

## Tinjauan Hukum Terhadap Kejahatan *Online Scamming* sebagai Bentuk Kejahatan Kontemporer

Fatmawaty<sup>1</sup>, Rusman Malik<sup>2</sup>

Program Studi Magister Hukum Pascasarjana Universitas Halu Oleo Kendari<sup>1,2</sup>

\*Email Korespondensi: [watyfatma774@gmail.com](mailto:watyfatma774@gmail.com)

### ABSTRACT

#### Sejarah Artikel:

Diterima 01-07-2026  
Disetujui 07-07-2026  
Diterbitkan 09-07-2026

*The rapid development of information technology and internet-based communication has significantly transformed various aspects of human life, particularly in the fields of commerce, finance, and social interaction. Along with these advancements, cybercrime has emerged as a growing threat, one of which is online scamming. Online scamming refers to fraudulent activities conducted through electronic media or digital platforms with the intention of deceiving victims for financial gain. This form of crime has become increasingly sophisticated through various methods, including phishing, love scams, online shop scams, investment scams, impersonation scams, and social engineering. The borderless nature of cyberspace, the anonymity of offenders, and the complexity of digital evidence present significant challenges for law enforcement agencies. This study aims to analyze online scamming as a contemporary crime, examine the legal framework governing online scamming in Indonesia, and evaluate the effectiveness of law enforcement efforts in addressing such offenses. The research employs a normative legal method using statutory, conceptual, and case approaches. The legal materials consist of primary legal sources, including the 1945 Constitution of the Republic of Indonesia, the Criminal Code (KUHP), and Law Number 1 of 2024 concerning the Second Amendment to the Electronic Information and Transactions Law (ITE Law), supported by secondary and tertiary legal materials. The findings indicate that online scamming fulfills the elements of fraud under the Criminal Code and may also be prosecuted under the ITE Law and other relevant regulations, including the Personal Data Protection Law. However, challenges remain in law enforcement due to technological advancements, transnational criminal networks, difficulties in tracing digital assets, and limited public awareness regarding cybercrime. Therefore, effective prevention and eradication of online scamming require not only penal measures through criminal law enforcement but also non-penal approaches, such as enhancing digital literacy, strengthening cybersecurity systems, and promoting international cooperation in combating cybercrime.*

**Keywords:** Online Scamming, Cybercrime, Fraud, ITE Law, Law Enforcement, Contemporary Crime.

### ABSTRAK

Perkembangan teknologi informasi dan komunikasi berbasis internet telah membawa perubahan yang signifikan dalam berbagai aspek kehidupan masyarakat, khususnya di bidang perdagangan, keuangan, dan interaksi sosial. Namun, kemajuan tersebut juga diikuti dengan meningkatnya berbagai bentuk kejahatan siber (cybercrime), salah satunya adalah online scamming atau penipuan daring. Online scamming merupakan tindakan penipuan yang dilakukan melalui media elektronik atau platform digital dengan tujuan memperoleh keuntungan secara melawan hukum. Modus yang digunakan semakin beragam dan canggih, seperti phishing, love scam, penipuan toko online, penipuan investasi, penyamaran identitas,

dan rekayasa sosial (social engineering). Karakteristik dunia maya yang tidak mengenal batas wilayah, anonimitas pelaku, serta kompleksitas pembuktian digital menjadi tantangan tersendiri dalam proses penegakan hukum. Penelitian ini bertujuan untuk menganalisis online scamming sebagai kejahatan kontemporer, mengkaji pengaturan hukum yang mengatur tindak pidana tersebut di Indonesia, serta menilai efektivitas upaya penegakan hukum dalam menanggulangi praktik online scamming. Metode penelitian yang digunakan adalah penelitian hukum normatif dengan pendekatan perundang-undangan (statute approach), pendekatan konseptual (conceptual approach), dan pendekatan kasus (case approach). Bahan hukum yang digunakan terdiri atas bahan hukum primer berupa Undang-Undang Dasar Negara Republik Indonesia Tahun 1945, Kitab Undang-Undang Hukum Pidana (KUHP), dan Undang-Undang Nomor 1 Tahun 2024 tentang Perubahan Kedua atas Undang-Undang Informasi dan Transaksi Elektronik (UU ITE), serta didukung oleh bahan hukum sekunder dan tersier. Hasil penelitian menunjukkan bahwa tindakan online scamming memenuhi unsur-unsur tindak pidana penipuan sebagaimana diatur dalam KUHP dan dapat pula dijerat dengan ketentuan dalam UU ITE serta peraturan terkait lainnya, termasuk Undang-Undang Perlindungan Data Pribadi. Meskipun demikian, penegakan hukum terhadap pelaku online scamming masih menghadapi berbagai kendala, antara lain perkembangan teknologi yang sangat cepat, jaringan kejahatan lintas negara, kesulitan pelacakan aset digital, serta rendahnya tingkat kesadaran masyarakat terhadap keamanan siber. Oleh karena itu, upaya penanggulangan online scamming tidak hanya memerlukan pendekatan penal melalui penegakan hukum pidana, tetapi juga pendekatan non-penal melalui peningkatan literasi digital, penguatan sistem keamanan siber, serta kerja sama internasional dalam pemberantasan kejahatan siber.

**Kata Kunci:** *Online Scamming*, Kejahatan Siber, Penipuan, UU ITE, Penegakan Hukum, Kejahatan Kontemporer.

**Bagaimana Cara Sitasi Artikel ini:**

Fatmawaty, F., & Malik, R. (2026). Tinjauan Hukum Terhadap Kejahatan Online Scamming sebagai Bentuk Kejahatan Kontemporer. *Jejak Digital: Jurnal Ilmiah Multidisiplin*, 2(4), 7577-7597. <https://doi.org/10.63822/74mm9245>

## PENDAHULUAN

Perkembangan teknologi informasi dan komunikasi telah membawa perubahan signifikan dalam berbagai aspek kehidupan masyarakat. Internet yang pada awalnya berfungsi sebagai sarana pertukaran informasi kini berkembang menjadi media utama dalam aktivitas ekonomi, sosial, pendidikan, hingga pemerintahan. Transformasi digital tersebut telah menciptakan berbagai kemudahan dalam kehidupan sehari-hari, termasuk dalam pelaksanaan transaksi elektronik yang semakin cepat, efisien, dan tidak dibatasi oleh ruang maupun waktu. Kehadiran teknologi digital juga telah mendorong lahirnya berbagai platform perdagangan elektronik (e-commerce), layanan perbankan digital, serta media sosial yang menjadi bagian penting dalam aktivitas masyarakat modern.

Peningkatan penggunaan internet di Indonesia menunjukkan bahwa masyarakat semakin bergantung pada teknologi digital dalam menjalankan aktivitasnya. Berbagai transaksi keuangan kini dilakukan secara daring melalui mobile banking, internet banking, dompet digital, dan platform marketplace. Selain itu, media sosial seperti Facebook, Instagram, WhatsApp, Telegram, dan TikTok telah menjadi sarana komunikasi yang dominan dalam kehidupan masyarakat. Kondisi ini menciptakan peluang yang besar bagi pertumbuhan ekonomi digital, namun di sisi lain juga membuka ruang bagi munculnya berbagai bentuk kejahatan yang memanfaatkan teknologi informasi sebagai sarana maupun objek kejahatan.

Seiring dengan perkembangan teknologi digital tersebut, muncul berbagai bentuk kejahatan siber (cybercrime) yang semakin kompleks dan sulit dikendalikan. Cybercrime merupakan tindak pidana yang memanfaatkan sistem komputer, jaringan internet, maupun teknologi informasi lainnya sebagai alat, sasaran, atau tempat terjadinya kejahatan. Bentuk-bentuk cybercrime yang berkembang saat ini antara lain peretasan (hacking), pencurian data pribadi, penyebaran malware, penipuan daring, perjudian online, pencucian uang melalui media elektronik, hingga berbagai bentuk manipulasi informasi digital. Karakteristik cybercrime yang bersifat lintas batas negara (borderless), anonim, dan mudah dilakukan menjadikan kejahatan ini sebagai salah satu tantangan terbesar dalam penegakan hukum modern.

Salah satu bentuk cybercrime yang mengalami peningkatan signifikan dalam beberapa tahun terakhir adalah online scamming atau penipuan daring. Online scamming merupakan tindakan penipuan yang dilakukan melalui media elektronik dengan tujuan memperoleh keuntungan secara melawan hukum melalui tipu muslihat, penyebaran informasi palsu, manipulasi identitas, maupun rekayasa sosial (social engineering). Modus operandi online scamming terus berkembang mengikuti kemajuan teknologi informasi. Pelaku tidak hanya memanfaatkan media sosial dan aplikasi pesan instan, tetapi juga menggunakan situs web palsu, akun media sosial fiktif, tautan phishing, investasi bodong, hingga penayaman sebagai lembaga resmi untuk memperoleh data pribadi dan aset korban.

Fenomena online scamming menjadi semakin mengkhawatirkan karena jumlah korbannya terus meningkat dan menjangkau seluruh lapisan masyarakat. Korban tidak hanya berasal dari kalangan yang memiliki tingkat literasi digital rendah, tetapi juga individu yang telah terbiasa menggunakan teknologi informasi. Dalam banyak kasus, pelaku memanfaatkan kelemahan psikologis korban melalui teknik manipulasi yang dirancang secara sistematis sehingga korban secara sukarela menyerahkan informasi pribadi, data perbankan, maupun sejumlah uang kepada pelaku. Kondisi tersebut menunjukkan bahwa online scamming tidak lagi merupakan kejahatan konvensional, melainkan telah berkembang menjadi bentuk kejahatan kontemporer yang memiliki tingkat kompleksitas tinggi.

