

**PENEGAKAN HUKUM TERHADAP TINDAK PIDANA *PHISHING*  
DIHUBUNGKAN DENGAN UNDANG UNDANG NO 19 TAHUN 2016  
TENTANG INFORMASI DAN TRASNSAKSI ELEKTRONIK  
*LAW ENFORCEMENT AGAINST PHISHING CRIMES IN RELATION TO  
LAW NO. 19 OF 2016 ON ELECTRONIC INFORMATION AND  
TRANSACTIONS***

**Muhammad Akhdan Alif Rizaldy, Muhammad Gary Gagarin Akbar dan  
Muhamad Abas**

**Fakultas Hukum, Universitas Buana Perjuangan Karawang**

Korespondensi Penulis: Hk22.muhammadrizaldy@mhs.ubpkarawang.ac.id,  
gary.akbar@ubpkarawang.ac.id, muhamad.abas@ubpkarawang.ac.id

Citation Structure Recommendation :

Rizaldy, Muhammad Akhdan Alif, Muhammad Gary Gagarin Akbar dan Muhamad Abas.  
*Penegakan Hukum terhadap Tindak Pidana Phishing Dihubungkan dengan Undang Undang No  
19 Tahun 2016 tentang Informasi dan Trasnsaksi Elektronik*. Lex Generalis. Vol.7. No.7 (2026).

**ABSTRAK**

Penelitian ini bertujuan menganalisis pengaturan hukum serta efektivitas penegakan hukum terhadap tindak pidana *phishing* di Indonesia berdasarkan Undang-Undang Nomor 19 Tahun 2016 tentang Informasi dan Transaksi Elektronik dan Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi. Penelitian menggunakan metode yuridis empiris dengan pendekatan peraturan perundang-undangan dan wawancara. Hasil penelitian menunjukkan bahwa pengaturan mengenai *phishing* masih bersifat umum sehingga belum mengakomodasi seluruh perkembangan modus kejahatan. Selain itu, penegakan hukum belum optimal karena keterbatasan aparat, rendahnya literasi digital masyarakat dan minimnya pelaporan korban. Oleh karena itu, diperlukan penguatan regulasi, peningkatan kapasitas aparat dan edukasi masyarakat.

**Kata Kunci:** Kejahatan Siber, Penegakan Hukum, Perlindungan Data Pribadi, *Phishing*, Undang Undang Informasi Transaksi Elektronik

**ABSTRACT**

*This study aims to analyze the legal regulation and the effectiveness of law enforcement against phishing crimes in Indonesia based on Law Number 19 of 2016 concerning Electronic Information and Transactions and Law Number 27 of 2022 concerning Personal Data Protection. This research employs an empirical juridical method using statutory and interview approaches. The findings indicate that the legal regulation of phishing remains general and has not fully accommodated the development of phishing methods. Law enforcement is also not yet optimal due to limited institutional capacity, low levels of digital literacy and the lack of victim reporting. Therefore, strengthening legal regulations and preventive measures is essential.*

**Keywords:** *Electronic Information and Transactions Law, Law Enforcement, Personal Data Protection, Cybercrime, Phishing*

## A. PENDAHULUAN

Transformasi digital yang semakin meluas dalam kehidupan masyarakat telah mengubah cara individu berinteraksi, bekerja dan melakukan berbagai aktivitas, termasuk dalam bidang komunikasi dan transaksi keuangan. Kemudahan akses internet memungkinkan berbagai kegiatan dilakukan secara daring dengan tingkat efisiensi yang tinggi. Di samping manfaat yang ditawarkan, kemajuan tersebut juga membawa konsekuensi yang ditandai dengan peningkatan potensi pelanggaran hukum berbasis teknologi yang dikenal sebagai *cybercrime*. Salah satu bentuk aktivitas ilegal yang sering terjadi dan menonjol dikenal sebagai *phishing*, yaitu praktik penipuan yang dilakukan dengan memanfaatkan rekayasa identitas pihak terpercaya untuk memperoleh informasi pribadi korban melalui media elektronik.<sup>1</sup>

Peningkatan penggunaan internet di Indonesia turut diiringi dengan bertambahnya kasus *phishing* yang menasar berbagai lapisan masyarakat, baik individu maupun institusi. Pelaku memanfaatkan berbagai metode, seperti pengiriman pesan elektronik, tautan mencurigakan, hingga pembuatan situs tiruan yang menyerupai platform resmi. Temuan tersebut mengindikasikan bahwa kemajuan teknologi selain memberikan kemudahan, tetapi juga menciptakan celah bagi terjadinya penyalahgunaan yang merugikan pengguna.<sup>2</sup>

Seiring dengan meningkatnya intensitas serangan *phishing*, kejahatan siber semakin berkembang menjadi ancaman nyata dalam ekosistem digital. Tingginya jumlah insiden yang terjadi menunjukkan bahwa sistem elektronik masih memiliki tingkat kerentanan tertentu, yang diperparah oleh rendahnya kesadaran masyarakat dalam menjaga keamanan data pribadi. Hal ini mengindikasikan bahwa perkembangan teknologi belum sepenuhnya diimbangi dengan kesiapan pengguna dalam menghadapi risiko keamanan digital. Fenomena tersebut tercermin dalam berbagai kasus *phishing* yang terjadi di Indonesia.

---

<sup>1</sup> Elshavira Suryaning Tyas dan Adhining Prabawati Rahmahani, *Analisis Kepastian Hukum Terkait Pencegahan Tindak Pidana Penipuan Online Berdasarkan Undang-Undang ITE: Penelitian*, Jurnal Pengabdian Masyarakat dan Riset Pendidikan, Vol.4, No.3 (2026).

<sup>2</sup> Triyanto, *Penegakan Hukum Tindak Pidana Cyber Crime dalam Bentuk Phising di Indonesia*, Majalah Ilmiah Gema, Vol.35, No.2 (2023).

Salah satu kasus yang banyak diberitakan media adalah penipuan yang mengatasnamakan layanan perbankan melalui pengiriman tautan palsu kepada nasabah. Korban diarahkan untuk mengakses situs yang menyerupai laman resmi bank dan diminta memasukkan data pribadi, seperti username, password, serta kode OTP. Informasi tersebut kemudian dimanfaatkan pelaku untuk mengambil alih rekening korban dan melakukan transaksi tanpa izin. Kasus ini menunjukkan bahwa *phishing* masih menjadi ancaman serius yang memanfaatkan rendahnya kewaspadaan masyarakat dalam menjaga keamanan data pribadi.<sup>3</sup>

Kerugian bukan satu-satunya dampak yang ditimbulkan, tetapi juga mencakup risiko nonmateriil, contohnya berupa kebocoran data pribadi yang berpotensi digunakan secara tidak sah untuk berbagai aktivitas ilegal lanjutan. Dalam jangka panjang, kondisi tersebut dapat memengaruhi tingkat keyakinan masyarakat terhadap keamanan perangkat digital yang digunakan dalam kehidupan sehari-hari.

Dari sisi normatif, Indonesia telah memiliki dasar hukum melalui ketentuan hukum Nomor Undang-Undang Nomor 19 Tahun 2016 tentang Informasi dan Transaksi Elektronik mencakup pengaturan terkait berbagai kejahatan di ruang siber, termasuk akses ilegal, penyebaran informasi menyesatkan, serta manipulasi data. Selain itu, keberadaan Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi ketentuan tersebut menjadi dasar hukum yang mengatur perlindungan informasi milik individu. Kendati demikian, pada praktiknya masih terdapat berbagai kendala, seperti kesulitan dalam pembuktian berbasis elektronik, keterbatasan kemampuan forensik digital, serta kompleksitas yurisdiksi lintas negara.

