial X, *Jurnal Hukum, Humaniora Dan Politik*, Vol.4, No. 4.

Sari, I. (2023). Perbedaan Bentuk Kejahatan Yang Dikategorikan Sebagai *Cyber crime* Dan *Cyber Warfare*. *JSI (Jurnal Sistem Informasi Universitas Suryadarma*, 10(1).

Setiadi, A. (2022). Tantangan penegakan hukum siber di Indonesia. *Jurnal Kriminologi Indonesia*.

Sinaulan, J. (2018). Perlindungan Hukum Terhadap Warga Masyarakat. *Ideas: Jurnal Pendidikan, Sosial, Dan Budaya*, 4(1).

UN General Assembly, Declaration of Basic Principles of Justice for Victims of Crime and Abuse of Power : resolution / adopted by the General Assembly, A/RES/40/34, 29 November 1985

Wahyudi Dheny, 2013, PERLINDUNGAN HUKUM TERHADAP KORBAN KEJAHATAN *CYBER CRIME* DI INDONESIA, Jurnal Ilmu Hukum

#### E. Lain – Lain

Kompas.com. (2020). *Jurnalis Pemeriksa Fakta Jadi Korban Doxing, Liputan6.com Tempuh Jalur Hukum*.  
<https://www.kompas.com/tren/read/2020/09/12/140425765/jurnalis-pemeriksa-fakta-jadi-korban-doxing-liputan6com-tempuh-jalur-hukum?>

Lembaga Perlindungan Saksi dan Korban (LPSK). (2023). *Pedoman perlindungan korban kejahatan siber*. Laporan Tahunan LPSK.

Liputan6.com. (2020). *Pernyataan Liputan6.com soal Doxing Jurnalis Cakrayuri Nuralam*.

Racha Chotia, “What is document tracking? Why is it important?”,  
<https://signeasy.com/blog/business/document-tracking?>

[https://www.garuda.website/blog/data-pengguna-sosial-media-indonesia-2024/?utm\\_](https://www.garuda.website/blog/data-pengguna-sosial-media-indonesia-2024/?utm_)

<https://quran.nu.or.id/al-hujurat/11>

<https://nu.or.id/syariah/hukum-membuka-rahasia-orang-lain-rA1ts>

[https://repositori.uma.ac.id/bitstream/123456789/1816/5/138400101\\_file5.pdf](https://repositori.uma.ac.id/bitstream/123456789/1816/5/138400101_file5.pdf)

<http://tesishukum.com/pengertian-perlindungan-hukum/>

<https://www.kompas.id/artikel/serangan-digital-masih-mengintai-aktivis-dan-kelompok-kritis>

<https://books.google.co.id/books?id=>