Kerugian yang ditimbulkan oleh online scamming tidak hanya bersifat ekonomi, tetapi juga berdampak pada aspek sosial dan psikologis. Dari sisi ekonomi, korban dapat mengalami kehilangan dana dalam jumlah besar akibat penipuan investasi, transaksi jual beli fiktif, maupun pencurian akses rekening.

Dari sisi sosial, meningkatnya kasus online scamming dapat menurunkan tingkat kepercayaan masyarakat terhadap sistem transaksi elektronik dan layanan digital. Sementara itu, dari sisi psikologis, korban sering mengalami stres, trauma, rasa malu, hingga hilangnya kepercayaan diri akibat menjadi sasaran penipuan. Dampak yang multidimensional tersebut menunjukkan bahwa online scamming telah menjadi ancaman serius terhadap keamanan dan ketertiban masyarakat di era digital.

Dalam perspektif hukum, online scamming menimbulkan berbagai persoalan yang memerlukan perhatian khusus. Pengaturan mengenai tindak pidana penipuan pada dasarnya telah diatur dalam Kitab Undang-Undang Hukum Pidana (KUHP), namun perkembangan teknologi informasi memunculkan berbagai modus kejahatan baru yang membutuhkan instrumen hukum yang lebih spesifik. Oleh karena itu, pemerintah telah membentuk berbagai regulasi, termasuk Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik sebagaimana telah beberapa kali diubah terakhir dengan Undang-Undang Nomor 1 Tahun 2024. Meskipun demikian, efektivitas penegakan hukum terhadap pelaku online scamming masih menghadapi berbagai kendala, antara lain keterbatasan pembuktian digital, penggunaan identitas palsu, serta keterlibatan jaringan pelaku lintas negara.

Berdasarkan uraian tersebut, dapat dipahami bahwa online scamming merupakan salah satu bentuk kejahatan kontemporer yang berkembang seiring dengan kemajuan teknologi informasi dan komunikasi. Kejahatan ini tidak hanya menimbulkan kerugian ekonomi yang signifikan, tetapi juga berdampak pada keamanan digital masyarakat serta efektivitas sistem hukum dalam memberikan perlindungan kepada korban. Oleh karena itu, kajian hukum mengenai online scamming menjadi penting untuk menganalisis karakteristik kejahatan tersebut, mengkaji kecukupan regulasi yang berlaku, serta mengevaluasi efektivitas penegakan hukum dalam upaya pencegahan dan pemberantasannya di Indonesia.

## **METODE PENELITIAN**

### **Jenis Penelitian**

Penelitian ini merupakan penelitian hukum normatif (normative legal research), yaitu penelitian yang dilakukan dengan mengkaji norma-norma hukum yang terdapat dalam peraturan perundang-undangan, doktrin hukum, putusan pengadilan, dan berbagai literatur yang berkaitan dengan kejahatan online scamming sebagai bentuk kejahatan kontemporer.

### **Pendekatan Penelitian**

Dalam penelitian ini digunakan beberapa pendekatan, yaitu:

1. Pendekatan Perundang-undangan (Statute Approach) yaitu pendekatan yang dilakukan dengan menelaah berbagai peraturan perundang-undangan yang mengatur mengenai tindak pidana penipuan dan kejahatan siber, khususnya yang berkaitan dengan online scamming.
2. Pendekatan Konseptual (Conceptual Approach) yaitu pendekatan yang dilakukan dengan mengkaji konsep-konsep, teori-teori, dan doktrin hukum yang berkaitan dengan cybercrime, penipuan elektronik, perlindungan hukum, dan penegakan hukum pidana.
3. Pendekatan Kasus (Case Approach) yaitu pendekatan yang dilakukan dengan menganalisis kasus-kasus online scamming yang pernah terjadi dan ditangani oleh aparat penegak hukum guna mengetahui penerapan hukum dalam praktik.

## **Sumber dan Jenis Bahan Hukum**

### **1. Bahan Hukum Primer**

Bahan hukum primer yang digunakan dalam penelitian ini meliputi:

- a. Undang-Undang Dasar Negara Republik Indonesia Tahun 1945.
- b. Kitab Undang-Undang Hukum Pidana (KUHP).
- c. Undang-Undang Nomor 1 Tahun 2024 tentang Perubahan Kedua atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik.
- d. Peraturan perundang-undangan lain yang berkaitan dengan tindak pidana siber dan penipuan elektronik.

### **2. Bahan Hukum Sekunder**

Bahan hukum sekunder yang digunakan dalam penelitian ini meliputi:

- a. Buku-buku hukum pidana;
- b. Buku-buku hukum siber (cyber law);
- c. Jurnal hukum nasional dan internasional;
- d. Hasil penelitian terdahulu;
- e. Artikel ilmiah yang relevan dengan objek penelitian.

### **3. Bahan Hukum Tersier**

Bahan hukum tersier yang digunakan dalam penelitian ini meliputi:

- a. Kamus hukum;
- b. Ensiklopedia hukum;
- c. Kamus Besar Bahasa Indonesia (KBBI);
- d. Sumber referensi lain yang mendukung penelitian.

## **Teknik Pengumpulan Bahan Hukum**

Pengumpulan bahan hukum dilakukan melalui studi kepustakaan (library research), yaitu dengan mengumpulkan, mempelajari, dan mengkaji berbagai bahan hukum primer, sekunder, dan tersier yang relevan dengan permasalahan penelitian.

## **Teknik Analisis Bahan Hukum**

Bahan hukum yang telah dikumpulkan dianalisis menggunakan metode analisis kualitatif dengan pendekatan deskriptif-analitis. Analisis dilakukan dengan cara mengidentifikasi, mengklasifikasikan, menginterpretasikan, dan mengevaluasi berbagai ketentuan hukum yang berkaitan dengan online scamming guna memperoleh kesimpulan yang sistematis mengenai pengaturan hukum dan penegakan hukum terhadap kejahatan tersebut di Indonesia.

## **HASIL DAN PEMBAHASAN**

### **A. Online Scamming sebagai Bentuk Kejahatan Kontemporer**

#### **1. Pengertian Online Scamming**

Perkembangan teknologi informasi dan komunikasi telah melahirkan berbagai bentuk kejahatan baru yang memanfaatkan internet sebagai sarana utama dalam melakukan tindak pidana. Salah satu bentuk kejahatan yang berkembang pesat dalam era digital adalah online scamming atau penipuan daring. Online scamming merupakan tindakan penipuan yang dilakukan melalui media elektronik dengan tujuan

memperoleh keuntungan secara melawan hukum melalui penggunaan informasi palsu, manipulasi identitas, rekayasa sosial (*social engineering*), maupun berbagai modus lainnya yang memanfaatkan kelemahan korban. Berbeda dengan penipuan konvensional yang umumnya dilakukan melalui pertemuan langsung antara pelaku dan korban, online scamming dilakukan melalui jaringan internet sehingga pelaku dan korban tidak perlu berada dalam lokasi yang sama.

Secara terminologis, istilah scam merujuk pada suatu tindakan penipuan yang dilakukan untuk memperoleh keuntungan secara tidak sah melalui tipu daya atau kebohongan. Dalam konteks digital, online scamming dapat dipahami sebagai segala bentuk penipuan yang memanfaatkan teknologi informasi dan internet sebagai media utama dalam menjalankan aksi kejahatannya. Pelaku biasanya menggunakan berbagai platform digital seperti media sosial, surat elektronik (*e-mail*), aplikasi pesan instan, situs web palsu, hingga aplikasi perdagangan elektronik untuk menjangkau calon korban.

Online scamming berkembang seiring meningkatnya penggunaan internet dan transaksi elektronik dalam kehidupan masyarakat. Kemudahan komunikasi digital, tingginya aktivitas transaksi daring, serta meningkatnya ketergantungan masyarakat terhadap teknologi informasi memberikan peluang bagi pelaku untuk melakukan berbagai bentuk penipuan dengan risiko yang relatif kecil. Bahkan dalam banyak kasus, pelaku dapat beroperasi dari wilayah atau negara yang berbeda dengan korban sehingga menyulitkan proses pelacakan dan penegakan hukum.

Dalam praktiknya, online scamming memiliki berbagai bentuk dan modus operandi yang terus berkembang mengikuti kemajuan teknologi. Salah satu bentuk yang paling umum adalah phishing, yaitu tindakan memperoleh data pribadi korban seperti kata sandi, nomor rekening, atau informasi kartu kredit melalui situs web atau pesan elektronik palsu yang menyerupai lembaga resmi. Selain itu terdapat pula online shopping scam, yaitu penipuan yang dilakukan melalui transaksi jual beli daring dengan menawarkan barang yang sebenarnya tidak pernah ada. Modus lain yang juga sering ditemukan adalah investment scam atau investasi bodong yang menjanjikan keuntungan besar dalam waktu singkat untuk menarik minat korban.

Selain itu, berkembang pula fenomena romance scam atau love scam, yaitu penipuan yang memanfaatkan hubungan emosional antara pelaku dan korban melalui media sosial atau aplikasi kencan daring. Dalam modus ini, pelaku membangun hubungan secara intensif dengan korban selama periode tertentu sebelum akhirnya meminta sejumlah uang dengan berbagai alasan yang dibuat-buat. Tidak sedikit korban yang mengalami kerugian hingga ratusan juta rupiah akibat manipulasi psikologis yang dilakukan oleh pelaku.

