

Vol. 10, No. 1,  
Januari 2024

#### Article History

Received: 08/12/2023

Revised: 22/12/2023

Accepted: 10/01/2024

## Perlindungan Hukum Terhadap Korban *Phising* Terkait Pengiriman File Apk

Artanti Zahra Adisa<sup>1</sup>, Andriyanto Adhi Nugroho<sup>2</sup>

<sup>1</sup>Fakultas Hukum, Universitas Pembangunan Nasional Veteran Jakarta. Email:  
[2010611085@mahasiswa.upnvj.ac.id](mailto:2010611085@mahasiswa.upnvj.ac.id)

<sup>2</sup>Fakultas Hukum, Universitas Pembangunan Nasional Veteran Jakarta. Email:  
[andriyanto.adhi.n@upnvj.ac.id](mailto:andriyanto.adhi.n@upnvj.ac.id)

\*surel korespondensi (email correspondence): [2010611085@mahasiswa.upnvj.ac.id](mailto:2010611085@mahasiswa.upnvj.ac.id)

**Abstract:** *In Indonesia, technological advancements are undergoing rapid changes, and this can be beneficial for the daily needs of people. However, apart from the positive aspects of technology itself, there are also cyber threats present in society, for example, phising. Phising is a cybercrime that initially carried out by deceiving victims through the transmission of fake links. However, as it has evolved, phising is now conducted by sending files in apk format through Whatsapp. This research aims to understand the urgency of legal regulations regarding phising cases in Indonesia. The author employs the juridical normative legal research method with a legislative approach, namely Law Number 19 of 2016 concerning Amendments to Law Number 11 of 2008 about Electronic Information and Transactions and Law Number 11 of 2008 about Electronic Information and Transactions to address the issues. The findings reveal that the current technological regulations in Indonesia do not clearly address phising. The ITE Law doesn't explicitly include articles that explain about phising. It's hoped that the result of this research will enlighten the public to be more cautious and prompt the government to establish regulations specifically addressing phising. The purpose of this research is to provide enlightenment to the public to be more cautious, and to urge the government to promptly formulate regulations related to phising as a form of legal protection for phising victims. From this research, it can also be concluded that Indonesia need to enhance regulations related to phising within the ITE Law or to formulate separate legislation as a derivative of the ITE Law specifically addressing phising.*

**Keyword:** *legal protection; phising; apk files*

**Abstrak:** Di Indonesia, perkembangan teknologi dapat dikatakan memiliki perubahan yang sangat pesat dan hal tersebut dapat bermanfaat bagi kebutuhan kehidupan sehari-hari manusia. Namun, selain datangnya hal-hal positif dari teknologi itu sendiri, terdapat ancaman-ancaman kejahatan siber yang juga hadir di kehidupan masyarakat, contohnya adalah *phising*. *Phising* merupakan kejahatan siber yang pada awalnya dilakukan dengan menipu korban dengan mengirimkan link palsu, tetapi pada perkembangannya, *phising*

dilakukan melalui pengiriman file apk melalui platform *Whatsapp*. Penelitian ini bertujuan untuk mengetahui urgensi adanya pengaturan hukum terhadap kasus *phising* di Indonesia. Penulis dalam mengerjakan penelitian ini menggunakan metode penelitian hukum yuridis normative dengan pendekatan perundang-undangan yaitu Undang-Undang Nomor 19 Tahun 2016 Tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik dan Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik untuk menjawab permasalahan yang dibahas. Diketahui hasil dari penelitian ini ialah dengan berlakunya peraturan perundang-undangan terkait teknologi di Indonesia saat ini masih belum mengatur secara jelas terkait *phising* terutama yang dilakukan melalui pengiriman file apk, di dalam UU ITE tidak mencantumkan pasal-pasal yang menjelaskan terkait *phising* secara jelas dan tujuan dari penelitian ini adalah untuk memberikan pencerahan pengetahuan kepada masyarakat untuk lebih berhati-hati dan pemerintah untuk segera mengusung pengaturan terkait *phising* sebagai bentuk perlindungan hukum terhadap korban *phising*. Dari penelitian ini juga dapat disimpulkan jika Indonesia memiliki urgensi untuk menambah pengaturan terkait *phising* di dalam UU ITE, atau menyusun peraturan perundang-undangan sebagai turunan dari UU ITE yang membahas secara khusus terkait *phising*.

**Kata Kunci** : perlindungan hukum; *phising*; file apk

## PENDAHULUAN

Kemajuan ilmu dalam bidang teknologi telah membawa negara Indonesia pada era digital, dimana pada era tersebut, kemajuan teknologi seperti dalam penggunaan internet menjadi sesuatu yang krusial dalam membantu manusia mengerjakan pekerjaannya.<sup>1</sup> Salah satu contohnya adalah kegiatan transaksi yang kini berpindah dengan menggunakan teknologi seperti melalui gadget. Ketua Umum Asosiasi Penyelenggara Jasa Internet Indonesia (disingkat APJII), mengungkapkan data terkait pemakai internet dari tahun ke tahun yang selalu mengalami pertumbuhan. Seperti pada tahun 2022, diketahui melalui data tersebut jika kurang lebih 77% (tujuh puluh tujuh persen) penduduk di Indonesia menjadi pengguna internet atau mencapai sekitar 210 juta penduduk.<sup>2</sup> Hal tersebut merupakan penambahan sebanyak 35 juta pengguna internet yang terhitung sebelumnya pada tahun 2020 hanya sebesar 175 juta saja.<sup>3</sup> Namun, dengan bertambahnya jumlah penduduk di Indonesia yang menggunakan internet, bertambah juga ancaman terhadap para pengguna internet tersebut. Penggunaan teknologi seperti internet harus digunakan oleh orang-orang yang dapat menggunakannya dengan baik, karena jika teknologi dimanfaatkan oleh oknum yang ingin melakukan kejahatan, maka fungsi utama adanya kemajuan teknologi akan

---

<sup>1</sup> Iskandar Wibawa et al., "Era Digital (Pergeseran Paradigma Dari Hukum Modern Ke Post Modernisme)," *Masalah - Masalah Hukum* 45, no. 4 (2016): 285–91, <https://doi.org/10.14710/mmh.45.4.2016.285-291>.

<sup>2</sup> Intan Rakhmayanti Dewi, "Data Terbaru! Berapa Pengguna Internet Indonesia 2022?," CNBC Indonesia, June 9, 2022, <https://www.cnbcindonesia.com/tech/20220609153306-37-345740/data-terbaru-berapa-pengguna-internet-indonesia-2022>.

<sup>3</sup> Dewi.

tergantikan dengan sesuatu yang dapat merugikan orang.<sup>4</sup> Banyak oknum kejahatan yang memanfaatkan kemajuan teknologi untuk menguntungkan dirinya sendiri, tetapi merugikan orang lain. Kejahatan-kejahatan tersebut dikenal dengan kejahatan siber atau *cybercrime*.

