JURNAL HUKUM PELITA, Vol. 5 No. 1 (2024) : Mei 2024 Hal 1-12
ISSN 2809-2082 (online)
Available online at: https://jurnal.pelitabangsa.ac.id/index.php/JH

Penerapan Hukum Terhadap Tindak Pidana *Doxing* di Indonesia

Yudha Adi Nugraha [1], Trias Saputra[2]
[12]Universitas Pelita Bangsa
*Korespondensi: Ais_yan97@mhs.pelitabangsa.ac.id

Info Artikel

Diterima : 1-10-2023	Direvisi : 13-5-2024	Disetujui : 13-5-2024	Diterbitkan : 31-5-2024

Keywords : *Doxing, ITE, Law*

Abstract : *The development of information technology and the Internet has led to criminal acts of Doxing, i.e., the unlawful disclosure of personal data. In Indonesia, Doxing has become a serious problem in the financial technology industry (Fintech). This study analyzes the enforcement of the Doxing law under the Personal Data Protection Act No. 27 of 2022 and the ITE Act No. 19 of 2016 in Indonesia and looks at its effectiveness in protecting the privacy of Fintech customers. The existing legal framework provides the basis, but it requires stronger legislative changes and more active enforcement. Public education is also important to raise awareness of cybersecurity risks and practices. International cooperation is needed to tackle Doxing that crosses national borders. Although law enforcement Doxing is complicated as perpetrators often use advanced technology and anonymous identities, with joint efforts, the protection of individual privacy and the security of fintech users in Indonesia can be enhanced.*

Kata kunci : *Doxing, ITE, Hukum*

Abstrak : Perkembangan teknologi informasi dan internet telah memunculkan tindakan kejahatan *Doxing*, yaitu pengungkapan *ilegal* data pribadi. Di Indonesia, *Doxing* menjadi masalah serius dalam industri *Financial Technology* (*Fintech*). Penelitian ini menganalisis penegakan hukum *Doxing* berdasarkan Undang-Undang No. 27 Tahun 2022 tentang Perlindungan Data Pribadi dan Undang-Undang ITE No. 19 Tahun 2016 di Indonesia serta melihat efektivitasnya dalam melindungi privasi nasabah Fintech. Kerangka hukum yang ada memberikan dasar, tetapi perlu perubahan hukum yang lebih tegas dan penegakan yang lebih aktif. Pendidikan publik juga penting untuk meningkatkan kesadaran akan risiko *Doxing* dan praktik keamanan siber. Kerjasama internasional diperlukan untuk mengatasi *Doxing* yang melintasi batas negara. Meskipun penegakan hukum *Doxing* rumit karena pelaku sering menggunakan teknologi canggih dan identitas anonim, dengan upaya bersama, perlindungan terhadap privasi individu dan keamanan penggunaan Fintech di Indonesia dapat ditingkatkan.

I. PENDAHULUAN

Perkembangan teknologi informasi dan internet telah mengubah secara fundamental cara kita berinteraksi, bekerja, dan beraktivitas. Seiring dengan kemajuan ini, muncul juga berbagai tantangan hukum yang harus dihadapi. Salah satu tantangan penting adalah tindak kejahatan *Doxing* dan penyebaran data pribadi yang telah menjadi perhatian serius dalam hukum *cyber*. *Doxing*, singkatan dari "*document tracing*" adalah praktik yang melibatkan pengumpulan dan penyebaran data pribadi seseorang secara ilegal, dengan tujuan merugikan individu tersebut. Hal ini mencakup informasi seperti alamat rumah, nomor telepon, alamat email, dan lainnya. Praktik ini dapat digunakan untuk berbagai tujuan jahat, termasuk pelecehan, penipuan, atau bahkan ancaman fisik.