Karakteristik utama online scamming terletak pada penggunaan teknologi informasi sebagai sarana utama dalam melakukan kejahatan. Pelaku memanfaatkan anonimitas yang disediakan oleh internet untuk menyembunyikan identitasnya sehingga sulit dilacak oleh aparat penegak hukum. Selain itu, online scamming juga bersifat lintas batas negara (*borderless crime*), yang berarti bahwa pelaku, korban, server, dan instrumen kejahatan dapat berada di yurisdiksi yang berbeda. Karakteristik tersebut menjadikan online scamming sebagai salah satu bentuk kejahatan modern yang memiliki tingkat kompleksitas tinggi dibandingkan dengan tindak pidana penipuan konvensional.

Dalam perspektif hukum pidana Indonesia, online scamming pada dasarnya memiliki unsur-unsur yang serupa dengan tindak pidana penipuan sebagaimana diatur dalam Kitab Undang-Undang Hukum Pidana (KUHP). Unsur utama yang terdapat dalam tindak pidana penipuan adalah adanya maksud untuk menguntungkan diri sendiri atau orang lain secara melawan hukum melalui penggunaan nama palsu, tipu muslihat, atau rangkaian kebohongan yang menyebabkan korban menyerahkan suatu barang, memberikan

utang, atau menghapuskan piutang. Namun demikian, perkembangan teknologi informasi mengakibatkan munculnya bentuk-bentuk penipuan baru yang dilakukan melalui media elektronik sehingga membutuhkan pengaturan hukum yang lebih spesifik melalui Undang-Undang Informasi dan Transaksi Elektronik (UU ITE).

Online scamming memiliki hubungan yang sangat erat dengan konsep cybercrime atau kejahatan siber. Secara umum, cybercrime merupakan segala bentuk tindak pidana yang memanfaatkan komputer, sistem elektronik, jaringan internet, maupun teknologi informasi lainnya sebagai alat, sasaran, atau tempat terjadinya kejahatan. *Cybercrime* mencakup berbagai jenis kejahatan seperti peretasan (*hacking*), pencurian data pribadi, penyebaran malware, sabotase sistem elektronik, pencucian uang digital, dan penipuan berbasis internet.

Dalam klasifikasi *cybercrime*, online scamming termasuk ke dalam kategori kejahatan siber yang menggunakan teknologi informasi sebagai sarana utama untuk melakukan penipuan terhadap korban. Dengan kata lain, online scamming merupakan salah satu bentuk spesifik dari cybercrime yang berorientasi pada perolehan keuntungan ekonomi melalui manipulasi informasi dan penyalahgunaan teknologi digital. Oleh karena itu, meskipun seluruh online scamming dapat dikategorikan sebagai *cybercrime*, tidak semua *cybercrime* merupakan online scamming karena cakupan cybercrime jauh lebih luas dan mencakup berbagai bentuk kejahatan lainnya.

Hubungan antara online scamming dan *cybercrime* semakin terlihat dalam perkembangan modus kejahatan yang memanfaatkan teknologi digital secara kompleks. Pelaku tidak hanya menggunakan media sosial atau aplikasi pesan instan, tetapi juga memanfaatkan kecerdasan buatan (*artificial intelligence*), teknik rekayasa sosial, manipulasi data digital, hingga sistem otomatis (*bot*) untuk meningkatkan efektivitas penipuannya. Perkembangan tersebut menunjukkan bahwa online scamming telah mengalami transformasi dari sekadar penipuan konvensional menjadi kejahatan siber modern yang membutuhkan pendekatan hukum, teknologi, dan kebijakan yang lebih komprehensif.

Berdasarkan uraian tersebut, dapat dipahami bahwa online scamming merupakan bentuk penipuan yang dilakukan melalui media elektronik dengan memanfaatkan teknologi informasi untuk memperoleh keuntungan secara melawan hukum. Kejahatan ini memiliki karakteristik khusus berupa penggunaan internet sebagai sarana utama, anonimitas pelaku, jangkauan lintas negara, serta tingginya tingkat adaptasi terhadap perkembangan teknologi. Oleh karena itu, online scamming dapat dikategorikan sebagai salah satu bentuk kejahatan kontemporer yang termasuk dalam ruang lingkup cybercrime dan memerlukan perhatian serius dalam aspek pengaturan maupun penegakan hukum di Indonesia.

## **2. Karakteristik Kejahatan Online Scamming**

Online scamming merupakan salah satu bentuk kejahatan siber yang memiliki karakteristik khusus yang membedakannya dari tindak pidana penipuan konvensional. Perkembangan teknologi informasi dan komunikasi telah menyebabkan perubahan pola kejahatan dari yang sebelumnya dilakukan secara langsung menjadi berbasis digital dengan memanfaatkan internet sebagai sarana utama. Karakteristik tersebut menjadikan online scamming sebagai bentuk kejahatan kontemporer yang memiliki tingkat kompleksitas tinggi dan menimbulkan tantangan tersendiri dalam proses penegakan hukum.

Karakteristik pertama dari online scamming adalah dilakukan melalui media elektronik. Dalam praktiknya, pelaku memanfaatkan berbagai sarana teknologi informasi seperti media sosial, aplikasi pesan instan, surat elektronik (*e-mail*), situs web, platform perdagangan elektronik (*e-commerce*), hingga aplikasi perbankan digital untuk melakukan aksinya. Penggunaan media elektronik memungkinkan pelaku

menjangkau korban dalam jumlah yang besar dalam waktu singkat tanpa harus melakukan kontak fisik secara langsung. Selain itu, perkembangan teknologi digital juga memungkinkan pelaku menggunakan berbagai perangkat lunak dan sistem otomatis untuk memperluas jangkauan kejahatannya.

Karakteristik kedua adalah bersifat lintas wilayah (*borderless crime*). Tidak seperti kejahatan konvensional yang umumnya terbatas pada wilayah tertentu, online scamming dapat dilakukan dari mana saja selama pelaku memiliki akses terhadap jaringan internet. Dalam banyak kasus, pelaku dapat berada di negara yang berbeda dengan korban sehingga menimbulkan persoalan yurisdiksi dalam proses penegakan hukum. Karakteristik lintas batas ini menjadikan online *scamming* sebagai bagian dari kejahatan transnasional yang membutuhkan kerja sama antarnegara dalam proses pencegahan, penyelidikan, dan penindakan.

Karakteristik ketiga adalah penggunaan identitas palsu oleh pelaku. Anonimitas yang ditawarkan oleh internet memungkinkan pelaku menyembunyikan identitas sebenarnya dengan menggunakan akun palsu, nomor telepon virtual, alamat surat elektronik fiktif, maupun dokumen identitas yang dipalsukan. Dalam beberapa kasus, pelaku bahkan menyamar sebagai pejabat pemerintah, petugas bank, perusahaan resmi, atau individu tertentu yang memiliki reputasi baik untuk memperoleh kepercayaan korban. Penggunaan identitas palsu tersebut merupakan salah satu faktor yang menyebabkan tingginya tingkat keberhasilan online scamming.

Karakteristik keempat adalah sulit dilacak dan dibuktikan. Pelaku online scamming sering menggunakan teknologi yang memungkinkan mereka menyamarkan lokasi dan identitas digital, seperti *Virtual Private Network* (VPN), *proxy server*, akun anonim, serta berbagai aplikasi komunikasi yang memiliki fitur enkripsi tinggi. Selain itu, alat bukti yang digunakan dalam perkara online scamming sebagian besar berbentuk data elektronik yang memerlukan proses digital forensik untuk memperoleh dan memverifikasinya. Kondisi ini sering menjadi kendala bagi aparat penegak hukum dalam mengungkap identitas pelaku dan membuktikan keterlibatannya dalam suatu tindak pidana.

Selain karakteristik tersebut, online scamming juga memiliki kemampuan adaptasi yang tinggi terhadap perkembangan teknologi. Pelaku terus mengembangkan metode baru sesuai dengan tren penggunaan teknologi dan perilaku masyarakat digital. Akibatnya, modus penipuan yang digunakan selalu berubah dan semakin sulit dikenali oleh masyarakat. Oleh karena itu, online scamming tidak hanya dipandang sebagai bentuk penipuan biasa, tetapi telah berkembang menjadi kejahatan kontemporer yang memerlukan pendekatan hukum, teknologi, dan edukasi masyarakat secara terpadu.

### **3. Modus Operandi Online Scamming**

Perkembangan teknologi informasi telah menyebabkan munculnya berbagai modus operandi online scamming yang semakin beragam dan kompleks. Pelaku memanfaatkan kemajuan teknologi digital untuk menciptakan berbagai bentuk penipuan yang sulit dideteksi oleh masyarakat. Modus operandi tersebut terus berkembang mengikuti perubahan pola penggunaan internet dan teknologi komunikasi yang digunakan oleh masyarakat.

Salah satu modus online scamming yang paling umum adalah phishing. Phishing merupakan metode penipuan yang dilakukan dengan cara mengelabui korban agar menyerahkan informasi pribadi seperti kata sandi, nomor rekening, kode OTP (*One Time Password*), atau data kartu kredit melalui situs web, surat elektronik, maupun pesan elektronik palsu yang menyerupai lembaga resmi. Dalam modus ini, pelaku biasanya mengatasnamakan bank, perusahaan teknologi, marketplace, atau instansi pemerintah untuk

memperoleh data penting milik korban yang kemudian digunakan untuk mengakses rekening atau akun digital korban.

Modus berikutnya adalah love scam atau romance scam. Dalam modus ini, pelaku membangun hubungan emosional dengan korban melalui media sosial atau aplikasi perkenalan daring. Pelaku biasanya menggunakan identitas palsu dan menciptakan cerita tertentu untuk mendapatkan simpati korban. Setelah memperoleh kepercayaan korban, pelaku mulai meminta sejumlah uang dengan berbagai alasan, seperti kebutuhan darurat, biaya perjalanan, atau pengiriman barang. Tidak sedikit korban yang mengalami kerugian besar akibat manipulasi psikologis yang dilakukan oleh pelaku dalam jangka waktu yang relatif lama.