Kondisi Regulasi yang telah ada masih belum sepenuhnya mampu, sebagaimana tercermin dari kondisi tersebut mengikuti dinamika perkembangan kejahatan siber di sisi lain, perlindungan terhadap korban masih belum berjalan optimal, yang juga dipengaruhi oleh rendahnya tingkat literasi digital masyarakat.

---

<sup>3</sup> Kompas, *Viral Saldo Rekening Hilang, Begini Saran BRI agar Uang Tetap Aman di Bank*, diakses dari [https://activity.kompas.com/baca-cepat/xplore/biz/read/2024/04/28/083436828/viral-saldo-rekening-hilang-begini-saran-bri-agar-uang-tetap-aman-di-bank?utm\\_source=](https://activity.kompas.com/baca-cepat/xplore/biz/read/2024/04/28/083436828/viral-saldo-rekening-hilang-begini-saran-bri-agar-uang-tetap-aman-di-bank?utm_source=), diakses pada 16 Juli 2026.

Hal tersebut meningkatkan risiko masyarakat menjadi korban *phishing*, sehingga pendekatan yang digunakan perlu melampaui fokus pada aspek regulasi, namun juga pada peningkatan kesadaran dan pemahaman masyarakat terhadap keamanan digital.<sup>4</sup>

Secara normatif, penanganan tindak pidana *phishing* dapat mengacu pada ketentuan dalam Undang-Undang Nomor 19 Tahun 2016 tentang Informasi dan Transaksi Elektronik serta Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi. Namun, kedua peraturan tersebut belum mengatur tindak pidana *phishing* secara eksplisit, sehingga penegakan hukumnya masih mengandalkan penerapan beberapa ketentuan yang memiliki keterkaitan dengan unsur-unsur perbuatan *phishing*. Berdasarkan kondisi empiris di wilayah Karawang, belum tersedianya unit khusus yang menangani kejahatan siber turut menunjukkan bahwa implementasi penegakan hukum masih belum optimal.

Secara de jure, Indonesia telah memiliki dasar hukum dalam penanganan tindak pidana *phishing* melalui Undang-Undang Nomor 19 Tahun 2016 tentang Informasi dan Transaksi Elektronik serta Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi. Meskipun demikian, kedua peraturan tersebut belum mengatur tindak pidana *phishing* secara eksplisit sehingga penegakan hukumnya masih mengacu pada ketentuan yang memiliki keterkaitan dengan unsur-unsur tindak pidana tersebut.

Sementara itu, secara de facto, penegakan hukum terhadap tindak pidana *phishing* masih menghadapi berbagai kendala. Berdasarkan hasil wawancara dan kondisi di wilayah Karawang, belum tersedianya unit khusus kejahatan siber serta rendahnya literasi digital masyarakat menyebabkan penanganan kasus *phishing* belum berjalan secara optimal. Kondisi ini menunjukkan masih terdapat kesenjangan antara pengaturan hukum yang berlaku dengan pelaksanaannya di lapangan.

Beberapa penelitian telah mengkaji tindak pidana *phishing* dari berbagai sudut pandang. Penelitian oleh Fauzan Mahdi Irawan, Muhammad Zibran Al Habsy dan Asmak Ul Hosnah menitikberatkan pada pertanggungjawaban pidana

---

<sup>4</sup> Fauzan Mahdi Irawan, dkk., *Pertanggungjawaban Pidana Pelaku Phishing dan Efektivitas Penegakan Hukum Berdasarkan UU Nomor 19 Tahun 2016 tentang Informasi dan Transaksi Elektronik*, Jurnal Komputer, Informasi dan Teknologi, Vol.5, No.2 (2025).

pelaku *phishing* berdasarkan UU ITE.<sup>5</sup> Sementara itu, Ahmad Fauzi Hasanudin lebih memfokuskan kajiannya pada perlindungan hukum bagi korban *phishing* yang mengalami kerugian finansial.<sup>6</sup> Penelitian lain oleh Benyamin mengkaji tindak pidana *phishing* melalui pendekatan yuridis normatif berdasarkan UU ITE.<sup>7</sup> Selain itu, D. Anjheli menganalisis efektivitas UU ITE dan UU PDP dalam menangani pelanggaran data akibat *phishing*.<sup>8</sup>

Berdasarkan uraian latar belakang dan penelitian terdahulu tersebut, penelitian ini bertujuan untuk menganalisis pengaturan hukum terhadap tindak pidana *phishing* berdasarkan Undang-Undang Nomor 19 Tahun 2016 tentang Informasi dan Transaksi Elektronik serta Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi. Selain itu, penelitian ini juga bertujuan untuk menganalisis efektivitas penegakan hukum terhadap tindak pidana *phishing* di Indonesia berdasarkan perspektif korban, sehingga diharapkan dapat memberikan gambaran mengenai kondisi pengaturan hukum dan implementasinya dalam praktik.

## **B. PEMBAHASAN**

### **1. Pengaturan Hukum terhadap Tindak Pidana *Phishing* dalam Undang-Undang Nomor 19 Tahun 2016 tentang Informasi dan Transaksi Elektronik dan Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi**

Transformasi bidang teknologi informasi dan komunikasi mengalami perluasan area digital sekaligus meningkatkan kompleksitas kejahatan siber, termasuk *phishing*. Kejahatan ini memanfaatkan kelemahan pengguna dalam menjaga keamanan data pribadi melalui berbagai bentuk rekayasa yang meniru pihak terpercaya. Dampaknya tidak terbatas pada kerugian ekonomi, tetapi juga mencakup aspek privasi maupun keamanan informasi individu.

---

<sup>5</sup> Fauzan Mahdi Irawan, dkk., *Op.Cit.*.

<sup>6</sup> Akhmad Fery Hasanudin dan A Basuki Babussalam, *Upaya Hukum bagi Korban Kejahatan Phising yang Menguras Saldo M-Banking*, Gagasan Hukum, Vol.6, No.1 (Juni 2024).

<sup>7</sup> Berdiawan Benyamin, *Analisis Yuridis Tindak Pidana Cyber Crime Phishing Ditinjau dari Undang-Undang Nomor 19 Tahun 2016*, Skripsi, Universitas Hasanuddin, Makassar, 2024.

<sup>8</sup> Devi Anjheli, *Privasi Digital dan Kejahatan Phishing di Indonesia: Evaluasi Kritis terhadap Efektivitas UU ITE dan UU PDP*, Staatsrecht: Jurnal Hukum Kenegaraan dan Politik Islam, Vol.4, No.1 (2025).



Kondisi tersebut menunjukkan bahwa peningkatan penggunaan teknologi belum sepenuhnya diimbangi dengan kesiapan pengguna dalam menghadapi risiko keamanan digital.

Dari perspektif hukum, Indonesia telah memiliki landasan melalui Undang-Undang Nomor 19 Tahun 2016 tentang Informasi dan Transaksi Elektronik serta Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi. Kedua regulasi tersebut memberikan kerangka dasar dalam penanganan aktivitas kriminal berbasis teknologi digital, termasuk perlindungan atas data pribadi. Di sisi lain, pengaturannya masih tergolong umum serta belum secara khusus mengatur praktik *phishing* yang terus berkembang<sup>9</sup>. Efektivitas pengamanan belum optimal, sebagaimana tercermin dari kondisi tersebut hukum tidak terbatas pada keberadaan regulasi, serta terhadap kemampuan norma hukum.<sup>10</sup>

Secara substansi, pengaturan yang ada telah mencakup berbagai aspek, seperti larangan, sanksi dan perlindungan korban sebagai upaya menjamin kepastian hukum. Akan tetapi, dalam praktiknya masih ditemukan sejumlah kendala, antara lain ketidakjelasan norma, keterbatasan kapasitas teknis, serta perubahan modus kejahatan yang berlangsung cepat. Keadaan ini menegaskan bahwa regulasi yang tersedia masih memerlukan penyempurnaan untuk mengimbangi kompleksitas praktik *phishing*. Di sisi lain, efektivitas penegakan hukum juga dipengaruhi oleh tingkat kesadaran masyarakat serta kesiapan penegak hukum dalam mengimplementasikan aturan yang berlaku. Dengan demikian, keberhasilan penanganan *phishing* bukan hanya ditentukan berdasarkan norma hukum, melainkan turut dipengaruhi oleh faktor implementasi sekaligus partisipasi masyarakat dalam menjaga keamanan data pribadi.<sup>11</sup>

---

<sup>9</sup> Indonesia, *Undang-Undang tentang Perlindungan Data Pribadi*, UU No.27 Tahun 2022, LN Tahun 2022 No.196, TLN No.6820.