*Cybercrime* merupakan suatu tindak kejahatan yang menjadikan internet sebagai ruang atau tempat dalam melakukan kejahatan tersebut.<sup>5</sup> Kejahatan-kejahatan tersebut mencakup kejahatan yang dilakukan melalui internet, kejahatan digital, dan kejahatan yang melibatkan jaringan telekomunikasi.<sup>6</sup> Kejahatan yang termasuk ke dalam *cybercrime* masuk ke dalam ranah hukum pidana. Dalam Kitab Undang-Undang Hukum Pidana (selanjutnya disebut KUHP) berisikan ketentuan-ketentuan hukum yang berfungsi sebagai pelindung untuk masyarakat di berbagai kepentingan, salah satunya dalam ancaman kemajuan teknologi yaitu pada kejahatan siber atau *cybercrime*,<sup>7</sup> seperti kasus-kasus pencurian data pribadi atau pembobolan saldo rekening korban. Pada penelitian ini, jenis kejahatan siber yang akan dibahas adalah kejahatan *phising*. *Phising* merupakan suatu tindakan kejahatan berupa penipuan dengan cara menipu korban dengan meniru situs terpercaya yang bertujuan untuk mengumpulkan informasi pribadi korban.<sup>8</sup> Akan tetapi pada kenyataannya, metode *phising* sendiri berkembang menjadi berbagai macam sehingga tidak terdapat definisi tetap dari kata *phising* karena terhitung dari berbagai cara pengaplikasian *phising* dan konteksnya.<sup>9</sup> Kasus *phising* biasanya dilakukan dengan cara pelaku menyamar sebagai pihak bank atau institusi keuangan dan mengirimkan sebuah email kepada korban yang berisikan sebuah link yang akan mengarahkan calon korban untuk mengisi data-data akun banknya.<sup>10</sup> Namun, seperti yang telah disebutkan, dalam perkembangannya cara kerja *phising* terus berkembang dengan berbagai cara untuk mencapai tujuannya yaitu mencuri data pribadi, seperti dimasukkannya beberapa kode berbahaya tanpa sepengetahuan pemilik komputer atau calon korban.<sup>11</sup>

Definisi tersebut terbukti dengan adanya kasus terkait *phising* yang terjadi di Indonesia baru-baru ini yaitu kasus *phising* tidak lagi dalam bentuk link mentah, melainkan link *phising* tersebut dimasukkan ke dalam aplikasi berformatkan *Android Package Kit*

---

<sup>4</sup> L E Reksten, *Using Technology to Increase Student Learning* (SAGE Publications, 2000), <https://books.google.co.id/books?id=P2QNhie84ikC>.

<sup>5</sup> Miftakhur Rokhman and Habibi-Isnatul Liviani, "Kejahatan Teknologi Informasi (Cyber Crime) Dan Penanggulangannya Dalam Sistem Hukum Indonesia" 23, no. 2 (2020).

<sup>6</sup> Yougal Joshi and Anand Singh, "A Study on Cyber Crime and Security Scenario in INDIA," *International Journal of Engineering and Management Research*, no. 3 (2013), [www.ijemr.net](http://www.ijemr.net).

<sup>7</sup> Fairuz Rhamdhatul Muthia dan Ridwan Arifin, "KAJIAN HUKUM PIDANA PADA KASUS KEJAHATAN MAYANTARA(CYBERCRIME) DALAM PERKARA PENCEMARAN NAMA BAIK DI INDONESIA" 5, no. 1 (2019), <https://doi.org/10.32661/resam.v5i1.18>.

<sup>8</sup> Vikran Fasyadhiyaksa Putra Y, "Modus Operandi Tindak Pidana Phising Menurut UU ITE," *Jurist-Diction* 4, no. 6 (November 5, 2021): 2525, <https://doi.org/10.20473/jd.v4i6.31857>.

<sup>9</sup> Zainab Alkhalil et al., "Phishing Attacks: A Recent Comprehensive Study and a New Anatomy," *Frontiers in Computer Science* (Frontiers Media S.A., March 9, 2021), <https://doi.org/10.3389/fcomp.2021.563060>.

<sup>10</sup> R Lininger and R D Vines, *Phishing: Cutting the Identity Theft Line* (Wiley, 2008), <https://books.google.co.id/books?id=dFK-trfdD1AC>.

<sup>11</sup> Lininger and Vines.

(selanjutnya disingkat apk). APK merupakan format distribusi biner untuk suatu aplikasi dalam Android, dan dokumen APK serupa dengan berkas yang telah dikompres seperti dokumen berformatkan Java Archive (JAR)/Zip.<sup>12</sup> Dalam kasus ini, jika file berformatkan APK tersebut diklik, maka dapat menyebabkan dicurinya data pribadi korban, seperti diambilnya uang dari rekening mbanking milik korban. Salah satu korban yang diberitakan oleh media adalah Ardi Maulana yang berasal dari Bakalanrajan, Malang. Saudara Ardi Maulana menjadi korban kasus *phising* ketika ia melaporkan telah kehilangan uang melalui *m-banking*nya setelah mengklik file yang dikirimkan oleh oknum yang menyamar menjadi kurir jasa antar barang dengan alasan ingin mengantarkan barang kepada korban. Setelah korban mengklik aplikasi berformat apk, setelah itu korban mendapatkan notifikasi melalui aplikasi *m-banking*nya jika ia baru saja terdapat kegiatan transaksi uang dengan jumlah Rp3.000.000,00- (tiga juta rupiah), padahal kenyataannya ia tidak melakukan transaksi apapun melalui *m-banking*nya. Korban telah melaporkan hal tersebut kepada pihak bank, dan pihak Bank segera melakukan pengecekan terhadap laporan Korban, tetapi setelah dilakukan proses tersebut, pihak Bank menyatakan jika mereka tidak memiliki tanggung jawab atas terjadinya kegiatan transaksi melalui *m-banking* yang pada kenyatannya tidak dilakukan oleh Korban tersebut.<sup>13</sup> Dengan maraknya kasus *phising* pengiriman file apk, Direktorat Tindak Pidana Siber Badan Reserse Kriminal Polisi Republik Indonesia (Selanjutnya disingkat dengan Dittipidsiber Bareskrim Polri) telah melakukan penindakan terhadap para pelaku yang berjumlah 58 orang, terhitung pada 30 Desember 2022 hingga 7 Januari 2023. Diketahui jika para pelaku menggunakan nama-nama jasa antar barang yang cukup ternama seperti J&T Express, JNE Express, Ninja Express, dan lainnya ketika melakukan penipuan.