Di Indonesia pada tahun 2021, tercatat beberapa kasus *Doxing* yang telah terjadi, seperti pada Warga Cilincing Jadi Korban *Doxing* oleh Pinjol[1], Wanita di Jakut Jadi Korban *Doxing* 'Open BO' Pinjaman Online[2], Terulang Lagi! Tak Terima Fotonya Dimanipulasi Seolah Bugil dengan Narasi 'Open BO', Wanita di Cikarang Ini Laporkan Pinjol ke Polisi[3], dan banyak lagi kasus serupa. *Financial Technology* (Fintech) adalah istilah yang digunakan untuk menggambarkan industri yang menggabungkan teknologi informasi dengan layanan keuangan. Ini mencakup berbagai inovasi dan solusi teknologi yang digunakan dalam sektor keuangan untuk memberikan layanan yang lebih efisien, praktis, dan mudah diakses kepada individu dan bisnis. Fintech mencakup beragam bidang, termasuk pembayaran digital, pinjaman daring (*peer-to-peer lending*), manajemen keuangan pribadi, investasi online, mata uang digital (seperti Bitcoin), dan banyak lagi[4]. Tujuan utama Fintech adalah untuk merampingkan proses keuangan, mengurangi biaya, meningkatkan aksesibilitas, dan memberikan pengalaman yang lebih baik kepada pengguna[5].

Di indonesia, industri Fintech diatur oleh Bank Indonesia (BI) dan Otoritas Jasa Keuangan (OJK) untuk memastikan keamanan dan kepatuhan dalam operasionalnya. Fintech telah mengubah cara orang bertransaksi, berinvestasi, dan mengelola keuangan

[1] Kompas.com Muhammad Naufal, Warga Cilincing Jadi Korban Doxing oleh Pinjol, Satgas Waspada Investigasi Minta Pelaku Ditangkap (2021).
[2] Merdeka.com, Wanita di Jakut Jadi Korban Doxing "Open BO" Pinjaman Online (2021).
[3] Pos Kota, Terulang Lagi! Tak Terima Fotonya Dimanipulasi Seolah Bugil dengan Narasi "Open BO", Wanita di Cikarang Ini Laporkan Pinjol ke Polisi (n.d.).
[4] Dhea Khoirunisa et al., "Analisis Peran Otoritas Jasa Keuangan (Ojk) dalam Mengawasi Pelayanan Pada Perusahaan Financial Technology (Fintech) di Indonesia" 2, no. 3 (2023): 127–32, https://doi.org/10.30640/inisiatif.v2i3.1108.
[5] D Meitiara P Bakrie and Fauzan Permana ABNR Counsellors at Law Emir Nurmansyah, Elsie F Hakim, "Fintech 2023, Definitive global law guides offering comparative analysis from top-ranked lawyers," 2023.

mereka, menjadikannya bagian integral dari perkembangan sektor keuangan di era digital[6]. Namun, perkembangan fintech juga telah memungkinkan masyarakat untuk mengakses layanan keuangan dengan lebih mudah dan cepat, yang menarik perhatian penjahat cyber yang berusaha untuk mendapatkan data pribadi nasabah fintech dengan cara yang ilegal. Dalam konteks ini, peran hukum sangat penting dalam melindungi privasi individu dan menghukum pelaku tindak kejahatan *Doxing*. Dalam kaitannya, Undang-Undang No. 27 Tahun 2022 dan Undang-Undang ITE No. 19 Tahun 2016 di Indonesia memiliki peran kunci dalam memberikan kerangka hukum untuk penegakan terhadap tindak kejahatan *Doxing*.

Penelitian ini bertujuan untuk menganalisis bagaimana penegakan hukum terkait tindak kejahatan *Doxing* dilakukan berdasarkan dua undang-undang tersebut, dan bagaimana efektivitasnya dalam melindungi privasi nasabah fintech dari tindakan ilegal. Kami juga akan mengeksplorasi berbagai tantangan yang dihadapi dalam penegakan hukum *Doxing* dan potensi solusi untuk mengatasinya. Dengan pemahaman yang lebih baik tentang peran hukum dalam menghadapi tindak kejahatan *Doxing*, diharapkan dapat meningkatkan perlindungan terhadap privasi individu dan keamanan penggunaan fintech di Indonesia.