<sup>10</sup> Bella Fistya Asherli dan Sidi Ahyar Wiraguna, *Perlindungan Keamanan Data Pribadi di Era Digital Menghadapi Serangan Phishing Ditinjau dari Undang-Undang Pelindungan Data Pribadi Nomor 27 Tahun 2022*, Jurnal Hukum, Administrasi Publik dan Negara, Vol.2, No.4 (2025).

<sup>11</sup> Nadila Cindy Qarolina, dkk., *Perlindungan Hukum bagi Korban Penyebaran Data yang Diretas Secara Ilegal Melalui Link Phishing*, Legal Dialogica, Vol.1, No.1 (2025).

Dalam kerangka Undang-Undang Nomor 19 Tahun 2016 tentang Informasi dan Transaksi Elektronik, *phishing* memang belum diatur secara spesifik, namun dapat dikaitkan dengan beberapa ketentuan.<sup>12</sup> Pasal 28 ayat (1) Undang-Undang Nomor 19 Tahun 2016 mengatur mengenai larangan menyebarkan berita bohong dan menyesatkan yang mengakibatkan kerugian konsumen dalam transaksi elektronik. Unsur-unsur yang terkandung dalam pasal ini meliputi adanya perbuatan menyebarkan informasi bohong atau menyesatkan, dilakukan dengan sengaja, serta menimbulkan kerugian bagi pihak lain dalam transaksi elektronik. Dalam praktik *phishing*, pelaku umumnya membuat pesan, tautan, atau situs web palsu yang menyerupai layanan resmi untuk mengelabui korban agar memberikan data pribadi maupun data perbankan. Dengan demikian, apabila terbukti memenuhi unsur penyebaran informasi yang menyesatkan hingga menimbulkan kerugian, Pasal 28 ayat (1) dapat diterapkan terhadap pelaku *phishing*, meskipun belum mengatur secara khusus mengenai tindak pidana tersebut.<sup>13</sup> Selain itu, Pasal 30 Undang-Undang Nomor 19 Tahun 2016 mengatur mengenai larangan mengakses komputer dan/atau sistem elektronik milik orang lain tanpa hak atau melawan hukum. Unsur pasal ini meliputi adanya tindakan mengakses sistem elektronik, dilakukan tanpa hak dan dilakukan dengan sengaja. Dalam tindak pidana *phishing*, pelaku memperoleh data akun korban melalui tipu muslihat, kemudian menggunakan data tersebut untuk mengakses rekening, akun media sosial, atau sistem elektronik lainnya tanpa izin pemiliknya. Oleh karena itu, unsur-unsur dalam Pasal 30 dapat terpenuhi sehingga pasal tersebut dapat dijadikan dasar hukum dalam menjerat pelaku *phishing*.<sup>14</sup> Selain itu, Pasal 30 Undang-Undang Nomor 19 Tahun 2016 mengatur mengenai larangan mengakses komputer dan/atau sistem elektronik milik orang lain tanpa hak atau melawan hukum. Unsur pasal ini meliputi adanya tindakan mengakses sistem elektronik, dilakukan tanpa hak dan dilakukan dengan sengaja. Dalam tindak pidana *phishing*,

---

<sup>12</sup> Indonesia, *Undang-Undang tentang Perubahan atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik*, Pasal 32 UU No.19 Tahun 2016, LN Tahun 2016 No.251, TLN No.5952.

<sup>13</sup> *Ibid.*.

<sup>14</sup> *Ibid.*, Pasal 28 ayat (1).

pelaku memperoleh data akun korban melalui tipu muslihat, kemudian menggunakan data tersebut untuk mengakses rekening, akun media sosial, atau sistem elektronik lainnya tanpa izin pemiliknya. Oleh karena itu, unsur-unsur dalam Pasal 30 dapat terpenuhi sehingga pasal tersebut dapat dijadikan dasar hukum dalam menjerat pelaku *phishing*.<sup>15</sup> Selanjutnya, Pasal 32 Undang-Undang Nomor 19 Tahun 2016 mengatur larangan mengubah, memindahkan, merusak, menghilangkan, atau mentransfer informasi elektronik maupun dokumen elektronik milik orang lain tanpa hak. Unsur pasal ini berkaitan dengan penyalahgunaan data elektronik yang dilakukan secara melawan hukum. Dalam praktik *phishing*, data pribadi yang berhasil diperoleh dari korban sering kali digunakan untuk kepentingan tertentu, seperti mengambil alih akun, melakukan transaksi tanpa izin, atau menyalahgunakan identitas korban. Dengan demikian, apabila terbukti memenuhi unsur penyalahgunaan data elektronik, Pasal 32 juga dapat diterapkan sebagai dasar hukum terhadap pelaku *phishing*.<sup>16</sup>

Berdasarkan analisis terhadap Pasal 28, Pasal 30 dan Pasal 32 Undang-Undang Nomor 19 Tahun 2016, ketiga pasal tersebut dapat digunakan sebagai dasar hukum dalam menindak pelaku *phishing*. Namun, ketentuan tersebut masih bersifat umum dan belum mengatur *phishing* secara eksplisit. Akibatnya, penegakan hukum masih memerlukan penafsiran terhadap unsur-unsur tindak pidana yang ada sehingga diperlukan pengaturan yang lebih spesifik agar mampu mengakomodasi perkembangan modus kejahatan *phishing* di era digital.

Meskipun demikian, ketiga pasal pengaturan yang ada masih belum spesifik karena cenderung bersifat umum *phishing*, sehingga menimbulkan keterbatasan dalam penerapannya. Hal ini menunjukkan perlunya penguatan ketentuan yang lebih sejalan dengan perkembangan kejahatan di ruang digital, khususnya dalam merespons modus *phishing* yang terus berkembang.

---

<sup>15</sup> *Ibid.*, Pasal 30 ayat (1), ayat (2) dan ayat (3).

<sup>16</sup> *Ibid.*, Pasal 32 ayat (1), ayat (2) dan ayat (3).



Di sisi lain, ketentuan dalam keberadaan Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi memberikan penegasan berkaitan data pribadi merupakan hak yang wajib dilindungi, sebagaimana tercermin dalam pengaturan mengenai hak subjek data dan kewajiban pengendali data. Namun, ketiadaan pengaturan yang secara tegas mengakomodasi mekanisme khusus terkait *phishing* menunjukkan bahwa upaya perlindungan hukum bagi korban masih belum memadai belum menemui kendala dalam implementasinya.