Selain itu terdapat pula online shop scam, yaitu penipuan yang dilakukan melalui transaksi jual beli secara daring. Pelaku menawarkan barang atau jasa dengan harga yang menarik melalui media sosial, marketplace, atau situs web tertentu. Setelah korban melakukan pembayaran, barang yang dijanjikan tidak pernah dikirim atau tidak sesuai dengan deskripsi yang ditawarkan. Modus ini merupakan salah satu bentuk online scamming yang paling sering terjadi seiring meningkatnya aktivitas perdagangan elektronik di Indonesia.

Modus lainnya adalah investment scam atau penipuan investasi. Dalam praktiknya, pelaku menawarkan investasi dengan janji keuntungan yang sangat tinggi dalam waktu singkat tanpa risiko yang jelas. Untuk meyakinkan korban, pelaku sering menampilkan testimoni palsu, laporan keuntungan fiktif, maupun dokumen yang seolah-olah menunjukkan legalitas usaha tersebut. Seiring perkembangan teknologi digital, investment scam kini banyak dilakukan melalui aplikasi investasi ilegal, perdagangan aset kripto palsu, maupun platform investasi berbasis media sosial.

Selanjutnya terdapat impersonation scam, yaitu modus penipuan yang dilakukan dengan cara menyamar sebagai individu atau lembaga tertentu. Pelaku dapat mengaku sebagai petugas bank, aparat penegak hukum, pegawai perusahaan, maupun kerabat korban untuk memperoleh informasi atau sejumlah uang. Kemajuan teknologi digital memungkinkan pelaku membuat akun media sosial, alamat surat elektronik, bahkan dokumen elektronik yang menyerupai identitas pihak yang ditiru sehingga korban sulit membedakan antara identitas asli dan identitas palsu.

Modus terakhir yang sering digunakan dalam online scamming adalah social engineering. Social engineering merupakan teknik manipulasi psikologis yang bertujuan mempengaruhi korban agar secara sukarela memberikan informasi rahasia atau melakukan tindakan tertentu yang menguntungkan pelaku. Dalam praktiknya, teknik ini sering dikombinasikan dengan phishing, impersonation scam, maupun love scam. Pelaku memanfaatkan rasa takut, panik, kepercayaan, empati, maupun keserakahan korban untuk mencapai tujuan kejahatannya. Oleh karena itu, banyak ahli keamanan siber menilai bahwa faktor manusia (*human factor*) masih menjadi celah terbesar yang dimanfaatkan dalam berbagai bentuk online scamming.

Berdasarkan berbagai modus operandi tersebut, dapat dipahami bahwa online scamming merupakan kejahatan yang terus berkembang dan beradaptasi dengan kemajuan teknologi informasi. Variasi modus yang digunakan menunjukkan bahwa pelaku tidak hanya memanfaatkan kelemahan sistem teknologi, tetapi juga kelemahan psikologis manusia. Oleh karena itu, upaya pencegahan online scamming tidak cukup hanya melalui penguatan regulasi dan penegakan hukum, tetapi juga memerlukan peningkatan literasi digital dan kesadaran masyarakat terhadap berbagai bentuk penipuan yang berkembang di ruang siber.

#### **4. Dampak Online Scamming**

Perkembangan teknologi informasi yang semakin pesat telah memberikan berbagai kemudahan bagi masyarakat dalam melakukan aktivitas ekonomi, komunikasi, maupun transaksi elektronik. Namun, di balik berbagai manfaat tersebut, perkembangan teknologi juga membuka peluang munculnya berbagai bentuk kejahatan siber (*cybercrime*), salah satunya adalah online scamming. Kejahatan ini tidak hanya menimbulkan kerugian ekonomi bagi korban, tetapi juga berdampak luas terhadap kondisi psikologis masyarakat serta kepercayaan publik terhadap sistem digital. Oleh karena itu, online scamming merupakan salah satu bentuk kejahatan kontemporer yang memiliki dampak multidimensional dan memerlukan perhatian serius dari berbagai pihak.

a. Kerugian Finansial

Dampak paling nyata dari online scamming adalah kerugian finansial yang dialami oleh korban. Pelaku online scamming umumnya memanfaatkan berbagai platform digital, seperti media sosial, aplikasi pesan instan, marketplace, maupun layanan perbankan elektronik untuk memperoleh keuntungan secara melawan hukum melalui tipu daya atau manipulasi informasi. Korban sering kali mengalami kehilangan sejumlah uang setelah melakukan transfer dana kepada pelaku yang mengaku sebagai penjual barang, pihak bank, investor, atau pihak lain yang memiliki kredibilitas tertentu.

Kerugian finansial yang ditimbulkan oleh online scamming tidak hanya menimpa individu, tetapi juga dapat merugikan perusahaan maupun lembaga keuangan. Dalam beberapa kasus, korban kehilangan seluruh tabungan atau aset yang dimilikinya akibat tergiur oleh investasi palsu (*investment scam*) yang menjanjikan keuntungan tinggi dalam waktu singkat. Modus semacam ini memanfaatkan rendahnya literasi digital dan kurangnya pemahaman masyarakat mengenai risiko transaksi elektronik.

Selain kerugian langsung berupa kehilangan uang, korban juga sering kali harus mengeluarkan biaya tambahan untuk memulihkan akun digital, melakukan pelaporan hukum, atau menyelesaikan berbagai permasalahan administratif yang timbul akibat penyalahgunaan data pribadi oleh pelaku. Oleh karena itu, dampak ekonomi yang ditimbulkan oleh online scamming dapat berlangsung dalam jangka panjang dan memengaruhi kondisi keuangan korban secara signifikan.

b. Kerugian Psikologis

Selain kerugian materiil, online scamming juga menimbulkan dampak psikologis yang tidak kalah serius. Korban sering mengalami tekanan emosional setelah menyadari bahwa dirinya telah menjadi sasaran penipuan. Perasaan malu, kecewa, marah, takut, dan kehilangan kepercayaan terhadap orang lain merupakan reaksi psikologis yang umum dialami oleh korban online scamming.

Dalam kasus tertentu, terutama pada modus love scam atau romance scam, dampak psikologis yang dirasakan korban dapat lebih berat dibandingkan kerugian finansial. Hal ini karena pelaku tidak hanya memanfaatkan kelemahan ekonomi korban, tetapi juga mengeksploitasi emosi dan kepercayaan yang telah dibangun melalui komunikasi intensif dalam jangka waktu tertentu. Ketika penipuan tersebut terungkap, korban sering mengalami trauma psikologis, depresi, hingga gangguan kecemasan yang berkepanjangan.

Dampak psikologis lainnya adalah munculnya rasa tidak aman dalam menggunakan teknologi digital. Korban menjadi lebih curiga terhadap berbagai bentuk komunikasi daring, transaksi elektronik, maupun interaksi melalui media sosial. Kondisi tersebut dapat memengaruhi kualitas hidup korban serta menghambat pemanfaatan teknologi yang sebenarnya dapat memberikan manfaat bagi kehidupan sehari-hari.

c. Menurunnya Kepercayaan terhadap Sistem Digital

Maraknya kasus online scamming juga berdampak pada menurunnya tingkat kepercayaan masyarakat terhadap sistem digital. Kepercayaan merupakan salah satu faktor utama yang mendukung perkembangan ekonomi digital, perdagangan elektronik (*e-commerce*), dan layanan berbasis internet. Apabila kasus penipuan online terus meningkat, masyarakat akan cenderung merasa ragu dan enggan melakukan transaksi melalui media elektronik.

Menurunnya kepercayaan publik dapat menghambat perkembangan transformasi digital yang sedang digalakkan oleh pemerintah maupun sektor swasta. Masyarakat yang merasa tidak aman dalam melakukan transaksi elektronik akan lebih memilih metode konvensional yang dianggap lebih terpercaya. Kondisi tersebut berpotensi mengurangi pertumbuhan ekonomi digital serta menghambat inovasi teknologi yang membutuhkan partisipasi aktif masyarakat.

Selain itu, meningkatnya kasus online scamming juga dapat menurunkan reputasi platform digital, lembaga perbankan, dan penyedia layanan teknologi informasi. Meskipun tidak seluruh kasus penipuan terjadi akibat kesalahan sistem, masyarakat sering kali menganggap bahwa penyedia layanan memiliki tanggung jawab terhadap keamanan transaksi yang dilakukan melalui platform mereka. Oleh karena itu, upaya pencegahan dan penanggulangan online scamming menjadi penting untuk menjaga kepercayaan publik terhadap ekosistem digital secara keseluruhan.

Berdasarkan uraian tersebut, dapat dipahami bahwa dampak online scamming tidak hanya terbatas pada kerugian finansial, tetapi juga mencakup aspek psikologis dan sosial yang lebih luas. Oleh karena itu, diperlukan pengaturan hukum yang efektif, peningkatan literasi digital masyarakat, serta penguatan sistem keamanan siber guna meminimalkan terjadinya tindak pidana online scamming dan melindungi masyarakat dari berbagai risiko yang ditimbulkannya.