II. METODE PENELITIAN

Penelitian ini merupakan jenis penelitian pustaka, di mana penelitian dilakukan melalui membaca buku-buku dan literatur yang relevan dengan permasalahan yang sedang dibahas. Dalam konteks ini, penulis mengamati buku-buku yang terkait dengan cybercrime untuk mengidentifikasi dan memahami temuan dari berbagai sumber literatur tersebut[7]. Metode yang digunakan dalam penelitian ini adalah metode kualitatif, di mana analisis data dilakukan sesuai dengan fokus studi yang telah ditetapkan oleh penulis[8].

Teknik analisis data yang diterapkan adalah metode deskriptif, yang bertujuan untuk mendeskripsikan data yang telah berhasil dikumpulkan. Pendekatan ini memungkinkan peneliti untuk menggambarkan secara terperinci obyek permasalahan yang dihadapi dan menghasilkan pemahaman yang konkret serta jelas. Dalam melakukan analisis, penulis menggunakan pola pikir deduktif, yakni dimulai dari konsep umum untuk kemudian

[6]Otoritas Jasa Keuangan, "Perusahaan Fintech Lending Berizin Per 9 Maret 2023," 2023, www.danacita.co.id.
[7] Mestika Zed, *Metode penelitian kepustakaan*, 5 ed. (Yayasan Pustaka Obor Indonesia, 2018).
[8] sugiono, *Metode Penelitian Kuantitatif, Kualitatif, dan R&D* (Bandung: Alfabeta, 2019).

diaplikasikan pada hal-hal yang lebih spesifik. Sumber data dalam penelitian ini diperoleh dari data hukum primer dan sekunder antaranya :

1. Bahan hukum primer, dalam penelitian ini bahan hukum primer yang digunakan adalah Undang-undang (UU) Nomor 19 Tahun 2016 tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik dan Undang – Undang Nomor 27 Tahun 2022 Tentang Pelindungan Data Pribadi beserta beberapa Putusan Pengadilan yang terkait.
2. Bahan hukum sekunder, Data-data yang diperoleh peneliti dari penelitian kepustakaan dan dokumantasi, yang merupakan hasil penelitian dan pengolahan orang lain, yang sudah tersedia dalam bentuk buku-buku atau dokumentasi yang biasanya disediakan di perpustakaan atau milik pribadi peneliti. Bahan Hukum Sekunder, yaitu bahan hukum yang memberikan penjelasan terhadap bahan hukum primer (buku ilmu hukum, jurnal hukum, laporan hukum, dan media cetak atau elektronik).

III. PEMBAHASAN

A. Pengertian *Doxing*

Doxing, singkatan dari "*document tracing*" atau "*dropping documents*," adalah tindakan pengungkapan informasi pribadi seseorang secara daring tanpa izin atau persetujuan mereka. Hal ini melibatkan pengumpulan dan penyebaran informasi seperti nama, alamat, nomor telepon, alamat email, informasi pekerjaan, atau data pribadi lainnya dengan niat untuk merusak reputasi, mengancam, atau mengekspos individu tersebut. Menurut M. Yusuf Samad[9] *Doxing* adalah menyalahgunakan data pribadi yang tersebar luas maupun yang disimpan oleh instansi tertentu. Serta menurut Febriana Kesuma Nastiti dalam peniltiannya *Doxing* adalah proses mengumpulkan, meretas, atau mengekspos informasi orang lain, seperti nama, foto, alamat, Nomor telepon, dan detail kartu kredit. *Doxing* dapat menargetkan individu atau organisasi tertent[10].

Peran *Doxing* dalam pelanggaran privasi sangat signifikan. Dengan mengungkapkan informasi pribadi seseorang, pelaku *Doxing* dapat mengakibatkan dampak serius, seperti

[9] P.D. Samad, Y.S & Persadha, "Pendekatan Intelijen Strategis Sebagai Upaya Memberikan Perlindungan di Ruang Siber Dalam Konteks Kebebasan Menyatakan Pendapat," *Kajian* 27, no. 1 (2022): 31–42, https://jurnal.dpr.go.id/index.php/kajian/article/viewFile/3588/1071.