Kondisi tersebut mengindikasikan terlihat kesenjangan antara pengakuan normatif terhadap perlindungan data pribadi dan efektivitas perlindungan tersebut dalam praktik. Kondisi ini menuntut penerapan pendekatan yang tidak hanya berfokus pada penguatan regulasi, serta mencakup upaya peningkatan kemampuan aparat penegak hukum yang diiringi dengan edukasi masyarakat sebagai langkah preventif guna meminimalkan risiko terjadinya *phishing*.<sup>17</sup>

Dalam perspektif hukum pidana, penalisasi merupakan tahapan lanjutan setelah suatu perbuatan dikategorikan sebagai tindak pidana. Penalisasi diwujudkan melalui pemberian ancaman sanksi pidana terhadap pelaku sebagai bentuk perlindungan hukum bagi masyarakat. Dalam tindak pidana *phishing*, penalisasi berfungsi sebagai sarana represif untuk memberikan efek jera kepada pelaku serta mencegah terulangnya kejahatan serupa. Oleh karena itu, keberadaan sanksi pidana dalam UU ITE menjadi bagian penting dalam mendukung efektivitas penegakan hukum terhadap kejahatan siber.<sup>18</sup>

Meski kerangka hukum yang berlaku telah tersedia tergolong terpadu, pelaksanaannya masih menghadapi berbagai kendala, seperti keterbatasan kemampuan teknis aparat, kesulitan dalam pembuktian digital, serta persoalan yurisdiksi lintas negara. Kondisi ini menyebabkan perlindungan terhadap korban belum berjalan secara optimal.

---

<sup>17</sup> Indonesia, *Undang-Undang tentang Perlindungan Data Pribadi*, UU No.27 Tahun 2022, LN Tahun 2022 No.196, TLN No.6820.

<sup>18</sup> Zarisnov Arafat, *Kriminologi (Suatu Pengantar Teoritik)*, FBIS Publishing (FBIS UBP Karawang), Karawang, 2018, p.90-93.

Di sisi pengaturan yang bersifat khusus terkait hal tersebut masih belum tersedia *phishing* mengarah pada adanya kekosongan norma yang berpotensi menciptakan ketidakpastian hukum kondisi tersebut menuntut adanya pembaruan ketentuan yang lebih terperinci dan responsif terhadap perkembangan agar mampu mengakomodasi seluruh unsur perbuatan *phishing* secara lebih efektif. sekaligus memperkuat jaminan kepastian hukum serta perlindungan terhadap korban.<sup>19</sup> Kondisi tersebut menunjukkan bahwa kondisi perlindungan data pribadi di Indonesia regulasi yang berlaku belum berjalan secara optimal, khususnya akibat belum terdapat pengaturan yang komprehensif dan mengikat secara menyeluruh. Akibatnya, pelanggaran terhadap privasi masih kerap terjadi dalam berbagai bentuk. Situasi ini mencerminkan bahwa sistem perlindungan data pribadi belum sepenuhnya mampu memberikan jaminan keamanan bagi masyarakat di tengah pesatnya perkembangan teknologi digital.

Dengan demikian, diperlukan perbaikan sistem hukum yang tidak sekedar berfokus di aspek regulasi, serta mencakup peningkatan kesadaran dan tanggung jawab seluruh keterlibatan berbagai pihak, yaitu pemerintah, aparat penegak hukum, serta masyarakat, dalam menjaga keamanan data pribadi secara berkelanjutan.<sup>20</sup>

Upaya penanggulangan *phishing* memerlukan pendekatan yang komprehensif melalui langkah preventif dan represif yang dilakukan secara berkelanjutan. Pendekatan tersebut meliputi penguatan literasi digital masyarakat, penguatan koordinasi antar pihak penegak hukum, serta pengembangan kapasitas sumber daya manusia yang didukung oleh pemanfaatan teknologi. Langkah-langkah ini menjadi penting mengingat karakteristik kejahatan siber yang terus berkembang dan memerlukan respons yang adaptif.

Selain itu, diperlukan penyempurnaan regulasi yang lebih responsif terhadap dinamika atas kejahatan siber agar perlindungan hukum dapat berjalan secara efektif dan berkeadilan. Sehingga dengan demikian,

---

<sup>19</sup> Devi Anjheli, *Op.Cit.*.

<sup>20</sup> Kadek Rima Anggen Suari dan I Made Sarjana, *Menjaga Privasi di Era Digital: Perlindungan Data Pribadi di Indonesia*, Jurnal Analisis Hukum, Vol.6, No.1 (2023).

penanggulangan *phishing* tidak sekedar bertumpu dari sisi penindakan, sekaligus pada upaya preventif yang melibatkan peran aktif berbagai pihak.<sup>21</sup>

Perlindungan data pribadi tidak terbatas pada ditentukan oleh adanya regulasi, sekaligus oleh efektivitas pelaksanaan dan pengawasan di lapangan. Keterbatasan teknis, rendahnya tingkat kepatuhan, hambatan juga muncul dari lemahnya koordinasi antar lembaga dalam optimalisasi perlindungan hukum. Kondisi ini menunjukkan bahwa implementasi regulasi belum sepenuhnya berjalan optimal, sehingga diperlukan penguatan sistem pengawasan dan peningkatan kapasitas institusional secara berkelanjutan.<sup>22</sup>

Efektivitas pengaturan hukum terkait *phishing* perlu terus disesuaikan guna mengimbangi perkembangan kejahatan siber yang kian kompleks. Hal ini menunjukkan bahwa regulasi yang ada tidak bisa bersifat statis, melainkan harus berkembang seiring perubahan teknologi. Selain keadaan tersebut menunjukkan perlunya kerja sama yang kuat yang melibatkan pemerintah bersama aparat penegak hukum, sektor swasta, bersama masyarakat. Peningkatan kapasitas teknis, literasi digital, serta kesadaran hukum juga menjadi faktor penting dalam upaya pencegahan. Dengan adanya sinergi tersebut, diharapkan perlindungan hukum terhadap masyarakat dapat berjalan lebih efektif, adaptif dan berkelanjutan dalam menghadapi tantangan kejahatan siber di Indonesia.<sup>23</sup>

Efektivitas pengaturan hukum terkait *phishing* perlu terus disesuaikan untuk menyesuaikan dengan dinamika kejahatan siber yang semakin kompleks. Hal ini menunjukkan bahwa regulasi tidak dapat bersifat statis, melainkan harus berkembang seiring perubahan teknologi. Selain keadaan tersebut mengarah pada pentingnya sinergi yang kuat antara pemerintah,

---

<sup>21</sup> Yazid Haikal Lokapala, dkk., *Aspek Yuridis Kejahatan Phishing dalam Ketentuan Hukum di Indonesia*, Indonesian Journal of Criminal Law and Criminology, Vol.5, No.1 (2024).

<sup>22</sup> Muhammad Gustry dan Zainal Arifin Hoesein, *Peran Undang-Undang ITE dan Undang-Undang Perlindungan Data Pribadi dalam Perlindungan Data dan Privasi di Era Ekonomi Digital*, Jurnal Minfo Polgan, Vol.14, No.2 (2025).

<sup>23</sup> Mohammad Fadil Imran, *Preventing and Combating Cybercrime in Indonesia*, International Journal of Cyber Criminology, Vol.17, No.1 (2023).

aparatus penegak hukum, dengan melibatkan sektor swasta dan masyarakat dalam mendukung upaya penanggulangan.