Adanya kasus penipuan dan pembobolan rekening ini merupakan bentuk pelanggaran terhadap ketentuan peraturan-peraturan hukum yang berlaku di Indonesia, salah satunya yang tercantum dalam Pasal 30 Ayat (1), 32 Ayat (1), dan Pasal 35 Undang-Undang Informasi dan Transaksi Elektronik (UU ITE). Pasal 30 menegaskan jika setiap orang dilarang untuk melakukan pengaksesan komputer dan/atau sistem elektronik orang lain yang dilakukan secara sengaja, tanpa hak, atau melawan hukum yang berlaku dan dilakukan dengan cara apa pun. Dalam kasus penelitian ini, tidak terfokus hanya pada "komputer" saja, melainkan perangkat-perangkat lain seperti handphone. Kemudian, Pasal 32 Ayat (1) juga mengatur jika setiap orang tidak diperbolehkan melakukan perubahan, penambahan, pengurangan, melakukan pemindahan, perusakan, penghilangan, pemindahan, penyembunyian suatu informasi elektronik atau dokumen elektronik baik itu milik orang lain maupun milik publik. Dari ketentuan kedua pasal tersebut, sesuai dengan pelaku *phising* yang telah melawan hukum mengakses perangkat korban melalui file "apk" yang dikirimkannya dan pelaku juga telah memindahkan kepemilikan milik korban berupa uang

---

<sup>12</sup> S K Rakshit, *Ethical Hacker's Penetration Testing Guide: Vulnerability Assessment and Attack Simulation on Web, Mobile, Network Services and Wireless Networks (English Edition)* (New Delhi: BPB Publications, 2022).

<sup>13</sup> Dewi, "Data Terbaru! Berapa Pengguna Internet Indonesia 2022?"

yang ada di dalam rekening korban ke rekening miliknya. Yang menjadi dokumen elektronik sesuai dengan pasal adalah rekening koran milik korban. Rekening koran merupakan dokumen seperti buku tabungan yang memuat tanggal dan sandi transaksi, mutase debit, mutasi kredit, saldo, dan riwayat transaksi.<sup>14</sup> Dari rekening koran tersebut dapat menjadi alat bukti dengan diprint-out rekening koran milik korban yang bentuk aslinya berupa dokumen elektronik, seperti pada pembuktian pada kasus Putusan Pengadilan Negeri Makassar Nomor 1124/Pid.Sus/2020/PN.Mks yang menggunakan rekening koran sebagai alat bukti.<sup>15</sup> Lalu, dijelaskan juga pada Pasal 35 UU ITE yang mengatakan jika tidak diperbolehkannya pemalsuan atau penciptaan pada suatu informasi elektronik atau dokumen elektronik yang memiliki intensi supaya informasi atau dokumen elektronik yang telah dimanipulasi tersebut dianggap sebagai data yang otentik. Hal yang disebutkan di dalam Pasal 35 UU ITE tersebut hampir memenuhi aspek-aspek tindakan *phising*, meskipun dalam pasal tersebut tidak secara jelas mengatur terkait konsep *phising* karena tindakan *phising* merupakan kegiatan yang dilakukan pelaku untuk memancing dan menjebak korban untuk memasukkan informasi pribadinya sehingga pelaku dapat mengakses akun milik korban. Namun, beberapa ahli berpendapat jika Pasal 35 UU ITE tidak dapat masuk ke dalam setiap kasus rekayasa, sehingga tergantung pada motif dan kerugian yang ditimbulkan. Untuk kasus *phising* melalui file yang berformat file Apk, menurut saya Pasal 35 merupakan pasal yang sesuai karena pelaku *phising* tersebut melakukan manipulasi pada data korban ketika korban telah mengklik file Apk yang dikirimkan oleh pelaku.

Penelitian ini membawa kebaruan yaitu berupa mengangkat penelitian terkait terdapat adanya urgensi bagi Indonesia untuk segera menambahkan atau membuat peraturan perundang-undangan baru yang dengan jelas mengatur kejahatan siber berupa *phising* dikarenakan kejahatan siber tersebut telah banyak terjadi di Indonesia saat ini dengan membahas terkait faktor yang menjadi penyebab maraknya terjadi *phising* di Indonesia. Namun, Indonesia saat ini belum memiliki pengaturan khusus terkait hal tersebut, sehingga terjadi ketidakpastian hukum dalam penerapan penjatuan hukuman bagi para pelaku *phising* yang biasa disebut dengan *phiser*. Melihat permasalahan terkait *phising* yang merupakan masalah yang sangat penting karena Indonesia sendiri telah memasuki era "digital", dengan itu penulis tertarik untuk meninjau lebih seksama sehingga menjadikan kasus *phising* melalui aplikasi apk sebagai fokus permasalahan penelitian yang berjudul "Perlindungan Hukum terhadap Korban *Phising* Terkait Pengiriman File Apk".

## **METODE PENELITIAN**

Dalam mengerjakan penelitian ini, Penulis menetapkan metode penelitian kualitatif berupa yuridis normatif sebagai metode yang diterapkan dalam penyusunan penelitian ini

---

<sup>14</sup> Hery, *Akuntansi Keuangan Menengah*, ed. Guns, 1st ed. (Jakarta: PT Grasindo, 2020).

<sup>15</sup> Hilikia Dimas Krishnugraha, "Analisis Pembuktian Oleh Penuntut Umum Atas Putusan Tindak Pidana Perbankan Pencatatan Palsu," *Verstek* 7, no. 2 (2021): 418–26, <https://doi.org/10.20956/verstek.v7i2.xxxx>.

yang dalam pelaksanaannya akan menelaah aturan-aturan serta mulai dari asas dan prinsip hukum, lalu juga doktrin dan teori hukum, dan kepustakaan lainnya untuk menyelesaikan fokus permasalahan hukum yang diteliti dalam penelitian dengan mengaitkan keduanya.<sup>16</sup> Dalam pembahasannya, jenis penelitian yuridis normative ini memfokuskan pada doktrin dan asas yang terdapat di dalam ilmu hukum (asas yang tercantum dalam Pasal 5 dan 6 Undang-Undang Nomor 10 Tahun 2004 tentang Pembentukan Peraturan Perundang-undangan).<sup>17</sup> Penelitian menggunakan penelitian hukum normative merupakan tahapan mengaplikasikan atau mengkaitkan teori hukum terhadap fokus permasalahan yang menjadi pembahasan dalam penelitian ini.

Penulis menerapkan teknik pengumpulan data dengan cara studi kepustakaan dalam penyusunan penelitian ini. Studi kepustakaan merupakan penelitian yang tidak mendapatkan sumber data dengan pergi ke lapangan atau saksi-mata, penelitian dengan studi kepustakaan menggunakan sumber sekunder yang tersedia di perpustakaan seperti dengan membaca buku atau artikel yang memiliki pembahasan yang berkaitan dengan penelitian yang dilakukan tanpa dibatasi oleh ruang dan waktu.<sup>18</sup> Studi kepustakaan dapat dilihat ketika dalam penyusunan penelitian melakukan mencari literatur-literatur yang terdapat kaitan atau hubungannya dengan fokus pembahasan,<sup>19</sup> seperti dalam penelitian ini adalah terkait perlindungan hukum korban *phising* file APK.