## **B. Pengaturan Hukum terhadap Kejahatan Online Scamming di Indonesia**

### **1. Pengaturan dalam Kitab Undang-Undang Hukum Pidana (KUHP)**

Kejahatan online scamming pada dasarnya merupakan bentuk penipuan yang dilakukan dengan memanfaatkan teknologi informasi dan media elektronik sebagai sarana untuk memperoleh keuntungan secara melawan hukum. Meskipun dilakukan melalui media digital, substansi perbuatan tersebut tetap memenuhi unsur-unsur tindak pidana penipuan sebagaimana diatur dalam Kitab Undang-Undang Hukum Pidana (KUHP). Oleh karena itu, ketentuan mengenai penipuan dalam KUHP masih dapat diterapkan terhadap pelaku online scamming sepanjang unsur-unsur tindak pidana yang diatur dalam undang-undang terpenuhi.

#### **a. Unsur-Unsur Tindak Pidana Penipuan**

Pengaturan mengenai tindak pidana penipuan terdapat dalam Pasal 378 KUHP yang menyatakan bahwa: *“Barang siapa dengan maksud untuk menguntungkan diri sendiri atau orang lain secara melawan hukum, dengan memakai nama palsu atau martabat palsu, dengan tipu muslihat ataupun rangkaian kebohongan, menggerakkan orang lain untuk menyerahkan suatu barang kepadanya, atau supaya memberi utang maupun menghapuskan piutang, diancam karena penipuan dengan pidana penjara paling lama empat tahun.”*

Berdasarkan ketentuan tersebut, terdapat beberapa unsur yang harus dipenuhi agar suatu perbuatan dapat dikualifikasikan sebagai tindak pidana penipuan, yaitu:

- a) Adanya maksud untuk menguntungkan diri sendiri atau orang lain secara melawan hukum;
- b) Menggunakan nama palsu, kedudukan palsu, tipu muslihat, atau rangkaian kebohongan;
- c) Adanya tindakan menggerakkan atau membujuk orang lain;

- d) Korban menyerahkan barang, uang, memberikan utang, atau menghapuskan piutang akibat adanya tipu daya tersebut.

Dalam praktik online scamming, unsur-unsur tersebut umumnya terpenuhi ketika pelaku menggunakan identitas palsu melalui media sosial, marketplace, aplikasi pesan instan, atau platform digital lainnya untuk meyakinkan korban agar menyerahkan sejumlah uang atau data pribadi tertentu. Bentuk-bentuk penipuan seperti online shop scam, investment scam, love scam, maupun impersonation scam pada hakikatnya merupakan manifestasi baru dari tindak pidana penipuan yang telah lama dikenal dalam hukum pidana Indonesia.

Walaupun Pasal 378 KUHP tidak secara khusus mengatur mengenai penipuan berbasis teknologi informasi, norma tersebut tetap relevan digunakan sebagai dasar penjatuhan pidana terhadap pelaku online scamming karena unsur-unsur yang terkandung di dalamnya masih dapat diterapkan terhadap berbagai modus penipuan digital yang berkembang saat ini.

b. Pertanggungjawaban Pidana Pelaku

Dalam hukum pidana, seseorang hanya dapat dipidana apabila dapat dibuktikan adanya perbuatan pidana (*actus reus*) dan kesalahan (*mens rea*). Pertanggungjawaban pidana terhadap pelaku online scamming didasarkan pada kemampuan pelaku untuk mempertanggungjawabkan perbuatannya serta adanya unsur kesengajaan dalam melakukan tindak pidana tersebut.

Pelaku online scamming umumnya melakukan perbuatannya dengan sengaja (*dolus*), yaitu dengan merencanakan dan menggunakan berbagai cara untuk menipu korban demi memperoleh keuntungan ekonomi. Kesengajaan tersebut dapat terlihat dari tindakan pelaku yang secara sadar membuat akun palsu, menyebarkan informasi bohong, memanipulasi identitas, atau mengarahkan korban untuk melakukan transfer dana ke rekening tertentu.

Apabila seluruh unsur tindak pidana penipuan dapat dibuktikan di persidangan, maka pelaku dapat dimintai pertanggungjawaban pidana sesuai dengan ketentuan yang berlaku. Selain pelaku utama, pihak-pihak yang turut membantu, memfasilitasi, atau bekerja sama dalam menjalankan skema penipuan juga dapat dimintai pertanggungjawaban pidana berdasarkan ketentuan mengenai penyertaan (*deelneming*) dalam hukum pidana.

Dengan demikian, KUHP tetap memiliki peran penting dalam penegakan hukum terhadap online scamming, khususnya dalam menjerat pelaku yang melakukan penipuan dengan memanfaatkan teknologi informasi sebagai sarana kejahatan.

## **2. Pengaturan dalam Undang-Undang Informasi dan Transaksi Elektronik (UU ITE)**

Seiring berkembangnya kejahatan berbasis teknologi informasi, pengaturan mengenai online scamming tidak cukup hanya mengandalkan ketentuan penipuan dalam KUHP. Oleh karena itu, negara membentuk regulasi khusus melalui Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik yang kemudian mengalami beberapa perubahan, terakhir melalui Undang-Undang Nomor 1 Tahun 2024 tentang Perubahan Kedua atas Undang-Undang Informasi dan Transaksi Elektronik.

UU ITE berfungsi sebagai instrumen hukum khusus (*lex specialis*) yang mengatur berbagai bentuk penyalahgunaan teknologi informasi, termasuk penyebaran informasi menyesatkan yang merugikan konsumen dalam transaksi elektronik.

a. Pasal 28 Ayat (1) UU ITE

Salah satu ketentuan yang sering digunakan untuk menindak pelaku online scamming adalah Pasal 28 ayat (1) UU ITE yang menyatakan: “*Setiap Orang dengan sengaja dan tanpa*

*hak menyebarkan berita bohong dan menyesatkan yang mengakibatkan kerugian konsumen dalam Transaksi Elektronik.*” Ketentuan tersebut memiliki beberapa unsur penting, yaitu:

- a) Setiap orang;
- b) Dengan sengaja dan tanpa hak;
- c) Menyebarkan berita bohong dan menyesatkan;
- d) Mengakibatkan kerugian konsumen dalam transaksi elektronik.

Dalam konteks online scamming, unsur tersebut dapat ditemukan ketika pelaku menyebarkan informasi palsu mengenai produk, investasi, hadiah, pekerjaan, atau layanan tertentu melalui media elektronik sehingga korban mengalami kerugian finansial. Oleh karena itu, Pasal 28 ayat (1) UU ITE menjadi salah satu dasar hukum yang relevan dalam menjerat pelaku penipuan berbasis digital.

b. Pasal 45A Ayat (1) UU ITE

Sanksi pidana terhadap pelanggaran Pasal 28 ayat (1) UU ITE diatur dalam Pasal 45A ayat (1) yang menyatakan bahwa: *“Setiap Orang yang dengan sengaja dan tanpa hak menyebarkan berita bohong dan menyesatkan yang mengakibatkan kerugian konsumen dalam transaksi elektronik sebagaimana dimaksud dalam Pasal 28 ayat (1) dipidana dengan pidana penjara dan/atau pidana denda sesuai ketentuan peraturan perundang-undangan.”*

Pasal ini memberikan dasar hukum bagi aparat penegak hukum untuk menjatuhkan sanksi pidana kepada pelaku online scamming yang melakukan penipuan melalui media elektronik. Pengaturan tersebut menunjukkan komitmen negara dalam memberikan perlindungan hukum kepada masyarakat sebagai pengguna teknologi informasi dan konsumen dalam transaksi elektronik.

Penggunaan Pasal 45A ayat (1) UU ITE juga memperkuat efektivitas penegakan hukum karena karakteristik online scamming yang dilakukan melalui jaringan internet sering kali sulit dijangkau hanya dengan menggunakan ketentuan penipuan konvensional dalam KUHP.

c. Alat Bukti Elektronik

Salah satu keunggulan UU ITE dalam penanganan perkara online scamming adalah pengakuan terhadap alat bukti elektronik sebagai alat bukti yang sah dalam proses peradilan. Ketentuan tersebut diatur dalam Pasal 5 ayat (1) UU ITE yang menyatakan bahwa Informasi Elektronik dan/atau Dokumen Elektronik beserta hasil cetaknya merupakan alat bukti hukum yang sah. Dalam perkara online scamming, alat bukti elektronik dapat berupa:

- a) Percakapan melalui aplikasi pesan instan;
- b) Surat elektronik (e-mail);
- c) Rekaman transaksi elektronik;
- d) Bukti transfer dana;
- e) Tangkapan layar (screenshot);
- f) Data akun media sosial;
- g) Riwayat komunikasi digital lainnya.

Pengakuan terhadap alat bukti elektronik sangat penting mengingat sebagian besar aktivitas online scamming dilakukan melalui media digital. Tanpa pengaturan tersebut,

proses pembuktian akan mengalami kesulitan karena banyak tindakan pelaku tidak meninggalkan bukti fisik sebagaimana tindak pidana konvensional. Oleh sebab itu, keberadaan UU ITE memberikan landasan hukum yang lebih kuat bagi aparat penegak hukum dalam mengungkap, menyelidiki, dan membuktikan tindak pidana online scamming di Indonesia.

### **3. Pengaturan Hukum Lain yang Relevan**

Selain diatur dalam Kitab Undang-Undang Hukum Pidana (KUHP) dan Undang-Undang Informasi dan Transaksi Elektronik (UU ITE), penanggulangan kejahatan online scamming juga didukung oleh berbagai peraturan perundang-undangan lain yang memiliki keterkaitan dengan perlindungan data pribadi dan sistem pembuktian dalam proses peradilan pidana. Kehadiran regulasi-regulasi tersebut menunjukkan bahwa penanganan online scamming memerlukan pendekatan hukum yang komprehensif karena kejahatan ini tidak hanya menyangkut aspek penipuan, tetapi juga sering melibatkan penyalahgunaan data pribadi dan penggunaan bukti elektronik dalam proses penegakan hukum.