Peningkatan kapasitas teknis, literasi digital, serta kesadaran hukum menjadi faktor penting dalam pencegahan *phishing*. Dengan adanya koordinasi dan dukungan berbagai pihak, perlindungan hukum diharapkan upaya yang ditujukan kepada masyarakat dapat berjalan lebih efektif dan adaptif dalam menghadapi dinamika kejahatan siber.<sup>24</sup>

## **2. Efektivitas Penegakan Hukum terhadap Tindak Pidana *Phishing* di Indonesia Berdasarkan Perspektif Korban**

Dalam perspektif viktimologi, korban merupakan pihak yang mengalami kerugian atau penderitaan akibat suatu tindak pidana, baik kerugian yang bersifat fisik, psikis, sosial, maupun ekonomi. Viktimologi tidak hanya mempelajari keberadaan korban, tetapi juga mengkaji proses seseorang menjadi korban (viktimisasi), faktor-faktor yang memengaruhinya, serta pentingnya perlindungan dan pemenuhan hak-hak korban dalam sistem peradilan pidana. Oleh karena itu, pendekatan viktimologi memberikan keseimbangan dalam penegakan hukum dengan tidak hanya berorientasi pada pelaku, tetapi juga memperhatikan kepentingan dan perlindungan terhadap korban.<sup>25</sup>

Kondisi tersebut juga perlu dianalisis berdasarkan Undang-Undang Nomor 3 Tahun 2006 tentang Perlindungan Saksi dan Korban. Pasal 7 memberikan berbagai hak kepada korban, antara lain memperoleh perlindungan, informasi mengenai perkembangan perkara, bantuan medis, rehabilitasi psikososial dan psikologis, program pemulihan, serta perlindungan dari ancaman digital. Ketentuan tersebut relevan dengan korban tindak pidana *phishing* karena kerugian yang dialami tidak hanya berupa kehilangan harta benda, tetapi juga penyalahgunaan data pribadi dan jejak digital yang berpotensi menimbulkan tindak pidana lanjutan.

---

<sup>24</sup> Sanchari Das, dkk., *All About Phishing: Exploring User Research through a Systematic Literature Review*, Prosiding 13th International Symposium on Human Aspects of Information Security & Assurance (2019).

<sup>25</sup> Zikra Askalani Azis dan Nurliman Prasetyo, *Konsep Viktimisasi dalam Perspektif Viktimologi*, Jurnal Multidisiplin Ilmu Akademik, Vol.3, No.2 (2026).

Namun, berdasarkan hasil wawancara dalam penelitian ini, sebagian korban lebih memilih segera menghubungi pihak bank dibandingkan melapor kepada aparat penegak hukum karena menganggap proses hukum berlangsung lama dan belum memberikan perlindungan maupun pemulihan secara optimal. Hal tersebut menunjukkan bahwa implementasi hak-hak korban sebagaimana diatur dalam Pasal 7 masih memerlukan penguatan agar perlindungan terhadap korban *phishing* dapat terlaksana secara efektif.<sup>26</sup>

Kelemahan pada aspek normatif hukum berdampak pada perlindungan korban *phishing*, karena ketentuan yang ada belum sepenuhnya mengakomodasi seluruh unsur perbuatan, sehingga menimbulkan kekaburan dan perbedaan penafsiran. Kondisi ini menyebabkan aparat penegak hukum menghadapi kendala dalam proses pembuktian, penentuan pasal, serta penerapan sanksi. Akibatnya, korban belum sepenuhnya memperoleh kepastian hukum, keadilan, maupun pemulihan yang memadai. Hal ini menunjukkan adanya kesenjangan antara pengaturan hukum sekaligus implementasi pelaksanaan hukum dalam menangani praktik *phishing* yang tergolong sebagai kejahatan siber di Indonesia.<sup>27</sup>

Dalam praktik penegakan hukum terhadap *phishing*, masih terdapat kendala dalam pembuktian alat bukti elektronik yang rentan dimanipulasi, digandakan, atau dihapus. Selain itu, perbedaan penafsiran, keterbatasan kemampuan teknis, serta sifat kejahatan yang lintas negara turut menyulitkan proses penanganan perkara. Kondisi ini menunjukkan bahwa penegakan hukum belum berjalan efektif, sehingga perlindungan dan pemulihan korban belum optimal.<sup>28</sup>

Mekanisme perlindungan terhadap korban kejahatan siber yang lemah sendiri menjadi suatu persoalan yang penting dalam penegakan hukum.

---

<sup>26</sup> Indonesia, *Undang-Undang tentang Pelindungan Saksi dan Korban*, Pasal 7 UU No.3 Tahun 2026, LN Tahun 2026 No.59, TLN No.7179.

<sup>27</sup> Ardi Saputra Gulo, Sahuri Lasmadi dan Kabib Nawawi, *Cyber Crime dalam Bentuk Phising Berdasarkan Undang-Undang Informasi dan Transaksi Elektronik*, PAMPAS: Journal of Criminal Law, Vol.1, No.2 (2020).

<sup>28</sup> Ibrahim Fikma Edrisy, *Pengantar Hukum Siber*, Sai Wawai Publishing, Metro, 2019.



Korban kerap tidak memperoleh akses yang memadai dalam proses pelaporan maupun pendampingan hukum, sehingga tingkat pelaporan cenderung rendah.<sup>29</sup> Selain itu, rendahnya literasi digital menyebabkan sebagian tanpa disadari, korban telah menjadi sasaran kejahatan. Situasi ini diperparah oleh respons aparat yang belum optimal, sehingga berdampak pada menurunnya kepercayaan masyarakat terhadap efektivitas penegakan hukum siber. Oleh karena itu, diperlukan penguatan kapasitas kelembagaan yang disertai dengan peningkatan literasi dan kesadaran hukum masyarakat guna memperkuat perlindungan korban secara lebih komprehensif.<sup>30</sup>

Untuk memperkuat analisis, penelitian ini dilengkapi dengan wawancara terhadap korban tindak pidana *phishing* di wilayah Karawang. Temuan menunjukkan bahwa kerentanan korban terutama dipicu oleh rendahnya pemahaman terhadap karakteristik kejahatan siber, sehingga tindakan pelaku tidak segera dikenali sebagai tindak pidana. Korban pada awalnya mempercayai pelaku sebagai pihak resmi dan mengikuti instruksi tanpa verifikasi, yang kemudian berujung pada transaksi mencurigakan dan potensi kerugian finansial. Dalam situasi tersebut, respons awal korban cenderung berfokus pada penyelamatan dana melalui pihak bank, bukan pada pelaporan kepada aparat penegak hukum.

Lebih lanjut, keengganan untuk melapor dipengaruhi oleh persepsi bahwa proses pelaporan bersifat rumit, memakan waktu, serta berpotensi menimbulkan biaya. Ketidadaan unit khusus penanganan kejahatan siber di tingkat daerah juga memperkuat keraguan terhadap efektivitas penegakan hukum. Temuan ini mengindikasikan adanya hambatan struktural sekaligus kesenjangan antara kerangka hukum yang tersedia dan implementasinya di lapangan. Akibatnya, mekanisme perlindungan korban belum berjalan optimal dan tingkat pelaporan cenderung rendah, yang pada akhirnya dapat menghambat efektivitas penegakan hukum atas tindak pidana *phishing*.<sup>31</sup>

---

<sup>29</sup> Ahmad Fadhil Jaelani dan Diky Dikrurahman, *Perlindungan Hukum Korban Pinjaman Online Illegal di Kota Cirebon*, Rewang Rencang: Jurnal Hukum Lex Generalis, Vol.7, No.7 (2026).

<sup>30</sup> Juanrico Alfaramona Sumarezs Titahelu, dkk., *Hukum Cyber*, Widina Media Utama, Bandung, 2023.

<sup>31</sup> Wawancara dengan Ilham Wahidin, Korban, Karawang 6 April 2026.