[10] Febriana Kesuma Nastiti, "Perlindungan Hukum Pidana Terhadap Mahasiswa Universitas Islam Indonesia yang Mengalami Doxing oleh Akun Uiicantikganteng di Platform Instagram" (Universitas Islam Indonesia, 2023).

pelecehan, ancaman, atau pencemaran nama baik. Selain itu, *Doxing* juga bisa digunakan untuk tujuan kriminal, seperti penipuan atau pencurian identitas.

B. Ketentuan Hukum dalam UU No. 27 Tahun 2022 dan UU ITE No. 19 Tahun 2016

Kedua undang-undang, yaitu UU No. 27 Tahun 2022 tentang Perlindungan Data Pribadi (UU PDP) dan UU ITE No. 19 Tahun 2016 tentang Informasi dan Transaksi Elektronik (UU ITE), memiliki ketentuan hukum terkait penyebaran data pribadi dan tindak kejahatan *Doxing*. Berikut analisis pasal-pasal terkait dan penjelasan sanksi hukum yang diberlakukan :

1. Ketentuan Hukum Undang – Undang No. 27 Tahun 2022 Perlindungan Data Pribadi (UU PDP)

UU No. 27 Tahun 2022 tentang Perlindungan Data Pribadi (UU PDP) memiliki ketentuan yang penting untuk melindungi data pribadi individu. Berikut adalah penjelasan lebih lanjut mengenai beberapa pasal dalam UU PDP :

a. Pasal 26 ayat (1) UU PDP: Pasal ini menegaskan bahwa setiap orang dilarang melakukan pemrosesan data pribadi tanpa izin dari pemilik data. Pemrosesan data pribadi mencakup pengumpulan, penggunaan, penyimpanan, pengungkapan, dan pemindahan data pribadi. Namun, terdapat pengecualian yang diatur dalam undang-undang, yang mengindahkan ketentuan ini. Hal ini bertujuan untuk melindungi privasi data pribadi individu dan mendorong praktik yang etis dalam pengelolaan data.

b. Pasal 26 ayat (3) UU PDP: Pasal ini memberikan hak kepada pemilik data pribadi untuk mengajukan keluhan jika terjadi penyebaran data pribadi yang melanggar ketentuan UU PDP. Ini berarti jika seseorang merasa data pribadinya disalahgunakan atau dilanggar, mereka memiliki hak untuk melaporkannya dan meminta tindakan hukum.

c. Pasal 34 ayat (1) UU PDP: Pasal ini mengatur bahwa setiap orang yang melanggar ketentuan mengenai perlindungan data pribadi dapat dikenai sanksi administratif. Sanksi administratif ini dapat berupa denda atau tindakan lain yang ditetapkan oleh otoritas yang berwenang. Sanksi ini bertujuan untuk memberikan sanksi kepada pelanggar dan mendorong kepatuhan terhadap UU PDP.

2. Ketentuan Hukum Undang – Undang No 19 Tahun 2016 Tentang Informasi dan Transaksi Elektronik

UU ITE No. 19 Tahun 2016. Ini adalah ringkasan ketentuan-ketentuan penting dalam undang-undang tersebut :

a. Pasal 27 ayat (3): UU ITE melarang setiap orang menyebarluaskan informasi elektronik atau dokumen elektronik yang berisi data pribadi tanpa izin dari pemilik data. Hal ini relevan dengan tindak kejahatan *Doxing*, di mana penyebaran data pribadi orang lain tanpa izin merupakan pelanggaran hukum.
b. Pasal 32 ayat (1): Undang-Undang ITE menyatakan bahwa pelanggaran terhadap ketentuan dalam Pasal 27 ayat (3) dapat dikenai sanksi pidana penjara dan/atau denda. Ini berarti bahwa pelaku *Doxing* yang melanggar ketentuan tersebut dapat dihukum dengan pidana penjara atau denda sesuai dengan keputusan pengadilan.
c. Pasal 38 ayat (1): UU ITE juga mengatur bahwa setiap orang yang mengakses elektronik dan/atau sistem komputer secara ilegal dapat dikenai sanksi pidana. Hal ini mencakup tindakan ilegal seperti peretasan atau akses tanpa izin ke sistem komputer.