Salah satu regulasi yang memiliki relevansi penting adalah Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi (UU PDP). Dalam praktiknya, pelaku online scamming sering memperoleh data korban melalui berbagai cara, seperti pencurian data, kebocoran data pribadi, phishing, maupun penyalahgunaan informasi yang diperoleh dari media sosial. Data pribadi tersebut kemudian digunakan untuk melakukan manipulasi, pemalsuan identitas, atau membangun kepercayaan korban sehingga memudahkan pelaku menjalankan aksi penipuannya.

UU PDP memberikan landasan hukum bagi perlindungan hak-hak subjek data pribadi dan mengatur kewajiban setiap pihak dalam mengelola data pribadi secara sah dan bertanggung jawab. Melalui undang-undang ini, penyalahgunaan data pribadi yang digunakan sebagai sarana untuk melakukan online scamming dapat dikenakan sanksi administratif maupun pidana sesuai dengan ketentuan yang berlaku. Keberadaan UU PDP menjadi penting karena banyak kasus online scamming berawal dari akses ilegal terhadap data pribadi korban yang kemudian dimanfaatkan untuk kepentingan kejahatan.

Selain UU PDP, pengaturan mengenai pembuktian tindak pidana online scamming juga berkaitan erat dengan ketentuan dalam Kitab Undang-Undang Hukum Acara Pidana (KUHAP). Sebagai hukum acara pidana yang berlaku di Indonesia, KUHAP mengatur mekanisme pembuktian dalam proses peradilan pidana. Meskipun KUHAP pada awalnya belum secara eksplisit mengatur alat bukti elektronik, perkembangan hukum melalui UU ITE telah memperluas jenis alat bukti yang dapat digunakan dalam proses pembuktian.

Dalam perkara online scamming, alat bukti elektronik memiliki peranan yang sangat penting karena sebagian besar aktivitas pelaku dilakukan melalui sarana digital. Bukti-bukti seperti rekaman percakapan elektronik, surat elektronik (*e-mail*), bukti transfer dana, tangkapan layar (*screenshot*), rekaman transaksi digital, dan data log sistem elektronik sering menjadi alat bukti utama untuk membuktikan adanya tindak pidana. Oleh karena itu, pengaturan mengenai pembuktian elektronik dalam sistem hukum Indonesia merupakan aspek yang sangat penting dalam mendukung efektivitas penegakan hukum terhadap pelaku online scamming.

Kombinasi antara KUHAP, UU ITE, dan UU Perlindungan Data Pribadi menunjukkan adanya upaya pembentukan sistem hukum yang saling melengkapi dalam menghadapi perkembangan kejahatan siber. Dengan adanya regulasi tersebut, aparat penegak hukum memiliki dasar hukum yang lebih kuat untuk melakukan penyelidikan, penyidikan, penuntutan, hingga pembuktian terhadap pelaku online scamming.

#### **4. Analisis Kecukupan Regulasi terhadap Online Scamming**

Pengaturan hukum yang berlaku di Indonesia pada dasarnya telah memberikan dasar normatif yang cukup untuk menindak pelaku online scamming. Keberadaan KUHP, UU ITE, UU Perlindungan Data Pribadi, serta berbagai peraturan pendukung lainnya menunjukkan bahwa negara telah berupaya mengantisipasi perkembangan kejahatan berbasis teknologi informasi. Regulasi-regulasi tersebut memungkinkan aparat penegak hukum untuk menjerat pelaku melalui berbagai ketentuan pidana yang relevan sesuai dengan karakteristik perbuatan yang dilakukan.

Salah satu kelebihan regulasi yang ada adalah tersedianya dasar hukum yang relatif lengkap dalam mengatur berbagai aspek kejahatan digital. KUHP dapat digunakan untuk menjerat unsur penipuan, sementara UU ITE memberikan pengaturan yang lebih spesifik terkait penyalahgunaan sistem elektronik dan penyebaran informasi bohong dalam transaksi elektronik. Selain itu, pengakuan terhadap alat bukti elektronik sebagai alat bukti yang sah juga menjadi kemajuan penting dalam sistem hukum Indonesia karena memberikan kemudahan dalam proses pembuktian tindak pidana siber.

Kehadiran UU Perlindungan Data Pribadi juga memperkuat perlindungan hukum terhadap masyarakat dari penyalahgunaan data yang sering menjadi sarana utama dalam praktik online scamming. Dengan adanya pengaturan yang lebih jelas mengenai hak subjek data dan kewajiban pengendali data, diharapkan risiko penyalahgunaan informasi pribadi dapat diminimalkan sehingga potensi terjadinya penipuan digital juga dapat ditekan.

Meskipun demikian, regulasi yang ada masih menghadapi berbagai tantangan dalam implementasinya. Salah satu kelemahan yang sering ditemukan adalah cepatnya perkembangan modus operandi online scamming dibandingkan dengan perkembangan regulasi yang tersedia. Pelaku kejahatan siber terus menciptakan metode baru yang lebih kompleks dan sulit dideteksi, sementara proses pembentukan maupun perubahan peraturan perundang-undangan memerlukan waktu yang relatif panjang.

Selain itu, karakteristik online scamming yang bersifat lintas wilayah (*borderless*) juga menimbulkan kendala dalam penegakan hukum. Tidak jarang pelaku berada di luar yurisdiksi Indonesia atau menggunakan server yang berlokasi di negara lain sehingga menyulitkan proses penyidikan dan penindakan. Dalam kondisi demikian, efektivitas penegakan hukum sangat bergantung pada kerja sama internasional serta kemampuan aparat dalam melakukan investigasi digital yang memadai.

Kendala lain yang masih sering ditemui adalah rendahnya tingkat literasi digital masyarakat serta keterbatasan kemampuan teknis sebagian aparat penegak hukum dalam menangani kasus-kasus kejahatan siber yang kompleks. Akibatnya, meskipun regulasi telah tersedia, proses penegakan hukum belum selalu berjalan secara optimal. Oleh karena itu, selain penyempurnaan regulasi, diperlukan peningkatan kapasitas sumber daya manusia, penguatan infrastruktur digital, serta edukasi masyarakat secara berkelanjutan untuk meningkatkan efektivitas pemberantasan online scamming di Indonesia.

Berdasarkan uraian tersebut, dapat disimpulkan bahwa regulasi yang ada pada prinsipnya telah memberikan dasar hukum yang cukup untuk menangani online scamming. Namun, perkembangan teknologi yang sangat cepat menuntut adanya pembaruan regulasi secara berkelanjutan, peningkatan kerja sama lintas negara, serta penguatan kapasitas aparat penegak hukum agar penanggulangan online scamming dapat dilakukan secara lebih efektif dan adaptif terhadap berbagai modus kejahatan yang terus berkembang.

### **C. Penegakan Hukum terhadap Pelaku Online Scamming**

#### **1. Proses Penyelidikan dan Penyidikan**

Penegakan hukum terhadap pelaku online scamming merupakan bagian penting dalam upaya perlindungan masyarakat dari kejahatan siber yang semakin berkembang. Berbeda dengan tindak pidana konvensional, online scamming dilakukan melalui media elektronik yang memungkinkan pelaku beroperasi tanpa harus bertemu langsung dengan korbannya. Kondisi tersebut menyebabkan proses penyelidikan dan penyidikan memerlukan metode serta teknik khusus yang didukung oleh pemanfaatan teknologi informasi dan kemampuan investigasi digital yang memadai.

Dalam sistem peradilan pidana Indonesia, penyelidikan dan penyidikan terhadap tindak pidana online scamming dilaksanakan oleh Kepolisian Negara Republik Indonesia (Polri) sebagai institusi yang memiliki kewenangan untuk mencari dan menemukan suatu peristiwa yang diduga sebagai tindak pidana serta mengumpulkan alat bukti guna membuat terang tindak pidana yang terjadi dan menemukan tersangkanya. Penanganan kasus online scamming umumnya dilakukan oleh Direktorat Tindak Pidana Siber (*Dittipidsiber*) Badan Reserse Kriminal Polri maupun unit-unit cyber crime pada tingkat kepolisian daerah dan kepolisian resor sesuai dengan kewenangan masing-masing.

Dalam proses penyelidikan, aparat kepolisian melakukan pengumpulan informasi awal terkait dugaan tindak pidana yang dilaporkan oleh korban. Informasi tersebut dapat berupa data akun media sosial, nomor telepon, alamat surat elektronik (*e-mail*), rekening bank yang digunakan pelaku, bukti percakapan elektronik, maupun bukti transfer dana. Data-data tersebut kemudian dianalisis untuk mengidentifikasi pola kejahatan dan mengarahkan penyidik kepada identitas pelaku.

Apabila ditemukan bukti permulaan yang cukup, proses dilanjutkan ke tahap penyidikan. Pada tahap ini, penyidik berwenang melakukan berbagai tindakan hukum seperti pemanggilan saksi, pemeriksaan ahli, penyitaan perangkat elektronik, pemblokiran rekening, serta koordinasi dengan penyedia layanan digital dan lembaga keuangan yang terkait dengan tindak pidana yang sedang ditangani.

Salah satu aspek penting dalam penyidikan online scamming adalah penggunaan digital forensic investigation atau investigasi forensik digital. Forensik digital merupakan proses ilmiah yang dilakukan untuk memperoleh, mengidentifikasi, mengamankan, menganalisis, dan menyajikan bukti elektronik yang dapat digunakan dalam proses peradilan. Melalui metode ini, penyidik dapat menelusuri aktivitas pelaku yang tersimpan dalam perangkat elektronik, jaringan internet, media penyimpanan digital, maupun sistem informasi yang digunakan untuk melakukan tindak pidana.