## PEMBAHASAN

### A. Pengaturan Hukum bagi Korban *Phising* di Indonesia

Kasus *phising* melalui pengiriman file apk masuk ke dalam tindak kejahatan pidana, akan tetapi untuk pengaturan hukum pada kasus *phising* menggunakan UU ITE dikarenakan Indonesia memangku suatu asas yang berbunyi "*lex specialis derogate legi generali*". Asas tersebut mengandung makna jika terjadi suatu peristiwa yang bersifat special atau khusus, maka peraturan perundang-undangan yang digunakan harus sesuai dengan peristiwa tersebut agar lebih efektif dalam pelaksanaannya.<sup>20</sup> Meskipun Indonesia menganut asas tersebut dan menggunakan Undang-Undang Nomor 19 Tahun 2016 Tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik dan Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik (UU ITE) sebagai peraturan yang secara khusus membahas terkait kejahatan-kejatan siber seperti

---

<sup>16</sup> S H Suyanto, *Metode Penelitian Hukum Pengantar Penelitian Normatif, Empiris Dan Gabungan* (Gresik: Unigres Press, 2022).

<sup>17</sup> Zainuddin Ali, *Metode Penelitian Hukum* (Jakarta: Sinar Grafika, 2009).

<sup>18</sup> Mestika Zed, *Metode Penelitian Kepustakaan* (Jakarta: Yayasan Pustaka Obor Indonesia, 2014).

<sup>19</sup> Jonaedi Efendi and Johnny Ibrahim, *Metode Penelitian Hukum: Normatif Dan Empiris* (Depok: Prenadamedia Group, 2018).

<sup>20</sup> Bintara Sura Priambada, Ashinta Sekar Bidari, and Elisa Putri Oktaviani, "Law Enforcement against Cybercrime in Banking in the Form of Theft of Customer Data," *BIRCI - Journal* 5, no. 2 (2022), <https://doi.org/10.33258/birci.v5i2.5298>.

*phising*, tetapi jika melihat ketentuan-ketentuan yang terdapat di dalam UU ITE, tidak ada pasal-pasal yang memenuhi unsur-unsur *phising* dan hanya mendekati dari unsur *phising* itu sendiri dan menurut Penulis hal ini dapat menimbulkan ketidakpastian hukum dalam penerapannya. Kasus *phising* masuk ke dalam kategori kejahatan siber atau *cybercrime*, sehingga dalam pengaturan hukumnya menggunakan Undang-Undang Nomor 19 Tahun 2016 Tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik karena Undang-Undang ini memiliki sifat "khusus" yang dalam pengimplementasiannya digunakan untuk mengatur penggunaan teknologi di Indonesia. Meskipun UU ITE tidak menjelaskan secara jelas terkait *phising*, terdapat beberapa pasal yang dirasa dapat menjadi payung hukum atas kasus *phising*, yaitu Pasal 30 Ayat (1), Pasal 32, dan Pasal 35 UU ITE. Berikut penjelasan dari pasal-pasal tersebut:

- Pasal 30 Ayat (1) UU ITE

Pasal 30 Ayat (1) UU ITE mengatakan jika setiap orang dilarang untuk melakukan pengaksesan komputer dan/atau sistem berbasis elektronik milik orang lain yang dilakukan secara sengaja, tanpa hak, atau melawan hukum yang berlaku dan dilakukan dengan cara apa pun. Isi pasal tersebut dapat dikaitkan dengan kasus *phising* melalui file apk. Unsur "setiap orang" dalam hal ini adalah *phiser* yang dengan sengaja dan tanpa haknya mengakses system elektronik korban dengan mengirimkan file apk yang jika diklik maka akan segera dapat terakses system jaringan telepon genggam korban, bahkan aplikasi m-banking milik korban. Penjatuhan hukuman dari Pasal 30 Ayat (1) ada pada ketentuan Pasal 46 yaitu dengan penjatuhan pidana penjara paling lama 6 (enam) tahun dan/atau denda paling banyak Rp600.000.000,00 (enam ratus juta rupiah).

- Pasal 32 Ayat (1) UU ITE

Pasal 32 Ayat (1) UU ITE mengatur jika setiap orang tidak diperbolehkan melakukan perubahan, penambahan, pengurangan, melakukan pemindahan, perusakan, penghilangan, pemindahan, penyembunyian suatu informasi atau dokumen berbasis elektronik baik itu milik orang lain maupun milik publik. Ketentuan pada pasal tersebut dapat dikaitkan dengan kasus *phising* melalui file apk. Unsur "setiap orang" dalam hal ini adalah *phiser* yang dengan sengaja dan tanpa haknya merusak system keamanan perangkat telepon milik korban dan melakukan transmisi berupa uang di rekening m-banking korban ke rekening miliknya. Penjatuhan hukuman dari Pasal 32 Ayat (1) ada pada ketentuan Pasal 48 yaitu dengan penjatuhan pidana penjara paling lama 8 (delapan) tahun dan/atau denda paling banyak Rp2.000.000.000,00 (dua miliar rupiah).

- Pasal 35 UU ITE

Pasal 35 UU ITE juga mengatur jika tidak diperbolehkannya melakukan

manipulasi, penciptaan suatu informasi elektronik atau dokumen elektronik dengan tujuan agar informasi atau dokumen elektronik tersebut dianggap sebagai data asli atau otentik. Bunyi pasal tersebut dapat dikaitkan dengan kasus *phising* melalui file apk. Unsur "setiap orang" dalam hal ini adalah *phiser* yang dengan sengaja dan tanpa haknya memanipulasi file berformat apk dengan memberikan nama untuk file tersebut seakan-akan dokumen penting (foto paket yang akan dikirimkan, undangan pernikahan, atau surat tilang elektronik). Penjatuhan hukuman dari Pasal 35 ada pada ketentuan Pasal 51 yaitu dengan penjatuhan hukuman pidana penjara yang akan dilakukan paling lama 12 (dua belas) tahun dan/atau dikenakan denda paling banyak Rp12.000.000.000,00 (dua belas miliar rupiah).