Ketentuan-ketentuan ini memiliki tujuan untuk melindungi privasi dan keamanan data pribadi individu serta mencegah tindakan kriminal seperti *Doxing* dan peretasan. Pelanggaran terhadap UU ITE dapat mengakibatkan sanksi pidana yang serius, seperti pidana penjara dan denda, untuk melindungi integritas data elektronik dan komputer.

Sanksi hukum yang diberlakukan dalam kedua undang-undang ini mencakup sanksi administratif, pidana penjara, dan denda. Pelanggaran terkait penyebaran data pribadi dan tindak kejahatan *Doxing* dapat mengakibatkan tindakan hukum sesuai dengan ketentuan yang diatur dalam kedua undang-undang tersebut. Oleh karena itu, penting bagi individu dan entitas untuk mematuhi aturan-aturan ini untuk menjaga privasi dan keamanan data pribadi.

C. Studi Kasus Penyebaran Data Pribadi Nasabah Fintech Ilegal

Perkembangan teknologi pada masa ini telah mengubah tatanan interaksi manusia dalam berbagai aspek seperti komunikasi bisnis, keuangan, dan sosial. Teknologi canggih saat ini telah memberikan kemudahan kepada manusia dalam berbagai sektor pekerjaan. Namun, dampak negatifnya telah menimbulkan fenomena baru, seperti yang terlihat dalam kasus pinjaman online yang muncul sejak tahun 2014. Pinjaman online menawarkan kenyamanan tanpa harus pergi ke bank, hanya dengan memanfaatkan internet, dan ini telah memikat banyak orang. Banyak orang beralih ke pinjaman online daripada bank konvensional, tetapi ini juga memicu peningkatan tindak pidana kejahatan online. Salah satu contohnya adalah *Doxing* oleh perusahaan pinjaman online. Penelitian mengungkapkan bahwa salah satu faktor utama dalam terjadinya tindak pidana *Doxing* adalah kurangnya kehati-hatian dari pihak peminjam. Kehati-hatian yang dimaksud melibatkan kurangnya pemeriksaan apakah pinjaman online tersebut terdaftar di Otoritas Jasa Keuangan (OJK) atau tidak. Selain itu, tindak pidana ini juga sering terjadi karena peminjam tidak memenuhi perjanjian pembayaran yang telah disepakati sebelumnya.

Penyalahgunaan data pribadi oleh perusahaan pinjaman online dapat berbentuk variasi, seperti penggunaan pihak ketiga dalam proses penagihan. Penyebaran data pribadi konsumen ini sering dimulai dengan keterlambatan pembayaran atau bahkan ketidakmampuan konsumen untuk membayar. Perusahaan pinjaman online ilegal kemudian menggunakan taktik yang merugikan konsumen dengan menyebarkan data pribadi mereka kepada pihak ketiga dan melakukan tekanan agar konsumen membayar. Perusahaan fintech peer to peer lending sering menggunakan jasa desk collection sebagai pihak ketiga dalam penagihan hutang. Namun, dalam beberapa kasus, seperti yang terlihat pada putusan Nomor 438/Pid.Sus/2020/PN Jkt.Utr, masalah muncul karena pihak ketiga ini tidak memiliki sertifikasi yang sah dari Asosiasi Fintech Pendanaan Bersama Indonesia, yang mengakibatkan penagihan ilegal dan melanggar hukum. Selanjutnya, tindakan penyalahgunaan data pribadi juga mencakup intimidasi dan ancaman terhadap konsumen. Dalam beberapa kasus, seperti yang terjadi dalam putusan Nomor 438/Pid.Sus/2020/PN Jkt.Utr, pegawai desk collection dari perusahaan fintech ilegal telah mengambil langkah-langkah ekstrem dengan mengakses kamera dan galeri ponsel konsumen untuk mengambil foto atau video yang dianggap merugikan mereka. Ini kemudian digunakan sebagai ancaman untuk memaksa konsumen membayar hutang. Tindakan semacam ini melanggar hukum dan dapat dikategorikan sebagai tindak pidana berdasarkan Undang-Undang Informasi dan Transaksi Elektronik (ITE).