Dalam perkara online scamming, forensik digital dapat digunakan untuk mengungkap identitas pengguna akun palsu, melacak alamat Internet Protocol (*IP Address*), mengidentifikasi pola komunikasi elektronik, memulihkan data yang telah dihapus, serta menemukan hubungan antara berbagai akun atau perangkat yang digunakan oleh pelaku. Bukti-bukti digital yang diperoleh melalui proses forensik kemudian dapat digunakan sebagai alat bukti elektronik yang sah sesuai dengan ketentuan peraturan perundang-undangan.

Keberhasilan proses penyelidikan dan penyidikan sangat bergantung pada kemampuan aparat penegak hukum dalam mengelola bukti digital serta melakukan koordinasi dengan berbagai pihak terkait, termasuk penyedia layanan internet, perbankan, penyelenggara sistem elektronik, dan lembaga internasional apabila tindak pidana melibatkan unsur lintas negara.

## **2. Kendala Penegakan Hukum**

Meskipun telah tersedia berbagai instrumen hukum untuk menindak pelaku online scamming, penegakan hukum terhadap kejahatan ini masih menghadapi berbagai kendala. Karakteristik online scamming yang memanfaatkan teknologi informasi menyebabkan proses identifikasi, pelacakan, dan penindakan terhadap pelaku menjadi lebih kompleks dibandingkan dengan tindak pidana konvensional.

Salah satu kendala utama adalah anonimitas pelaku dalam dunia digital. Pelaku online scamming umumnya menggunakan identitas palsu, akun fiktif, nomor telepon yang tidak terdaftar atas nama sebenarnya, serta berbagai aplikasi yang memungkinkan penyembunyian identitas pengguna. Kondisi tersebut menyulitkan aparat penegak hukum dalam mengidentifikasi pelaku secara cepat dan akurat. Bahkan dalam beberapa kasus, pelaku menggunakan teknologi Virtual Private Network (VPN), proxy server, atau berbagai metode penyamaran digital lainnya untuk menghindari pelacakan.

Kendala berikutnya adalah penggunaan server yang berada di luar negeri. Banyak platform digital, media sosial, aplikasi komunikasi, maupun layanan penyimpanan data yang digunakan dalam praktik online scamming beroperasi dengan server yang berlokasi di luar yurisdiksi Indonesia. Akibatnya, proses memperoleh data elektronik yang diperlukan untuk kepentingan penyidikan sering memerlukan mekanisme kerja sama internasional yang membutuhkan waktu cukup lama. Perbedaan sistem hukum antarnegara juga sering menjadi hambatan dalam proses pertukaran informasi dan penegakan hukum lintas batas negara.

Selain itu, aparat penegak hukum juga menghadapi kesulitan dalam pelacakan aset digital hasil kejahatan. Perkembangan teknologi finansial memungkinkan pelaku memindahkan hasil kejahatan dengan cepat melalui berbagai rekening bank, dompet digital (*e-wallet*), aset kripto, maupun platform pembayaran elektronik lainnya. Dana hasil kejahatan sering kali dipindahkan secara berlapis melalui berbagai akun untuk menghilangkan jejak transaksi sehingga menyulitkan proses pelacakan dan pemulihan aset korban.

Kendala lain yang tidak kalah penting adalah rendahnya kesadaran korban untuk melapor kepada aparat penegak hukum. Banyak korban online scamming memilih untuk tidak melaporkan tindak pidana yang dialaminya karena merasa malu, menganggap kerugiannya relatif kecil, atau beranggapan bahwa peluang pengembalian kerugian sangat rendah. Akibatnya, banyak kasus online scamming yang tidak terungkap dan tidak tercatat secara resmi sehingga menyulitkan upaya pemetaan serta penanggulangan kejahatan tersebut secara menyeluruh.

Rendahnya tingkat literasi digital masyarakat juga menjadi faktor yang memperparah kondisi tersebut. Sebagian masyarakat belum memahami pentingnya menjaga keamanan data pribadi maupun mengenali berbagai modus penipuan digital yang berkembang. Akibatnya, korban tidak hanya rentan menjadi sasaran online scamming, tetapi juga sering tidak mengetahui langkah-langkah hukum yang dapat ditempuh setelah mengalami kerugian.

Berdasarkan uraian tersebut, dapat dipahami bahwa penegakan hukum terhadap pelaku online scamming menghadapi tantangan yang cukup kompleks, baik dari aspek teknologi, yurisdiksi, maupun kesadaran masyarakat. Oleh karena itu, diperlukan penguatan kapasitas aparat penegak hukum, peningkatan kerja sama internasional, pengembangan teknologi investigasi digital, serta peningkatan literasi digital masyarakat guna mewujudkan penegakan hukum yang lebih efektif terhadap kejahatan online scamming di Indonesia.

### **3. Analisis Beberapa Kasus Online Scamming**

Perkembangan teknologi informasi telah melahirkan berbagai bentuk online scamming dengan modus yang semakin beragam dan kompleks. Pada praktiknya, pelaku memanfaatkan kemudahan akses internet, media sosial, aplikasi pesan instan, serta layanan transaksi elektronik untuk menjalankan aksinya. Beberapa kasus yang sering terjadi di Indonesia antara lain penipuan toko online, love scam, dan phishing perbankan. Analisis terhadap kasus-kasus tersebut penting untuk memahami pola kejahatan, kelemahan sistem yang dimanfaatkan pelaku, serta efektivitas pengaturan hukum yang berlaku dalam menanggulangi.

Kasus penipuan toko online (*online shop scam*) merupakan salah satu bentuk online scamming yang paling banyak ditemukan di Indonesia. Modus yang digunakan biasanya berupa penawaran barang dengan harga yang jauh lebih murah dibandingkan harga pasar melalui media sosial, marketplace, maupun situs web tertentu. Setelah korban melakukan pembayaran, barang yang dijanjikan tidak pernah dikirim atau pelaku menghilang tanpa dapat dihubungi. Dalam beberapa kasus, pelaku menggunakan identitas palsu dan rekening yang dipinjam dari pihak lain untuk menyulitkan proses pelacakan oleh aparat penegak hukum.

Dari perspektif hukum pidana, perbuatan tersebut memenuhi unsur penipuan sebagaimana diatur dalam Pasal 378 KUHP karena pelaku menggunakan rangkaian kebohongan untuk menggerakkan korban menyerahkan sejumlah uang. Selain itu, apabila transaksi dilakukan melalui sistem elektronik dengan menggunakan informasi yang menyesatkan, pelaku juga dapat dikenakan ketentuan dalam Pasal 28 ayat (1) jo. Pasal 45A ayat (1) UU ITE. Kasus penipuan toko online menunjukkan bahwa rendahnya kehati-hatian konsumen dalam melakukan transaksi elektronik masih menjadi faktor yang sering dimanfaatkan oleh pelaku.

Bentuk online scamming lainnya yang semakin berkembang adalah love scam atau penipuan asmara daring. Dalam modus ini, pelaku membangun hubungan emosional dengan korban melalui media sosial, aplikasi kencan daring, atau platform komunikasi lainnya. Setelah memperoleh kepercayaan korban, pelaku mulai meminta sejumlah uang dengan berbagai alasan, seperti biaya pengiriman hadiah, kebutuhan mendesak, biaya pengobatan, atau investasi bersama. Tidak jarang pelaku mengaku sebagai warga negara asing, anggota militer, atau profesional yang bekerja di luar negeri guna meningkatkan kredibilitasnya di mata korban.

Love scam memiliki karakteristik yang berbeda dibandingkan bentuk penipuan lainnya karena eksploitasi yang dilakukan tidak hanya menasar aspek ekonomi, tetapi juga kondisi emosional korban. Akibatnya, banyak korban mengalami kerugian finansial yang besar sekaligus trauma psikologis yang berkepanjangan. Dari sudut pandang hukum, pelaku tetap dapat dimintai pertanggungjawaban pidana atas dasar penipuan, meskipun pembuktian dalam kasus ini sering kali lebih kompleks karena hubungan antara pelaku dan korban dibangun melalui komunikasi daring dalam jangka waktu yang relatif lama.

Kasus berikutnya adalah phishing perbankan, yaitu bentuk penipuan yang dilakukan dengan tujuan memperoleh data rahasia nasabah seperti nomor rekening, PIN, kata sandi, kode OTP (One Time Password), maupun informasi perbankan lainnya. Pelaku biasanya mengirimkan tautan palsu melalui pesan singkat, surat elektronik (e-mail), aplikasi pesan instan, atau media sosial yang menyerupai situs resmi bank. Ketika korban memasukkan data pribadinya, informasi tersebut akan direkam dan digunakan oleh pelaku untuk mengakses rekening korban secara ilegal.

Phishing perbankan merupakan salah satu bentuk kejahatan siber yang sangat berbahaya karena tidak hanya menimbulkan kerugian finansial bagi korban, tetapi juga mengancam keamanan sistem transaksi elektronik secara keseluruhan. Dalam kasus semacam ini, pelaku dapat dijerat dengan berbagai ketentuan pidana, baik berdasarkan KUHP, UU ITE, maupun regulasi lain yang berkaitan dengan akses ilegal terhadap sistem elektronik dan penyalahgunaan data pribadi.

Ketiga kasus tersebut menunjukkan bahwa online scamming terus mengalami perkembangan seiring dengan kemajuan teknologi informasi. Modus operandi yang digunakan pelaku semakin beragam dan memanfaatkan berbagai celah keamanan maupun kelemahan psikologis korban. Oleh karena itu, diperlukan pendekatan yang tidak hanya berorientasi pada penegakan hukum, tetapi juga pada upaya pencegahan melalui edukasi dan peningkatan keamanan sistem digital.