Berdasarkan pasal-pasal Undang-Undang Nomor 19 Tahun 2016 Tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik dan Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik (yang selanjutnya disingkat dengan UU ITE) yang sekiranya relevan untuk kasus *phising* melalui pengiriman file apk, pasal-pasal tersebut memberikan hukuman dalam bentuk hukuman pidana pokok dalam bentuk baik itu pidana penjara maupun pidana denda seperti apa yang tercantum dalam KUHP.<sup>21</sup> Namun kenyataannya, pasal-pasal tersebut masih belum cukup memenuhi unsur-unsur yang ada pada kasus *phising*. Contohnya seperti yang dapat dilihat dari isi Pasal 35 UU ITE. Isi Pasal 35 UU ITE tersebut memiliki unsur-unsur yang paling memenuhi konsep *phising* itu sendiri, tetapi beberapa unsur *phising* tidak terdapat di dalam pasal tersebut sehingga menyebabkan Pasal 34 mengalami kekaburan norma karena tidak memiliki konsep yang jelas terkait *phising* itu sendiri.<sup>22</sup> Kemudian jika pelaku *phising* atau *phiser* dalam aksinya juga mengambil data pribadi milik korban contohnya seperti informasi terkait Kesehatan korban, data-data biometric yang terdapat di dalam device milik korban, dan lainnya disamping *phiser* tersebut mengambil uang yang terdapat di dalam rekening m-banking korban, maka *phiser* tersebut dapat dikenakan hukuman berdasarkan Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi (selanjutnya disingkat menjadi UU PDP). Namun, UU PDP hanya sebatas memberikan pengaturan terkait pencurian data pribadi saja seperti yang tercantum dalam Pasal 67 Ayat (1) UU PDP, dan hal tersebut kurang relevan jika dikenakan untuk kasus *phising* melalui pengiriman file berformatkan apk.

Dengan itu, Indonesia memiliki urgensi untuk menambah atau merubah pasal-pasal yang sudah ada tersebut dengan memasukkan unsur-unsur yang memenuhi konsep *phising* atau membentuk suatu peraturan perundang-kare-undangan yang baru

---

<sup>21</sup> Leticia M Malunsenge, Cornelis Dj Massie, and Ronald E Rorie, "Penegakan Hukum Terhadap Pelaku Dan Korban Tindak Pidana Cyber Crime Berbentuk Phising Di Indonesia," *Lex Crimen* 11, no. 3 (2022), <https://doi.org/->.

<sup>22</sup> Ardi Saputra Gulo, Sahuri Lasmadi, and Kabib Nawawi, "Cyber Crime Dalam Bentuk Phising Berdasarkan Undang-Undang Informasi Dan Transaksi Elektronik," *PAMPAS: Journal Of Criminal* 1 (n.d.): 2020.

yang secara khusus membahas terkait *phising* na kasus-kasus *phising* di Indonesia masih banyak terjadi. Selain itu, diperlukan juga sosialisasi yang dilakukan secara berkala dan merata terhadap seluruh Masyarakat di Indonesia terkait ancaman siber yang salah satunya adalah *phising* melalui pengiriman file apk dan upaya penanggulangan jika telah terlanjur mengklik file tersebut.

## **B. Urgensi Perlindungan Hukum bagi Korban *Phising* di Indonesia**

Pada dasarnya dengan adanya perkembangan teknologi yang begitu pesat akan menimbulkan pengaruh yang begitu besar terhadap aktivitas sehari-hari manusia. Tujuan utama adanya suatu kemajuan pada bidang teknologi dan industri adalah dapat dimanfaatkan oleh manusia, tetapi pada faktanya, terdapat dampak-dampak negative yang terjadi dengan adanya kemajuan teknologi. Dampak negatif yang ditimbulkan oleh adanya kemajuan teknologi tersebut adalah adanya kejahatan yang memanfaatkan kemampuan internet dan teknologi atau yang dikenal dengan kejahatan siber (*cybercrime*). Kejahatan siber hadir akibat adanya penggunaan teknologi yang semakin meningkat, terutama pada bidang dunia maya. Dari beragamnya kejahatan siber di awal tahun ini, bentuk kejahatan siber yang terjadi di Indonesia adalah kejahatan siber berbentuk *phising*. *Phising* adalah tindak kejahatan yang dalam pelaksanaannya menggunakan rekayasa sosial dan seseorang yang menjadi pelaku kejahatan *phising* disebut dengan *phiser*. *Phising* juga merupakan salah satu bentuk upaya dari oknum yang tidak bertanggung jawab untuk dapat mengakses dan mendapatkan berbagai informasi pribadi yang terdapat di dalam device milik korban seperti system keamanan berupa *password*, nomor-nomor penting seperti yang ada di dalam kartu kredit milik korban, dan lain sebagainya dengan berkedokan sebagai pihak asli dari entitas tertentu yang terpercaya.<sup>23</sup> Ketika melakukan kejahatan *phising* ini, pelaku mengirimkan pesan melalui aplikasi yang berisikan pesan atau situs web palsu yang terlihat seperti dikirim oleh pihak asli yang terpercaya untuk menipu korban yang tidak menaruh rasa curiga dan kehati-hatian ketika melihat pesan tersebut. Pelaku akan mendapatkan akses jika korban telah berhasil terjebak pada pesan yang mereka kirimkan. Terdapat beberapa faktor pemicu adanya kejahatan siber, yaitu sebagai berikut:<sup>24</sup>

### **1. Kemajuan teknologi**

Pelaku kejahatan siber mendapatkan begitu banyak kesempatan dalam melakukan aksi kejahatannya dikarenakan adanya kemajuan teknologi, dengan memanfaatkan eksistensi dari perangkat-perangkat yang terhubung ke internet, serta

---

<sup>23</sup> Sasty Hendri Wibowo et al., *Cyber Crime Di Era Digital*, ed. Diana Purnama Sari, 1st ed. (Padang: PT Global Eksekutif Teknologi Anggota IKAPI, 2022).

<sup>24</sup> Naufal Mahira Dewantoro and Dian Alan Setiawan S.H., M.H., "Penegakan Hukum Kejahatan Siber Berbasis Phising Dalam Bentuk Application Package Kit (APK) Berdasarkan Undang-Undang Informasi Dan Transaksi Elektronik," *Bandung Conference Series: Law Studies* 3, no. 2 (July 31, 2023): 892–900, <https://doi.org/10.29313/bcsls.v3i2.7247>.

pelaku memiliki begitu banyak cara untuk mencuri data, merusak sistem, atau lainnya dengan adanya pemanfaatan teknologi informasi yang begitu banyak.

## **2. Keuntungan finansial**

Terdapat dorongan finansial yang begitu besar bagi pelaku kejahatan siber dalam melakukan aksinya. Kegiatan seperti *phising* akan membuahkan suatu keuntungan finansial dengan jumlah yang besar bagi pelaku.

## **3. Anonimitas**

Terdapat satu alasan mengapa pelaku melakukan kejahatan siber yaitu dikarenakan adanya kemampuan dari pelaku untuk melakukan aksi kejahatannya secara anonim dengan menggunakan jaringan privat virtual atau yang biasa dikenal dengan VPN, atau dengan cara lainnya untuk menyembunyikan jejak mereka.

## **4. Kurangnya keamanan sistem**

Masih kurang memadainya keamanan suatu sistem yang menyebabkan suatu kerentanan pada perangkat lunak atau pembaruan pada sistem sehingga dapat menjadi celah bagi para pelaku untuk melakukan perubahan dalam bentuk "pengrusakkan" pada sistem yang ia serang.

## **5. Faktor dari manusia itu sendiri**

Pelaku kejahatan siber memanfaatkan rendahnya pengetahuan pengguna dalam memanfaatkan teknologi untuk dapat melakukan aksi kejahatan sibernya seperti *phising*.