Selain itu, penyalahgunaan data pribadi mencakup penggunaan nomor kontak darurat yang telah didaftarkan oleh konsumen untuk menyebarkan fitnah dan menimbulkan kebencian atau permusuhan. Dalam banyak kasus, *debt collector* akan menghubungi orang lain yang tidak terkait dengan peminjam dana dengan menggunakan nomor telepon yang diperoleh tanpa izin atau pengetahuan konsumen. Tindakan ini melanggar hukum karena melibatkan akses ilegal terhadap data pribadi konsumen. Penting untuk dicatat bahwa perusahaan pinjaman online ilegal juga dapat menjual data pribadi konsumen kepada pihak lain. Hal ini telah terbukti dalam beberapa kasus, seperti yang diungkapkan oleh Yoshua Markus Mariwu, *Co-Founder* Digikai Studio. Praktik semacam ini merupakan bentuk serius dari pelanggaran privasi dan dapat mengakibatkan kerugian finansial yang signifikan bagi konsumen.

Pemerintah dan lembaga yang berwenang perlu mengambil langkah-langkah yang tegas untuk mengatasi tindak pidana penyalahgunaan data pribadi oleh perusahaan pinjaman online ilegal. Selain itu, edukasi dan kesadaran konsumen juga penting agar mereka dapat melindungi data pribadi mereka sendiri dan menghindari jatuh victim dari praktik-praktik ilegal tersebut.

D. Tantangan dalam Penegakan Hukum *Doxing*

Doxing, singkatan dari "*document tracing*" adalah praktik yang melibatkan pengungkapan dan penyebaran data pribadi seseorang secara ilegal. Tindakan ini seringkali didorong oleh motivasi yang beragam, seperti balas dendam, kejahatan siber, atau peretasan. Salah satu tantangan utama dalam penegakan hukum *Doxing* adalah kompleksitas teknologi yang digunakan oleh pelaku. Berikut ini adalah beberapa aspek utama dari kompleksitas ini :

1. **Teknik Penelusuran Data**

   Para pelaku *Doxing* menggunakan berbagai teknik penelusuran data untuk mengidentifikasi individu yang menjadi target mereka. Ini termasuk pencarian online, pemantauan media sosial, dan bahkan teknik-teknik yang lebih canggih seperti analisis metadata pada berkas gambar atau dokumen.

2. **Penggunaan Alat Otomatisasi**

   Dalam beberapa kasus, pelaku *Doxing* dapat menggunakan alat otomatisasi yang dirancang khusus untuk mengumpulkan informasi secara massal. Ini bisa mencakup web scraping atau perangkat lunak pengenalan wajah untuk mengidentifikasi individu dalam foto atau video.

3. **Kriptografi**

   Para pelaku *Doxing* sering menggunakan teknologi kriptografi untuk melindungi identitas mereka dan mengamankan data yang mereka curi. Ini membuat pelacakan mereka lebih sulit.

4. **Jaringan Gelap**

   Sebagian besar pelaku *Doxing* beroperasi di dunia maya yang gelap, di mana identitas mereka benar-benar disembunyikan. Mereka dapat menggunakan jaringan Tor atau layanan VPN untuk menyembunyikan alamat IP mereka.

5. **Penyebaran Data**

   Setelah mendapatkan data pribadi, pelaku *Doxing* menggunakan berbagai saluran, termasuk forum daring, situs web gelap, atau media sosial, untuk menyebarkan informasi tersebut. Ini memperumit proses penelusuran dan penegakan hukum.

Salah satu ciri khas pelaku *Doxing* adalah mereka sering bersembunyi di balik identitas palsu atau anonim. Ini adalah strategi yang digunakan untuk menghindari tanggung jawab hukum dan memberikan tingkat perlindungan terhadap upaya penegakan hukum. Tantangan yang terkait dengan anonimitas pelaku *Doxing* adalah:

1. **Identitas Palsu**

   Pelaku *Doxing* sering menggunakan identitas palsu saat beroperasi online. Mereka dapat membuat akun media sosial atau forum dengan nama palsu yang sulit dilacak.