Sejalan dengan temuan sebelumnya, hasil wawancara dengan ahli IT menunjukkan bahwa rendahnya literasi digital masyarakat tidak hanya disebabkan oleh keterbatasan pengetahuan, tetapi juga oleh perilaku pengguna yang kurang waspada dalam berinteraksi di ruang digital. Masyarakat masih cenderung mempercayai pesan atau tautan mencurigakan tanpa melakukan verifikasi yang memadai. Faktor psikologis, seperti kepanikan, rasa percaya terhadap pihak yang dianggap resmi, serta iming-iming keuntungan, turut memperbesar kerentanan pengguna terhadap praktik *phishing*.<sup>32</sup>

Dalam praktiknya, kondisi tersebut dimanfaatkan oleh pelaku melalui berbagai modus, antara lain dengan membuat situs tiruan yang menyerupai platform resmi untuk memperoleh data pribadi korban. Pola keadaan ini mengindikasikan bahwa keberhasilan *phishing* tidak semata-mata bergantung pada kecanggihan teknik pelaku, tetapi juga pada kelemahan perilaku pengguna. Oleh karena itu, upaya pencegahan perlu diarahkan pada penguatan regulasi, serta terhadap peningkatan literasi digital sehingga berorientasi pada perubahan perilaku, khususnya dalam hal verifikasi informasi dan kewaspadaan terhadap aktivitas digital yang mencurigakan.<sup>33</sup>

Berdasarkan temuan empiris di lapangan, metode *phishing* di Indonesia, termasuk di wilayah Karawang, tidak hanya dilakukan melalui tautan atau situs yang menarik perhatian. Terdapat pula metode yang relatif kurang diketahui, yaitu melalui jaringan *Wifi* publik. Dalam praktiknya, pelaku memutus koneksi *Wifi* asli dan menggantinya dengan jaringan palsu yang telah dikendalikan. Ketika korban terhubung kembali ke jaringan tersebut, data pengguna berpotensi diakses dan disalahgunakan oleh pelaku.

Meskipun dibandingkan metode lainnya, metode ini termasuk yang membutuhkan waktu lebih lama dalam pelaksanaannya *phishing* melalui tautan atau situs, tingkat risikonya tetap tinggi karena korban sering tidak menyadari adanya manipulasi jaringan. Hal ini menunjukkan bahwa *phishing*

---

<sup>32</sup> Rahil Sasia Putri Harahap dan Fiona Chrisanta, *Pembatasan Klausul pada Perjanjian Baku dalam Upaya Perlindungan Konsumen melalui Undang-Undang Perlindungan Konsumen*, Rewang Rencang: Jurnal Hukum Lex Generalis, Vol.4, No.4 (2023).

<sup>33</sup> Wawancara dengan Garrick, Ahli IT, Karawang 23 April 2026.

tidak hanya mengandalkan rekayasa sosial, tetapi juga memanfaatkan kelemahan pada aspek keamanan jaringan. Dengan demikian, upaya pencegahan perlu melampaui fokus pada peningkatan literasi digital dan juga kesadaran keamanan jaringan, khususnya dalam penggunaan *Wifi* publik.

Kelemahan dalam implementasi hukum siber di Indonesia menunjukkan adanya ketidaksesuaian antara kerangka regulasi dan praktik di lapangan. Meskipun Undang-Undang Informasi dan Transaksi Elektronik telah tersedia sebagai dasar hukum, penerapannya kendala yang dihadapi masih beragam, salah satunya keterbatasan sumber daya manusia, kemampuan teknis, juga koordinasi antar lembaga. Di samping itu, kesulitan dalam melacak sifat anonim pelaku dan jangkauan lintas negara juga turut menghambat prosedur penegakan hukum. Kondisi tersebut mengindikasikan bahwa efektivitas penegakan hukum siber belum sepenuhnya optimal, sehingga perlindungan terhadap korban kejahatan siber masih menghadapi berbagai keterbatasan dalam praktiknya.<sup>34</sup>

Lebih lanjut, implementasi hukum siber masih menghadapi hambatan struktural yang memengaruhi efektivitas penanganan perkara. Meskipun perangkat hukum telah tersedia, pelaksanaannya belum konsisten akibat keterbatasan kesiapan institusi dan sarana pendukung. Selain itu, pemanfaatan teknologi oleh aparat penegak hukum dalam proses penyidikan belum optimal, sehingga penanganan kasus cenderung lambat. Kondisi ini berdampak pada korban karena proses penyelesaian menjadi berlarut dan belum memberikan kepastian hukum. Oleh karena itu, penguatan implementasi hukum melalui peningkatan kapasitas institusi dan pemanfaatan teknologi menjadi langkah penting untuk memperbaiki kinerja penegakan hukum serta perlindungan bagi korban pelanggaran hukum di dunia digital.<sup>35</sup>

---

<sup>34</sup> Agus Wibowo dan Joseph Teguh Santoso, *Hukum Siber dan Keamanan Informasi*, Penerbit Yayasan Prima Agus Teknik, Semarang, 2024.

<sup>35</sup> Zainal Arifin dan Emi Puasa Handayani, *Buku Ajar Hukum Siber Perspektif Pidana*, Gemilang Press Indonesia, Kediri, 2025.

Kelemahan implementasi hukum siber juga tercermin dari belum optimalnya perlindungan hak individu di ruang digital. Ketidaksiapan sistem serta rendahnya literasi hukum masyarakat menyebabkan aturan yang ada belum berjalan efektif, sehingga potensi pelanggaran tetap tinggi. Kondisi ini menggambarkan bahwa perlindungan yang diberikan melalui penegakan hukum masih belum optimal bagi masyarakat.<sup>36</sup>

Kondisi tersebut menunjukkan bahwa regulasi hukum siber belum sepenuhnya mampu mengikuti perkembangan teknologi informasi yang berlangsung cepat. Keterbatasan sumber daya manusia serta belum meratanya pemahaman aparat penegak hukum menyebabkan implementasi aturan belum optimal, sehingga belum mampu menjawab berbagai persoalan hukum di ruang digital secara efektif.<sup>37</sup> Kendala penegakan hukum siber dipengaruhi oleh perkembangan teknologi digital yang belum sepenuhnya dapat diimbangi oleh regulasi yang ada. Selain itu, tingkat literasi digital masyarakat yang masih rendah serta lemahnya koordinasi antar lembaga turut meningkatkan potensi kejahatan siber, sehingga upaya pencegahan dan penindakan belum berjalan optimal.<sup>38</sup> Kegagalan sistem perlindungan data juga dipengaruhi oleh rendahnya kesiapan infrastruktur keamanan digital serta belum optimalnya mekanisme pencadangan data.<sup>39</sup> Ketergantungan pada satu sistem tanpa mitigasi risiko yang memadai memperbesar dampak serangan siber, sehingga proses pemulihan menjadi lambat dan menimbulkan kerugian yang luas, khususnya bagi instansi pemerintah.<sup>40</sup>

Tantangan dalam penegakan hukum siber dipengaruhi oleh kompleksitas ruang digital, sifat lintas batas, serta anonimitas yang menyulitkan penentuan yurisdiksi serta identifikasi pelaku.

---

<sup>36</sup> Erry Fitrya Primadhany, dkk., *Pengantar Hukum Siber Indonesia*, Sada Kurnia Pustaka, Bekasi, 2025.

<sup>37</sup> Edi Saputra Hasibuan, *Pengantar Hukum Siber Indonesia*, Modul Pembelajaran, Universitas Bhayangkara Jakarta Raya, Bekasi, 2022, p.9-11.

<sup>38</sup> Seri Mughni Sulubara, Viridya Tasril dan Nurkhalisah, *Perlindungan Hukum Tindak Pidana Cybercrime dalam Cyberlaw di Indonesia: Perkembangan Teknologi dan Tantangan Hukum dalam Mewujudkan Cybersecurity*, Tahta Media Group, Sukoharjo, 2025.

<sup>39</sup> Raden Andhitya dan Jamaludin Umam, *Analisis Kritis terhadap Penegakan Hukum dalam Penanganan Kejahatan Siber pada Kasus Data Breach dalam Perspektif Hukum Pidana Indonesia*, Rewang Rencang: Jurnal Hukum Lex Generalis, Vol.6, No.7 (2025).