Adanya kasus *phising* yang dilakukan dengan berbagai cara seperti melalui pengiriman file apk menunjukkan jika Indonesia mengalami suatu kemajuan teknologi yang diikuti dengan kesenjangan sosial. Kemudian minimnya sosialisasi terkait penggunaan internet dan kehati-hatian dalam menggunakannya juga menjadi contoh aspek utama timbulnya kejahatan siber berupa *phising*.<sup>25</sup> Selain dikarenakan kemajuan teknologi, faktor utama penyebab terjadinya *phising* adalah pengguna internet itu sendiri yang tidak memiliki kesadaran dan pengetahuan terkait ancaman *phising* sehingga pada kasus *phising* melalui pengiriman file apk melalui platform *Whatsapp*, korban tidak memiliki kecurigaan ketika membaca pesan dan mengklik file apk yang dikirimkan oleh *phiser*.<sup>26</sup> *Phiser* ketika melakukan aksi kejahatannya dapat menyamar sebagai pihak kurir jasa antar paket yang ingin mengirimkan paket, seseorang yang menyebarkan undangan pernikahan, dan pihak kepolisian yang mengirimkan surat tilang elektronik. Oleh sebab itu, seseorang yang menjadi korban *phising* yang tidak berhati-hati, tanpa sadar segera mengklik file yang dikirimkan oleh *phiser* untuk membaca atau melihat file. Untuk itu diperlukan sosialisasi terkait

<sup>25</sup> Akbar Galih Hariyono and Frans Simangunsong, "Perlindungan Hukum Korban Pencurian Data Pribadi (Phishing Cybercrime) Dalam Perspektif Kriminologi," *Bureaucracy Journal: Indonesia Journal of Law and Social-Political Governance* 3, no. 1 (2023), <https://doi.org/10.53363/bureau.v3i1.191>.

<sup>26</sup> Irvan Hadi Ramadhan and Erna Kumalasari Nurnawati, "Analisis Ancaman Phishing Dalam Layanan E-Commerce," in *Prosiding Seminar Nasional Aplikasi Sains & Teknologi (SNAST) 2022* (Yogyakarta: Institut Sains & Teknologi AKPRIND Yogyakarta, 2022), <https://doi.org/10.34151/prosidingsnast.v8i1.4169>.

ancaman-ancaman kejahatan siber kepada Masyarakat secara berkala dan merata kepada seluruh Masyarakat di Indonesia.

Terdapat salah satu teori kriminologi yang dapat dikaitkan dengan adanya kasus *phising*, yaitu teori kontrol sosial. Salah satu jenis teori kriminologi tersebut merupakan suatu teori yang berfokus terhadap pengendalian perilaku manusia dan teori ini mengangkat suatu permasalahan kepada suatu pembahasan aksi kejahatan yang dihubungkan kepada setiap variable yang mengandung sifat sosiologis seperti struktur suatu pendidikan, suatu kelompok, dan keluarga yang dominan.<sup>27</sup> Dalam teori kontrol sosial ini, terdapat beberapa elemen yang dapat dikaitkan dengan faktor terjadinya kejahatan siber, seperti adanya keterikatan (*commitment*), keterlibatan (*attachment*), keyakinan (*belief*), dan keterampilan (*involvement*), dengan penjelasan sebagai berikut:<sup>28</sup>

1. Keterikatan (*commitment*)

Seseorang yang memiliki keterikatan pada sub sistem yang umum seperti yang terdapat di dalam organisasi, pekerjaan, sekolah, dan lainnya yang memiliki output dalam bentuk manfaat bagi banyak orang, seperti berupa benda, harta, reputasi, masa depan, dan lain sebagainya. Dengan adanya hasil dari keterikatan tersebut, seseorang akan terdorong untuk taat pada aturan yang berlaku.

2. Keterlibatan (*attachment*)

Keterlibatan adalah cara dari manusia untuk melibatkan dirinya sendiri terhadap orang lain, atau yang bias akita lihat dalam kegiatan bersosialisasi atau tolong menolong antar manusia. dalam pelaksanaannya, manusia melibatkan pikiran, perasaan, dan kehendak orang lain, sehingga dirinya menjadi lebih peka. Hubungan antara penyimpangan dengan "keterlibatan" yaitu sejauh apa seseorang tersebut dapat peka terhadap pikiran, perasaan, dan kehendak orang lain.

3. Keyakinan (*belief*)

Keyakinan dalam hal ini merupakan keyakinan atau seseorang terhadap nilai-nilai moral yang berlaku di lingkungannya yang akan menimbulkan ketaatan terhadap suatu norma.

4. Keterampilan (*involvement*)

Jika seseorang aktif pada kegiatan-kegiatan positif di dalam suatu organisasi maka kecil kemungkinannya seseorang tersebut untuk melakukan penyimpangan atau deviasi.

Dari keempat elemen yang terdapat pada teori kontrol sosial tersebut, jika keempatnya tidak terpenuhi pada diri seseorang, maka dapat menjadi faktor seseorang melakukan tindak kejahatan siber seperti dalam bentuk *phising* karena seseorang tersebut tidak memiliki kepekaan terhadap pikiran, perasaan, dan kehendak orang lain, tidak memiliki keyakinan terhadap nilai moral sehingga dirinya tidak memiliki kepatuhan terhadap norma

---

<sup>27</sup> A.S. Alam and Amir Ilyas, *Kriminologi Suatu Pengantar*, 1st ed. (Jakarta: Kencana, 2018).

<sup>28</sup> Alfiyan Umbara and Dian Alan Setiawan, "Analisis Kriminologis Terhadap Peningkatan Kejahatan Siber Di Masa Pandemi Covid-19," *Jurnal Riset Ilmu Hukum*, December 20, 2022, 81–88, <https://doi.org/10.29313/jrih.v2i2.1324>.

yang berlaku, dan orang tersebut tidak memiliki kegiatan positif yang membuat dirinya berpikir untuk mendapatkan keuntungan dari melakukan suatu kejahatan yang merugikan banyak orang.

Berdasarkan uraian terkait faktor atau aspek penyebab terjadinya kejahatan *phising* di Indonesia, maka hal tersebut menandakan jika Indonesia perlu memberikan perlindungan hukum yang tegas untuk para korban dari kasus *phising* melalui pengiriman file apk. Philipus M. Hadjon berpendapat jika perlindungan hukum diperuntukkan untuk rakyat sebagai bentuk aksi nyata dari pemerintah yang dapat menjadi upaya preventif dan represif.<sup>29</sup> Dengan adanya perlindungan hukum yang bersifat preventif bertujuan untuk dapat menghindari timbulnya suatu peristiwa yang tidak diinginkan, seperti adanya serangan siber yang dapat dilakukan melalui berbagai cara. Lalu untuk upaya represif merupakan langkah tegas pemerintah untuk menyelesaikan dan memberikan perlindungan hukum kepada masyarakat yang menjadi korban pada kasus *phising* dengan kepastian hukum. Contoh upaya preventif dari pemerintah Indonesia terhadap ancaman-ancaman siber seperti kasus *phising* melalui pengiriman file apk adalah pembentukan peraturan perundang-undangan yang berkaitan dengan teknologi.