#### **4. Upaya Penanggulangan Online Scamming**

Penanggulangan online scamming memerlukan strategi yang komprehensif dan berkelanjutan karena karakteristik kejahatan ini sangat dinamis serta berkembang mengikuti kemajuan teknologi informasi. Upaya penanggulangan tidak dapat hanya mengandalkan pendekatan hukum pidana semata, tetapi juga harus didukung oleh langkah-langkah preventif yang melibatkan pemerintah, aparat penegak hukum, sektor swasta, dan masyarakat. Secara umum, penanggulangan online scamming dapat dilakukan melalui pendekatan penal dan non-penal.

Pendekatan penal merupakan upaya penanggulangan yang dilakukan melalui penerapan hukum pidana terhadap pelaku kejahatan. Pendekatan ini diwujudkan melalui proses penyelidikan, penyidikan, penuntutan, dan pemidanaan terhadap pelaku online scamming berdasarkan ketentuan yang terdapat dalam KUHP, UU ITE, UU Perlindungan Data Pribadi, serta berbagai regulasi lainnya yang relevan. Tujuan utama pendekatan penal adalah memberikan efek jera kepada pelaku sekaligus memberikan perlindungan hukum kepada masyarakat dari ancaman kejahatan siber.

Keberhasilan pendekatan penal sangat bergantung pada kemampuan aparat penegak hukum dalam mengungkap identitas pelaku, mengumpulkan alat bukti elektronik, serta melakukan koordinasi dengan berbagai pihak yang terkait. Dalam konteks online scamming yang sering melibatkan jaringan lintas negara, penegakan hukum juga memerlukan dukungan kerja sama internasional agar proses penindakan dapat berjalan secara efektif.

Di samping pendekatan penal, penanggulangan online scamming juga harus dilakukan melalui pendekatan non-penal. Pendekatan ini berfokus pada upaya pencegahan sebelum tindak pidana terjadi, antara lain melalui peningkatan keamanan sistem elektronik, penguatan regulasi perlindungan data pribadi, pengawasan terhadap aktivitas transaksi digital, serta peningkatan kapasitas lembaga yang bertugas menangani kejahatan siber. Pendekatan non-penal dianggap penting karena penegakan hukum semata tidak akan mampu menghilangkan kejahatan apabila faktor-faktor penyebabnya tidak ditangani secara menyeluruh.

Salah satu bentuk pendekatan non-penal yang sangat penting adalah peningkatan literasi digital masyarakat. Rendahnya pemahaman masyarakat mengenai keamanan digital sering kali menjadi faktor utama yang dimanfaatkan oleh pelaku online scamming. Oleh karena itu, edukasi mengenai cara mengenali modus penipuan daring, menjaga kerahasiaan data pribadi, memverifikasi informasi sebelum melakukan transaksi, serta melaporkan tindak pidana siber perlu terus ditingkatkan.

Program literasi digital dapat dilaksanakan oleh pemerintah, lembaga pendidikan, perbankan, perusahaan teknologi, maupun organisasi masyarakat melalui berbagai media dan platform yang mudah diakses oleh publik. Dengan meningkatnya kesadaran masyarakat terhadap risiko kejahatan siber, peluang keberhasilan pelaku online scamming dapat diminimalkan secara signifikan.

Selain itu, mengingat sifat online scamming yang sering melintasi batas negara, diperlukan kerja sama internasional dalam pemberantasan cybercrime. Kerja sama tersebut dapat dilakukan melalui pertukaran informasi, bantuan hukum timbal balik (mutual legal assistance), ekstradisi pelaku, serta kolaborasi dalam investigasi lintas negara. Kerja sama internasional menjadi sangat penting karena banyak pelaku online scamming memanfaatkan perbedaan yurisdiksi hukum antarnegara untuk menghindari proses penegakan hukum.

Dalam era globalisasi dan digitalisasi saat ini, tidak ada negara yang dapat menangani kejahatan siber secara efektif tanpa dukungan komunitas internasional. Oleh karena itu, penguatan kerja sama regional maupun global menjadi salah satu langkah strategis untuk meningkatkan efektivitas pencegahan dan

pemberantasan online scamming. Dengan kombinasi pendekatan penal dan non-penal yang dilakukan secara terpadu, diharapkan upaya penanggulangan online scamming dapat berjalan lebih efektif serta mampu memberikan perlindungan yang optimal bagi masyarakat pengguna teknologi informasi.

## KESIMPULAN

1. Online scamming merupakan bentuk kejahatan kontemporer yang memanfaatkan teknologi informasi dan memiliki karakteristik lintas batas, anonim, serta menimbulkan kerugian ekonomi maupun psikologis.
2. Pengaturan hukum terhadap online scamming telah terdapat dalam KUHP dan UU ITE, namun masih memerlukan penyempurnaan untuk mengimbangi perkembangan modus kejahatan digital.
3. Penegakan hukum menghadapi berbagai hambatan teknis dan yuridis sehingga diperlukan penguatan kapasitas aparat penegak hukum serta kerja sama lintas negara.

## SARAN

1. Pemerintah perlu memperkuat regulasi mengenai penipuan digital dan perlindungan korban.
2. Aparat penegak hukum perlu meningkatkan kemampuan digital forensik.
3. Masyarakat perlu meningkatkan literasi digital guna mencegah menjadi korban online scamming.

## DAFTAR PUSTAKA

- Abdul Wahid dan Mohammad Labib. *Kejahatan Mayantara (Cyber Crime)*. Bandung: Refika Aditama, 2017.
- Adami Chazawi. *Kejahatan terhadap Harta Benda*. Malang: Bayumedia Publishing, 2019.
- Andi Hamzah. *Asas-Asas Hukum Pidana Indonesia*. Jakarta: Rineka Cipta, 2019.
- Andi Hamzah. *Hukum Acara Pidana Indonesia*. Jakarta: Sinar Grafika, 2020.
- Barda Nawawi Arief. *Bunga Rampai Kebijakan Hukum Pidana*. Jakarta: Kencana, 2017.
- Barda Nawawi Arief. *Kapita Selekta Hukum Pidana*. Bandung: Citra Aditya Bakti, 2020.
- Barda Nawawi Arief. *Masalah Penegakan Hukum dan Kebijakan Hukum Pidana dalam Penanggulangan Kejahatan*. Jakarta: Kencana, 2018.
- Debarati Halder dan K. Jaishankar. *Cyber Crime and the Victimization of Women*. New York: IGI Global, 2016.
- Edmon Makarim. *Kompilasi Hukum Telematika*. Jakarta: Rajawali Pers, 2021.
- Edmon Makarim. *Pengantar Hukum Telematika: Suatu Kompilasi Kajian*. Jakarta: Rajawali Pers, 2019.
- Eoghan Casey. *Digital Evidence and Computer Crime*. 3rd Edition. London: Academic Press, 2011.
- Jonathan Clough. *Principles of Cybercrime*. Cambridge: Cambridge University Press, 2015.
- Josua Sitompul. *Cyberspace, Cybercrime, Cyberlaw: Tinjauan Aspek Hukum Pidana*. Jakarta: Tatanusa, 2021.
- Kevin D. Mitnick dan William L. Simon. *The Art of Deception: Controlling the Human Element of Security*. Indianapolis: Wiley Publishing, 2002.
- Maskun. *Cyber Crime: Teori dan Praktik Penanganannya di Indonesia*. Jakarta: Prenadamedia Group, 2020.

- Maskun. *Kejahatan Siber (Cyber Crime): Suatu Pengantar*. Jakarta: Kencana, 2018.
- Moeljatno. *Kitab Undang-Undang Hukum Pidana*. Jakarta: Bumi Aksara, 2021.
- Muladi dan Barda Nawawi Arief. *Teori-Teori dan Kebijakan Pidana*. Bandung: Alumni, 2015.
- Sudarto. *Hukum Pidana I*. Semarang: Yayasan Sudarto, 2018.
- Susan W. Brenner. *Cybercrime and the Law: Challenges, Issues and Outcomes*. Boston: Northeastern University Press, 2012.
- Teguh Prasetyo. *Hukum Pidana*. Jakarta: Rajawali Pers, 2020.
- Widodo. *Aspek Hukum Pidana Kejahatan Siber di Indonesia*. Yogyakarta: Aswaja Pressindo, 2020.
- Widodo. *Hukum Pidana di Bidang Teknologi Informasi (Cybercrime Law)*. Yogyakarta: Aswaja Pressindo, 2019.
- Republik Indonesia. *Undang-Undang Dasar Negara Republik Indonesia Tahun 1945*.
- Republik Indonesia. *Kitab Undang-Undang Hukum Pidana (KUHP)*.
- Republik Indonesia. *Undang-Undang Nomor 1 Tahun 2024 tentang Perubahan Kedua atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik*.
- Republik Indonesia. *Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi*.
- Kepolisian Negara Republik Indonesia. *Peraturan Kepolisian Negara Republik Indonesia Nomor 6 Tahun 2019 tentang Penyidikan Tindak Pidana*.
- Kementerian Komunikasi dan Digital Republik Indonesia. *Indonesia Digital Report*. Jakarta, 2024.
- Kementerian Komunikasi dan Informatika Republik Indonesia. *Modul Literasi Digital Nasional*. Jakarta: Kominfo, 2023.
- United Nations Office on Drugs and Crime (UNODC). *Comprehensive Study on Cybercrime*. New York: United Nations Publication, 2013.