<sup>40</sup> Seri Mughni Sulubara, Viridya Tasril dan Nurkhalisah, *Op.Cit.*.

Ketidaksinkronan regulasi antarnegara, lemahnya kerja sama internasional, serta keterbatasan mekanisme bantuan hukum timbal balik turut menjadi hambatan. Selain itu, pesatnya perkembangan teknologi yang tidak diimbangi dengan kesiapan regulasi dan kapasitas aparat membuka celah bagi meningkatnya kejahatan siber.<sup>41</sup>

Permasalahan dalam penegakan hukum siber di Indonesia tidak hanya berkaitan dengan keterbatasan regulasi, tetapi juga kesiapan sistem hukum dalam menghadapi perkembangan teknologi yang dinamis. Peraturan yang ada belum sepenuhnya mampu mengakomodasi berbagai bentuk kejahatan, sehingga menimbulkan celah hukum. Selain itu, keterbatasan kapasitas aparat, minimnya pelatihan, serta sarana forensik digital turut menghambat proses pembuktian. Faktor kultural, seperti rendahnya kesadaran hukum masyarakat, juga memperburuk kondisi tersebut. Akibatnya, penegakan hukum belum berjalan secara efektif dan memerlukan penanganan yang komprehensif, baik dari aspek normatif, struktural, maupun kultural.<sup>42</sup>

Efektivitas penanganan kasus *phishing* melalui mekanisme hukum di Indonesia dalam merespons berbagai kompleksitas. Meskipun kerangka hukum telah tersedia, implementasinya masih belum mampu menjamin perlindungan yang optimal optimal bagi individu yang menjadi korban. Kompleksitas lintas yurisdiksi serta pesatnya perkembangan teknologi menuntut kemampuan adaptasi aparat penegak hukum.

Oleh karena itu, diperlukan sinergi antara penguatan regulasi, peningkatan kapasitas kelembagaan dan partisipasi masyarakat guna mewujudkan penegakan hukum yang lebih responsif, berkeadilan dan berorientasi pada perlindungan korban. Pendekatan tersebut juga perlu didukung oleh pemanfaatan teknologi dan penguatan koordinasi antar lembaga agar implementasi penegakan hukum dapat berjalan lebih optimal dan berkelanjutan.<sup>43</sup>

---

<sup>41</sup> Danrivanto Budhijanto, *Hukum Pelindungan Data Pribadi dan Data Nasional*, Logoz Publishing, Bandung, 2024, p.2-3.

<sup>42</sup> Dian Eka Kusuma Wardani, *Cyber Law*, Agma, Gowa, 2024.

<sup>43</sup> Citranu, dkk., *Hukum Siber*, Get Press Indonesia, Padang, 2024.



Sebagai perbandingan, Singapura telah memperkuat penanggulangan tindak pidana *phishing* melalui Computer Misuse Act dan Online Criminal Harms Act 2023. Pengaturan tersebut memberikan kewenangan kepada pemerintah untuk memerintahkan pemblokiran situs *phishing*, menghapus konten berbahaya, serta mempercepat koordinasi antara aparat penegak hukum, penyedia layanan digital dan lembaga keuangan dalam melindungi masyarakat. Dibandingkan dengan Indonesia yang masih menggunakan beberapa ketentuan umum dalam UU ITE dan UU Perlindungan Data Pribadi, pengaturan di Singapura lebih spesifik sehingga mampu memberikan respons yang lebih cepat terhadap perkembangan modus *phishing*. Oleh karena itu, Indonesia dapat menjadikan penguatan regulasi dan koordinasi antarinstansi sebagai salah satu upaya meningkatkan efektivitas penegakan hukum terhadap tindak pidana *phishing*.<sup>44</sup>

Efektivitas penegakan hukum *phishing* di Indonesia masih menghadapi tantangan multidimensional. Meski kerangka hukum tersedia, implementasi belum optimal melindungi korban. Kompleksitas lintas yurisdiksi dan perkembangan teknologi menuntut adaptasi aparat. Diperlukan sinergi regulasi, kapasitas kelembagaan dan partisipasi masyarakat guna mewujudkan sistem penegakan hukum yang responsif, berkeadilan dan berorientasi pada perlindungan korban.<sup>45</sup>

### **C. PENUTUP**

Penelitian ini menunjukkan bahwa pengaturan hukum terhadap tindak pidana *phishing* di Indonesia telah memiliki dasar hukum melalui Undang-Undang Nomor 19 Tahun 2016 tentang Informasi dan Transaksi Elektronik serta Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi. Namun, kedua regulasi tersebut belum mengatur *phishing* secara khusus sehingga masih menimbulkan kendala dalam penerapannya. Dilihat dari sisi penegakan hukum, efektivitas penanganan tindak pidana *phishing* juga belum optimal. Hasil penelitian menunjukkan bahwasanya keterbatasan kemampuan teknis aparat,

---

<sup>44</sup> Online Criminal Harms Act 2023 (Act No. 24 of 2023), Singapore.

<sup>45</sup> Erry Fitrya Primadhany, dkk., *Op.Cit.*.

**Muhammad Akhdan Alif Rizaldy, Muhammad Gary Gagarin Akbar dan Muhamad Abas**

***Penegakan Hukum terhadap Tindak Pidana Phishing Dihubungkan dengan Undang-Undang No 19 Tahun 2016 tentang Informasi dan Transaksi Elektronik***

belum meratanya unit siber di daerah, rendahnya literasi digital masyarakat, serta minimnya kepercayaan korban untuk melapor menjadi faktor yang memengaruhi efektivitas penegakan hukum.

Oleh karena itu, diperlukan langkah yang lebih operasional, antara lain penyusunan pengaturan yang lebih spesifik mengenai tindak pidana *phishing*, peningkatan kapasitas penyidik melalui pelatihan forensik digital secara berkala, pembentukan atau penguatan unit siber pada tingkat kepolisian daerah yang belum memiliki unit khusus, serta peningkatan kerja sama antara kepolisian, perbankan, penyelenggara sistem elektronik dan Kementerian Komunikasi dan Digital dalam percepatan pemblokiran situs maupun rekening yang terindikasi digunakan untuk *phishing*. Selain itu, edukasi mengenai keamanan digital perlu dilakukan secara berkelanjutan kepada masyarakat agar mampu mengenali berbagai modus *phishing* dan mengurangi risiko menjadi korban.



## **DAFTAR PUSTAKA**

### **Buku**

- Arafat, Zarisnov. 2018. *Kriminologi (Suatu Pengantar Teoritik)*. (Karawang: FBIS Publishing (FBIS UBP Karawang)).
- Arifin, Zainal dan Emi Puasa Handayani. 2025. *Buku Ajar Hukum Siber Perspektif Pidana*. (Kediri: Gemilang Press Indonesia).
- Budhijanto dan rivanto. 2024. *Hukum Pelindungan Data Pribadi dan Data Nasional*. (Bandung: Logoz Publishing).
- Citrano, dkk.. 2024. *Hukum Siber*. (Padang: Get Press Indonesia).
- Edrisy, Ibrahim Fikma. 2019. *Pengantar Hukum Siber*. (Metro: Sai Wawai Publishing).
- Primadhany, Erry Fitrya, dkk.. 2025. *Pengantar Hukum Siber Indonesia*. (Bekasi: Sada Kurnia Pustaka).
- Sulubara, Seri Mughni, Viridya Tasril dan Nurkhalisah. 2025. *Perlindungan Hukum Tindak Pidana Cybercrime dalam Cyberlaw di Indonesia: Perkembangan Teknologi dan Tantangan Hukum dalam Mewujudkan Cybersecurity*. (Sukoharjo: Tahta Media Group).
- Titahelu, Juanrico Alfaromona Sumarezs, dkk.. 2023. *Hukum Cyber*. (Bandung: Widina Media Utama).
- Wardani, Dian Eka Kusuma. 2024. *Cyber Law*. (Gowa: Agma).
- Wibowo, Agus dan Joseph Teguh Santoso. 2024. *Hukum Siber dan Keamanan Informasi*. (Semarang: Penerbit Yayasan Prima Agus Teknik).