Saat ini Indonesia memang telah mengesahkan Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik dan Undang-Undang Nomor 19 Tahun 2016 tentang Perubahan atas Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik, yang keduanya dikenal dengan UU ITE yang berperan sebagai payung hukum yang mengatur terkait ketentuan-ketentuan pemanfaatan teknologi di Indonesia. Kemudian jika *phising* melalui pengiriman file apk tersebut juga mencuri informasi pribadi korban, maka kasus tersebut juga dapat ditinjau melalui Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi (UU PDP). Pembentukan peraturan perundang-undangan tersebut merupakan upaya perlindungan hukum preventif dari pemerintah Indonesia jika terjadi kasus-kasus *cybercrime* di Indonesia. Untuk upaya represif adalah pelaksanaan dari undang-undang itu sendiri terhadap kasus riil yang melibatkan aspek teknologi, contohnya adalah ketika pihak kepolisian Dittipidsiber saat melakukan penyidikan terhadap kasus *phising* dengan mengenakan pasal 45A Ayat (1) Jo Pasal 28 Ayat (1) UU ITE terhadap *phiser* yang melakukan aksi *phisingnya* tersebut karena menurut pihak kepolisian, tindakan *phiser* masuk ke dalam tindakan penipuan.

Meskipun begitu, menurut penulis, untuk saat ini perlindungan hukum baik preventif maupun represif belum berjalan secara efektif dikarenakan belum terdapat ketentuan-ketentuan yang secara khusus mengatur terkait *phising* itu sendiri. Hal tersebut dikarenakan peraturan perundang-undangan seperti UU ITE dan UU PDP belum dapat mencakup seluruh

---

<sup>29</sup> Philipus. M Hadjon, *Perlindungan Hukum Bagi Rakyat Indonesia* (Surabaya: PT. Bina Ilmu, 1987).

permasalahan yang berkaitan dengan teknologi yang ada karena peraturan perundang-undangan tersebut tidak secara tegas mencakup ketentuan-ketentuan terkait *phising*.<sup>30</sup>

Untuk itu terdapat urgensi pembentukan atau penambahan ketentuan peraturan terkait *phising* pada peraturan perundang-undangan di Indonesia sehingga terdapat kejelasan mengenai apa itu *phising* dan pemutusan hukuman yang tepat untuk para *phiser*. Dengan adanya kasus *phising* melalui pengiriman file apk yang banyak terjadi saat ini, Indonesia membutuhkan peraturan perundang-undangan yang dapat menjadi payung perlindungan hukum untuk kasus kejahatan siber tersebut. Sebagai tambahan pada tanggal 5 Desember 2023, telah disahkan RUU ITE menjadi revisi UU ITE, tetapi pasal-pasal yang berkaitan dengan kasus *phising* yang telah disebutkan sebelumnya, tidak mengalami perubahan di dalam revisi UU ITE tersebut. Oleh karena itu masih diperlukan penambahan ketentuan terkait *phising* pada undang-undang yang telah ada atau pembentukan peraturan perundang-undangan yang baru untuk membahas secara menyeluruh terkait *phising*.

## KESIMPULAN

Undang-Undang ITE (Pasal 30 Ayat (1), Pasal 32, Pasal 35 dan Pasal 28 Ayat (1) UU ITE) masih belum cukup memenuhi unsur-unsur yang ada pada kasus *phising* sehingga belum terdapat kepastian hukum yang kuat pada kasus-kasus *phising* melalui pengiriman file apk yang marak terjadi di Indonesia. Dari penelitian ini juga dapat ditarik kesimpulan jika Indonesia belum memiliki pengaturan hukum yang secara khusus mengatur terkait *phising* yang dalam pelaksanaannya dapat menjadi perlindungan hukum bagi korban *phising* melalui file apk dikarenakan pasal-pasal yang terdapat di dalam UU ITE saat ini belum ada yang memenuhi unsur *phising*, sehingga terdapat suatu urgensi bagi Indonesia untuk menambah ketentuan terkait *phising* di dalam UU ITE, atau menyusun peraturan perundang-undangan sebagai turunan dari UU ITE yang membahas secara khusus terkait *phising*.

## ACKNOWLEDGEMENT

Saya selaku Penulis penelitian ini mengucapkan syukur yang begitu banyak kepada Tuhan YME yang telah membantu Penulis dengan dilimpahkannya begitu banyak karunia dan nikmatnya kepada Penulis sehingga Penulis dapat mengerjakan hingga selesai penelitian ini dengan lancar. Saya juga berterima kasih kepada keluarga Penulis yang terdiri dari kedua orang tua dan satu kakak perempuan yang tiada hentinya memberikan dukungan kepada Penulis. Penulis ingin mengutarakan ucapan terima kasih kepada Dosen Pembimbing Penulis yang telah membantu dan memberikan banyak arahan kepada Penulis dalam penyusunan penelitian ini. Serta, Penulis juga ingin berterima kasih kepada rekan-rekan

---

<sup>30</sup> Rahmat Syah, "Strategi Kepolisian Dalam Pencegahan Kejahatan Phising Melalui Media Sosial Di Ruang Siber," *Jurnal Impresi Indonesia* 2, no. 9 (September 15, 2023): 864–70, <https://doi.org/10.58344/jii.v2i9.3594>.

Penulis yang memberikan bantuan berupa gagasan ide untuk terciptanya penelitian ini. Terakhir, Penulis mengucapkan banyak terima kasih kepada Civitas Akademika Fakultas Hukum, Universitas Pembangunan Nasional "Veteran" Jakarta yang telah memberikan Penulis banyak pengetahuan selama menjadi mahasiswa di Fakultas Hukum, Universitas Pembangunan Nasional "Veteran" Jakarta.