2. **Penggunaan Layanan Anonim**

   Ada layanan dan alat yang memungkinkan pengguna untuk menjaga anonimitas mereka secara online. Ini termasuk jaringan Tor, layanan VPN, atau bahkan layanan email anonim.

3. **Penghapusan Jejak**

   Pelaku *Doxing* cenderung berhati-hati dalam menjaga jejak online mereka. Mereka dapat menghapus informasi pribadi mereka dari internet atau menggunakan teknik-teknik untuk mengaburkan jejak digital mereka.

Efektivitas penegakan hukum dalam kasus-kasus *Doxing* juga bergantung pada kerangka hukum yang ada. Sayangnya, beberapa yurisdiksi mungkin belum memiliki undang-undang yang cukup kuat atau jelas yang mengatasi *Doxing*. Tantangan terkait hukum dalam penegakan hukum *Doxing* meliputi:

1. **Definisi yang Belum Jelas**

   Beberapa undang-undang mungkin tidak memiliki definisi yang jelas tentang apa yang termasuk dalam *Doxing*. Ini dapat mengaburkan penegakan hukum dan memberikan ruang bagi pelaku untuk menghindari hukuman.

2. **Keterbatasan Yurisdiksi**

   Doxing sering melibatkan pelaku dari berbagai yurisdiksi Hukum. Ini dapat membuat penegakan hukum sulit karena hukum satu negara mungkin tidak mencakup pelaku di negara lain.

3. **Tingkat Hukuman yang Tidak Seimbang**

   Hukuman yang ditetapkan untuk pelaku *Doxing* mungkin tidak seimbang dengan kerugian yang diderita korban. Ini dapat mengurangi insentif untuk mengejar kasus-kasus *Doxing*.

4. **Lemahnya Aspek Perlindungan Korban**

   Salah satu aspek yang tidak kalah pentig untuk diperhatikan dari adanya suatu tindak pidana yakni keadaan korban setelah tindak pidana itu terjadi. Perlunya penerapan Restitusi dalam perkara tindak pidana *Doxing*. Restitusi merupakan ganti kerugian yang diberikan kepada korban atau keluarganya oleh pelaku atau pihak ketiga[11].

Penegakan hukum *Doxing* adalah tugas yang rumit dan memerlukan upaya kolaboratif dari berbagai lembaga penegak hukum, perusahaan teknologi, dan komunitas internasional. Dengan pemahaman yang lebih baik tentang kompleksitas teknologi, perlindungan identitas, perubahan hukum, dan kerjasama lintas batas, penegakan hukum *Doxing* dapat menjadi lebih efektif dalam melindungi privasi dan keamanan individu secara online.

IV. KESIMPULAN

Dalam penelitian ini, telah diidentifikasi bahwa penyebaran data pribadi ilegal, atau yang dikenal sebagai *Doxing*, merupakan salah satu tantangan serius dalam hukum cyber di Indonesia. Perkembangan teknologi informasi dan sektor Fintech yang pesat telah memperkuat kebutuhan untuk perubahan dan peningkatan dalam kerangka hukum yang

[11] Trias Saputra & Yudha Adi Nugraha, Pemenuhan Hak Restitusi : Upaya Pemulihan Korban Tindak Pidana, Krtha Bhayangkara Vol 16 No 1, 2022, pp 65-80 (https://ejurnal.ubharajaya.ac.id/index.php/KRTHA/article/view/1190/901)

mengatasi masalah ini. Dua undang-undang kunci, yaitu Undang-Undang No. 27 Tahun 2022 tentang Perlindungan Data Pribadi dan Undang-Undang ITE No. 19 Tahun 2016, memiliki peran penting dalam melindungi privasi individu dan menghukum pelaku *Doxing*. Namun, penegakan hukum *Doxing* masih dihadapkan pada sejumlah tantangan teknis dan hukum yang kompleks.