### **Publikasi**

- Andhitya, Raden dan Jamaludin Umam. *Analisis Kritis terhadap Penegakan Hukum dalam Penanganan Kejahatan Siber pada Kasus Data Breach dalam Perspektif Hukum Pidana Indonesia*. Rewang Rencang: Jurnal Hukum Lex Generalis. Vol.6. No.7 (2025).
- Anjheli, Devi. *Privasi Digital dan Kejahatan Phishing di Indonesia: Evaluasi Kritis terhadap Efektivitas UU ITE dan UU PDP*. Staatsrecht: Jurnal Hukum Kenegaraan dan Politik Islam. Vol.4. No.1 (2025).
- Asherli, Bella Fistya dan Sidi Ahyar Wiraguna. *Perlindungan Keamanan Data Pribadi di Era Digital Menghadapi Serangan Phishing Ditinjau dari Undang-Undang Pelindungan Data Pribadi Nomor 27 Tahun 2022*. Jurnal Hukum, Administrasi Publik dan Negara. Vol.2. No.4 (2025).
- Azis, Zikra Askalani dan Nurliman Prasetyo. *Konsep Viktimisasi dalam Perspektif Viktimologi*. Jurnal Multidisiplin Ilmu Akademik. Vol.3. No.2 (2026).
- Das, Sanchari, dkk.. *All About Phishing: Exploring User Research through a Systematic Literature Review*. Prosiding 13th International Symposium on Human Aspects of Information Security & Assurance (2019).
- Gulo, Ardi Saputra, Sahuri Lasmadi dan Kabib Nawawi. *Cyber Crime dalam Bentuk Phising Berdasarkan Undang-Undang Informasi dan Transaksi Elektronik*. PAMPAS: Journal of Criminal Law. Vol.1. No.2 (2020).
- Gustryan, Muhammad dan Zainal Arifin Hoesein. *Peran Undang-Undang ITE dan Undang-Undang Perlindungan Data Pribadi dalam Perlindungan Data dan Privasi di Era Ekonomi Digital*. Jurnal Minfo Polgan. Vol.14. No.2 (2025).

**Muhammad Akhdan Alif Rizaldy, Muhammad Gary Gagarin Akbar dan Muhamad Abas**

***Penegakan Hukum terhadap Tindak Pidana Phishing Dihubungkan dengan Undang-Undang No 19 Tahun 2016 tentang Informasi dan Transaksi Elektronik***

- Harahap, Rahil Sasia Putri dan Fiona Chrisanta. *Pembatasan Klausul pada Perjanjian Baku dalam Upaya Perlindungan Konsumen melalui Undang-Undang Perlindungan Konsumen*. Rewang Rencang: Jurnal Hukum Lex Generalis. Vol.4. No.4 (2023).
- Hasanudin, Akhmad Fery dan A Basuki Babussalam. *Upaya Hukum bagi Korban Kejahatan Phising yang Menguras Saldo M-Banking*. Gagasan Hukum. Vol.6. No.1 (Juni 2024).
- Imran, Mohammad Fadil. *Preventing and Combating Cybercrime in Indonesia*. International Journal of Cyber Criminology. Vol.17. No.1 (2023).
- Irawan, Fauzan Mahdi, dkk.. *Pertanggungjawaban Pidana Pelaku Phishing dan Efektivitas Penegakan Hukum Berdasarkan UU Nomor 19 Tahun 2016 tentang Informasi dan Transaksi Elektronik*. Jurnal Komputer, Informasi dan Teknologi. Vol.5. No.2 (2025).
- Jaelani, Ahmad Fadhil dan Diky Dikrurahman. *Perlindungan Hukum Korban Pinjaman Online Ilegal di Kota Cirebon*. Rewang Rencang: Jurnal Hukum Lex Generalis. Vol.7. No.7 (2026).
- Lokapala, Yazid Haikal, dkk.. *Aspek Yuridis Kejahatan Phishing dalam Ketentuan Hukum di Indonesia*. Indonesian Journal of Criminal Law and Criminology. Vol.5. No.1 (2024).
- Novel, Saugi dan Achmad Edi Subiyanto. *Perlindungan Hukum terhadap Data Pribadi Konsumen dalam Tindak Pidana Phishing pada Jasa Layanan E-Commerce Tokopedia*. Jurnal Pendidikan Tambusai. Vol.9. No.2 (2025).
- Qarolina, Nadila Cindy, dkk.. *Perlindungan Hukum bagi Korban Penyebaran Data yang Diretas Secara Ilegal Melalui Link Phishing*. Legal Dialogica. Vol.1. No.1 (2025).
- Suari, Kadek Rima Anggen dan I Made Sarjana. *Menjaga Privasi di Era Digital: Perlindungan Data Pribadi di Indonesia*. Jurnal Analisis Hukum. Vol.6. No.1 (2023).
- Triyanto. *Penegakan Hukum Tindak Pidana Cyber Crime dalam Bentuk Phising di Indonesia*. Majalah Ilmiah Gema. Vol.35. No.2 (2023).
- Tyas, Elshavira Suryaning dan Adhining Prabawati Rahmahani. *Analisis Kepastian Hukum Terkait Pencegahan Tindak Pidana Penipuan Online Berdasarkan Undang-Undang ITE: Penelitian*. Jurnal Pengabdian Masyarakat dan Riset Pendidikan. Vol.4. No.3 (2026).

**Karya Ilmiah**

- Benyamin, Berdiawan. 2024. *Analisis Yuridis Tindak Pidana Cyber Crime Phishing Ditinjau dari Undang-Undang Nomor 19 Tahun 2016*. Skripsi. Makassar: Universitas Hasanuddin.
- Hasibuan, Edi Saputra. 2022. *Pengantar Hukum Siber Indonesia*. Modul Pembelajaran. Bekasi: Universitas Bhayangkara Jakarta Raya.

**Website**

- Kompas. *Viral Saldo Rekening Hilang, Begini Saran BRI agar Uang Tetap Aman di Bank*. diakses dari [https://activity.kompas.com/baca-cepat/xplore/biz/read/2024/04/28/083436828/viral-saldo-rekening-hilang-begini-saran-bri-agar-uang-tetap-aman-di-bank?utm\\_source=](https://activity.kompas.com/baca-cepat/xplore/biz/read/2024/04/28/083436828/viral-saldo-rekening-hilang-begini-saran-bri-agar-uang-tetap-aman-di-bank?utm_source=). diakses pada 16 Juli 2026.

**Sumber Hukum**

Undang-Undang Nomor 19 Tahun 2016 tentang Perubahan atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik. Lembaran Negara Republik Indonesia Tahun 2016 Nomor 251. Tambahan Lembaran Negara Republik Indonesia Nomor 5952.

Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi. Lembaran Negara Republik Indonesia Tahun 2022 Nomor 196. Tambahan Lembaran Negara Republik Indonesia Nomor 6820.

Undang-Undang Nomor 3 Tahun 2026 tentang Pelindungan Saksi dan Korban. Lembaran Negara Republik Indonesia Tahun 2026 Nomor 59. Tambahan Lembaran Negara Republik Indonesia Nomor 7179.

Singapore Online Criminal Harms Act 2023 (Act No. 24 of 2023).

**Sumber Lain**

Wawancara dengan Garrick. Ahli IT. Karawang 23 April 2026.

Wawancara dengan Ilham Wahidin. Korban. Karawang 6 April 2026.