## REFERENSI

- Alam, A.S., and Amir Ilyas. *Kriminologi Suatu Pengantar*. 1st ed. Jakarta: Kencana, 2018. [https://www.google.co.id/books/edition/Kriminologi\\_Suatu\\_Pengantar/K8u2DwAAQBAJ?hl=en&gbpv=1&dq=Kriminologi+Suatu+Pengantar&pg=PA165&printsec=frontcover](https://www.google.co.id/books/edition/Kriminologi_Suatu_Pengantar/K8u2DwAAQBAJ?hl=en&gbpv=1&dq=Kriminologi+Suatu+Pengantar&pg=PA165&printsec=frontcover).
- Ali, Zainuddin. *Metode Penelitian Hukum*. Jakarta: Sinar Grafika, 2009.
- Alkhalil, Zainab, Chaminda Hewage, Liqaa Nawaf, and Imtiaz Khan. "Phishing Attacks: A Recent Comprehensive Study and a New Anatomy." *Frontiers in Computer Science*. Frontiers Media S.A., March 9, 2021. <https://doi.org/10.3389/fcomp.2021.563060>.
- Dewi, Intan Rakhmayanti. "Data Terbaru! Berapa Pengguna Internet Indonesia 2022?" *CNBC Indonesia*, June 9, 2022. <https://www.cnbcindonesia.com/tech/20220609153306-37-345740/data-terbaru-berapa-pengguna-internet-indonesia-2022>.
- Efendi, Jonaedi, and Johnny Ibrahim. *Metode Penelitian Hukum: Normatif Dan Empiris*. Depok: Prenadamedia Group, 2018.
- Galih Hariyono, Akbar, and Frans Simangunsong. "Perlindungan Hukum Korban Pencurian Data Pribadi (Phishing Cybercrime) Dalam Perspektif Kriminologi." *Bureaucracy Journal: Indonesia Journal of Law and Social-Political Governance* 3, no. 1 (2023). <https://doi.org/10.53363/bureau.v3i1.191>.
- Hadjon, Philipus. M. *Perlindungan Hukum Bagi Rakyat Indonesia*. Surabaya: PT. Bina Ilmu, 1987.
- Hery. *Akuntansi Keuangan Menengah*. Edited by Guns. 1st ed. Jakarta: PT Grasindo, 2020.
- Joshi, Yougal, and Anand Singh. "A Study on Cyber Crime and Security Scenario in INDIA." *International Journal of Engineering and Management Research*, no. 3 (2013). [www.ijemr.net](http://www.ijemr.net).
- Krishnugraha, Hilikia Dimas. "Analisis Pembuktian Oleh Penuntut Umum Atas Putusan Tindak Pidana Perbankan Pencatatan Palsu." *Verstek* 7, no. 2 (2021): 418–26. <https://doi.org/10.20956/verstek.v7i2.xxxx>.
- Liningar, R, and R D Vines. *Phishing: Cutting the Identity Theft Line*. Wiley, 2008. <https://books.google.co.id/books?id=dFK-trfdD1AC>.
- Mahira Dewantoro, Naufal, and Dian Alan Setiawan S.H., M.H. "Penegakan Hukum Kejahatan Siber Berbasis Phising Dalam Bentuk Application Package Kit (APK) Berdasarkan Undang-Undang Informasi Dan Transaksi Elektronik." *Bandung Conference Series: Law Studies* 3, no. 2 (July 31, 2023): 892–900. <https://doi.org/10.29313/bcsls.v3i2.7247>.
- Malunsenge, Leticia M, Cornelis Dj Massie, and Ronald E Rorie. "Penegakan Hukum Terhadap Pelaku Dan Korban Tindak Pidana Cyber Crime Berbentuk Phising Di

- Indonesia." *Lex Crimen* 11, no. 3 (2022). <https://doi.org/->.
- Putra Y, Vikran Fasyadhiyaksa. "Modus Operandi Tindak Pidana Phising Menurut UU ITE." *Jurist-Diction* 4, no. 6 (November 5, 2021): 2525. <https://doi.org/10.20473/jd.v4i6.31857>.
- Rakshit, S K. *Ethical Hacker's Penetration Testing Guide: Vulnerability Assessment and Attack Simulation on Web, Mobile, Network Services and Wireless Networks (English Edition)*. New Delhi: BPB Publications, 2022. <https://books.google.co.id/books?id=ZetwEAAAQBAJ>.
- Ramadhan, Irvan Hadi, and Erna Kumalasari Nurnawati. "Analisis Ancaman Phishing Dalam Layanan E-Commerce." In *Prosiding Seminar Nasional Aplikasi Sains & Teknologi (SNAST) 2022*. Yogyakarta: Institut Sains & Teknologi AKPRIND Yogyakarta, 2022. <https://doi.org/10.34151/prosidingsnast.v8i1.4169>.
- Reksten, L E. *Using Technology to Increase Student Learning*. SAGE Publications, 2000. <https://books.google.co.id/books?id=P2QNhie84ikC>.
- Rhamdhatul Muthia dan Ridwan Arifin, Fairuz. "Kajian Hukum Pidana Pada Kasus Kejahatan Mayantara(Cybercrime) Dalam Perkara Pencemaran Nama Baik Di Indonesia" 5, no. 1 (2019). <https://doi.org/10.32661/resam.v5i1.18>.
- Rokhman, Miftakhur, and Habibi-Isnatul Liviani. "Kejahatan Teknologi Informasi (Cyber Crime) Dan Penanggulangannya Dalam Sistem Hukum Indonesia" 23, no. 2 (2020).
- Saputra Gulo, Ardi, Sahuri Lasmadi, and Kabib Nawawi. "Cyber Crime Dalam Bentuk Phising Berdasarkan Undang-Undang Informasi Dan Transaksi Elektronik." *PAMPAS: Journal Of Criminal* 1 (n.d.): 2020.
- Sura Priambada, Bintara, Ashinta Sekar Bidari, and Elisa Putri Oktaviani. "Law Enforcement against Cybercrime in Banking in the Form of Theft of Customer Data." *BIRCI - Journal* 5, no. 2 (2022). <https://doi.org/10.33258/birci.v5i2.5298>.
- Suyanto, S H. *Metode Penelitian Hukum Pengantar Penelitian Normatif, Empiris Dan Gabungan*. Gresik: Unigres Press, 2022.
- Syah, Rahmat. "Strategi Kepolisian Dalam Pencegahan Kejahatan Phising Melalui Media Sosial Di Ruang Siber." *Jurnal Impresi Indonesia* 2, no. 9 (September 15, 2023): 864–70. <https://doi.org/10.58344/jii.v2i9.3594>.
- Umbara, Alfiyan, and Dian Alan Setiawan. "Analisis Kriminologis Terhadap Peningkatan Kejahatan Siber Di Masa Pandemi Covid-19." *Jurnal Riset Ilmu Hukum*, December 20, 2022, 81–88. <https://doi.org/10.29313/jrih.v2i2.1324>.
- Wibawa, Iskandar, Jl Lingkar, Utara Gondangmanis, and Bae Kudus. "Era Digital (Pergeseran Paradigma Dari Hukum Modern Ke Post Modernisme)." *Masalah - Masalah Hukum* 45, no. 4 (2016): 285–91. <https://doi.org/10.14710/mmh.45.4.2016.285-291>.
- Wibowo, Sastya Hendri, Joseph Dedy Irawan, Wahyuddin S, Bambang Winardi, Leo Willyanto Santoso, Safrizal, Yuniansyah, et al. *Cyber Crime Di Era Digital*. Edited by Diana Purnama Sari. 1st ed. Padang: PT Global Eksekutif Teknologi Anggota IKAPI, 2022.
- Zed, Mestika. *Metode Penelitian Kepustakaan*. Jakarta: Yayasan Pustaka Obor Indonesia, 2014.