V. SARAN

Diperlukan upaya lebih lanjut untuk memperkuat kerangka hukum yang mengatasi *Doxing* dan penyalahgunaan data pribadi di sektor Fintech. Perubahan hukum yang lebih tegas dan sanksi yang lebih berat dapat menjadi deteren untuk pelaku *Doxing*. Selain itu, penegakan hukum perlu meningkatkan aktifitasnya dalam menginvestigasi dan menindak pelaku *Doxing*. Pendidikan dan kesadaran publik tentang risiko *Doxing* dan cara melindungi data pribadi mereka perlu ditingkatkan. Program edukasi yang ditujukan kepada masyarakat dapat membantu individu lebih waspada terhadap potensi ancaman *Doxing*, serta memberikan wawasan tentang praktik cyber yang aman. *Doxing* sering melintasi batas negara, dan ini menambah kompleksitas dalam penegakan hukum. Oleh karena itu, perlu ditingkatkan kerjasama internasional dalam hal pertukaran informasi dan koordinasi penegakan hukum untuk mengatasi tindakan kejahatan *Doxing* yang melibatkan lebih dari satu yurisdiksi.

DAFTAR PUSTAKA

Buku

Sugiono. *Metode Penelitian Kuantitatif, Kualitatif, dan R&D*. Bandung: Alfabeta, 2019.

Zed, Mestika. *Metode penelitian kepustakaan*. 5 ed. Yayasan Pustaka Obor Indonesia, 2018.

Jurnal

Nastiti, Febriana Kesuma. "Perlindungan Hukum Pidana Terhadap Mahasiswa Universitas Islam Indonesia yang Mengalami *Doxing* oleh Akun Uiicantikganteng di Platform Instagram." Universitas Islam Indonesia, 2023.

Otoritas Jasa Keuangan. "Perusahaan Fintech Lending Berizin Per 9 Maret 2023," 2023. www.danacita.co.id.

Samad, Y.S & Persadha, P.D. "Pendekatan Intelijen Strategis Sebagai Upaya

Memberikan Perlindungan di Ruang Siber Dalam Konteks Kebebasan Menyatakan Pendapat." *Kajian* 27, no. 1 (2022): 31–42. https://jurnal.dpr.go.id/index.php/kajian/article/viewFile/3588/1071.

Emir Nurmansyah, Elsie F Hakim, D Meitiara P Bakrie and Fauzan Permana ABNR Counsellors at Law. "Fintech 2023, Definitive global law guides offering comparative analysis from top-ranked lawyers," 2023.

Khoirunisa, Dhea, Nia Desy Arifiani, Muhammad Rizqi, Maulana Endang, dan Kartini Panggiarti. "Analisis Peran Otoritas Jasa Keuangan (Ojk) dalam Mengawasi Pelayanan Pada Perusahaan Financial Technology (Fintech) di Indonesia" 2, no. 3 (2023): 127–32. https://doi.org/10.30640/inisiatif.v2i3.1108.

Trias Saputra & Yudha Adi Nugraha, Pemenuhan Hak Restitusi : Upaya Pemulihan Korban Tindak Pidana, Krtha Bhayangkara Vol 16 No 1, 2022, pp 65-80 (https://ejurnal.ubharajaya.ac.id/index.php/KRTHA/article/view/1190/901)

Peraturan Perundang-Undangan.

Undang-Undang Dasar Negara Republik Indonesia Tahun 1945.

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

Putusan Pengadilan Negeri 438/Pid.Sus/2020/PN Jkt.Utr

Website.

Kota, Pos. Terulang Lagi! Tak Terima Fotonya Dimanipulasi Seolah Bugil dengan Narasi "Open BO", Wanita di Cikarang Ini Laporkan Pinjol ke Polisi (n.d.).

Merdeka.com. Wanita di Jakut Jadi Korban *Doxing* "Open BO" Pinjaman Online (2021).

Muhammad Naufal, Kompas.com. Warga Cilincing Jadi Korban *Doxing* oleh Pinjol, Satgas Waspada Investigasi Minta Pelaku Ditangkap (2021).

Uiicantikganteng di Platform Instagram." Universitas Islam Indonesia, 2023.

Otoritas Jasa Keuangan. "Perusahaan Fintech Lending Berizin Per 9 Maret 2023," 2023. www.danacita.co.id.