**HUKUM DINAMIKA EKSELENSIA**

https://journalversa.com/s/index.php/hde Volume 07, No. 3, September 2025

# PENYELESAIAN HUKUM DALAM PENYIDIKAN TERHADAP TINDAK PIDANA PENIPUAN ONLINE MELALUI PENDEKATAN DIGITAL FORENSIK

**Fidelis Laurdyan Julianto**[1]
[1]Universitas Pancasila
fidelislaurdyan99@gmail.com

***ABSTRACT**; Digital forensics is an effective tool in investigating Online fraud, which often involves the use of information technology to deceive victims. Online fraud in Indonesia continues to rise, primarily due to the low level of digital literacy among the population. A common modus operandi involves sending invitations or notifications through digital messages, which, when accessed by victims, can be used to hack their personal data. This lack of awareness about digital security makes the public vulnerable to cybercrime. This study focuses on how digital forensics is used to identify Online fraud perpetrators, trace digital transactions, and collect relevant evidence for court proceedings. In Online fraud cases, digital evidence such as email traces, financial transaction records, and data from electronic devices is crucial in uncovering the perpetrators' modus operandi. The study aims to analyze the role of digital forensics throughout the investigation process, from evidence collection and data security to the preparation of forensic reports used in court. The research method employed is normative juridical, examining the laws and regulations related to Online fraud and the mechanisms for proving it in court. Based on the research findings, digital forensics has proven to be a critical element in law enforcement against Online fraud, ensuring that the evidence obtained can lead to the prosecution of perpetrators in accordance with applicable laws.*
***Keywords:** Digital Forensics, Online Fraud, Digital Evidence.*

**ABSTRAK;** Digital forensik merupakan salah satu alat yang efektif dalam penyidikan tindak pidana penipuan *Online*, yang seringkali melibatkan penggunaan teknologi informasi untuk menipu korban. Penipuan *Online* di Indonesia terus meningkat, terutama karena rendahnya literasi digital masyarakat. Modus operandi yang sering digunakan adalah dengan mengirimkan undangan atau surat pemberitahuan melalui pesan digital, yang ketika diakses oleh korban, dapat digunakan untuk meretas data pribadi mereka. Rendahnya kesadaran akan keamanan digital ini menjadikan masyarakat rentan menjadi korban kejahatan siber. Penelitian ini berfokus pada bagaimana digital forensik digunakan untuk mengidentifikasi pelaku

penipuan *Online*, melacak transaksi digital, dan mengumpulkan bukti yang relevan untuk dibawa ke pengadilan. Dalam kasus penipuan *Online*, bukti digital seperti jejak email, rekaman transaksi keuangan, dan data dari perangkat elektronik menjadi kunci untuk mengungkap modus operandi pelaku. Penelitian ini bertujuan untuk menganalisis peran digital forensik dalam seluruh proses penyidikan, mulai dari pengumpulan bukti, pengamanan data, hingga penyusunan laporan forensik yang digunakan di persidangan. Metode yang digunakan dalam penelitian ini adalah yuridis normatif, dengan menelaah peraturan perundang-undangan terkait tindak pidana penipuan *Online* dan mekanisme pembuktiannya di pengadilan. Berdasarkan hasil penelitian, digital forensik terbukti menjadi elemen penting dalam penegakan hukum terhadap kejahatan penipuan *Online*, memastikan bahwa bukti yang diperoleh dapat mengarahkan pada penghukuman pelaku sesuai dengan hukum yang berlaku.
**Kata Kunci:** Digital Forensik, Penipuan *Online*, Bukti Digital.

## PENDAHULUAN

Kemajuan dalam bidang teknologi informasi dan komputer berkembang sangat pesat, khususnya sejak hadirnya teknologi jaringan yang menghubungkan komputer melalui internet. Perkembangan ini telah membuka peluang terciptanya ruang interaksi sosial baru di dunia digital, di mana orang-orang dapat berkomunikasi tanpa terikat oleh batasan geografis maupun waktu.[1] Menurut laporan Data Reportal yang mengutip survei We Are Social tahun 2021, jumlah pengguna internet di Indonesia mencapai sekitar 202,6 juta orang, atau sekitar 73,7% dari total populasi. Jumlah ini meningkat sekitar 27 juta pengguna, atau naik sebesar 15,5% dibandingkan dengan tahun sebelumnya. Salah satu aktivitas dominan di kalangan pengguna internet Indonesia adalah e-commerce, di mana 79,1% melakukan transaksi pembelian produk melalui perangkat seluler, sementara 87,1% memanfaatkan perangkat lain untuk keperluan yang sama.[2]

Seiring dengan pesatnya kemajuan teknologi informasi dan komputer, muncul pula sisi negatifnya, yaitu kejahatan siber. Tindak pidana ini menghadirkan kerumitan tersendiri dalam proses penegakan hukum. Kompleksitas ini meliputi berbagai aspek, mulai dari formulasi aturan hukum yang relevan hingga penentuan wilayah hukum

[1] Nurlely Darwis, Kriminology pada Bidang Kebijakan "Cyber Security", Jurnal Ilmiah Hukum Dirgantara, Fakultas Hukum Unversitas Dirgantara Marsekal Suryadarma, Volume 9, No. 2, Maret 2019, Hlm. 25.
[2] Syaza Dyah Utami, dkk, Analisis Live Forensic pada Whatsapp Web untuk Pembuktian Kasus Penipuan Transaksi Elektronik, Cyber Security dan Forensik Digital, Volume 4, No. 1, Mei 2021, Hlm. 25.

pengadilan yang berwenang menangani kasus tersebut. Di Indonesia, selain Kitab Undang-Undang Hukum Pidana (KUHP), kejahatan siber juga secara khusus diatur dalam Undang-Undang Nomor 19 Tahun 2016 tentang Perubahan atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE). Keberadaan UU ITE ini menjadi penting mengingat karakteristik unik dari kejahatan siber yang seringkali melintasi batas-batas teritorial dan melibatkan bukti digital yang memerlukan penanganan khusus.[3]

Penipuan daring menjadi salah satu jenis kejahatan siber yang sering muncul, terutama karena melibatkan penggunaan informasi, komunikasi, dan transaksi elektronik. Tindakan penipuan ini dijalankan dengan berbagai cara licik dengan tujuan untuk mendapatkan keuntungan pribadi, sebagaimana yang termaktub dalam Pasal 378 Kitab Undang-Undang Hukum Pidana (KUHP). Di era digital seperti sekarang ini, praktik penipuan yang memanfaatkan platform media sosial semakin menimbulkan keresahan di masyarakat. Sebuah survei yang dilakukan oleh Kaspersky Lab dan B2B Internasional menunjukkan bahwa lebih dari seperempat konsumen di Indonesia, tepatnya 26%, pernah menjadi sasaran kejahatan daring. Angka ini menggarisbawahi betapa rentannya masyarakat Indonesia terhadap ancaman penipuan yang terjadi di ranah digital.[4]

Perkembangan teknologi informasi yang pesat telah membawa dampak positif dalam berbagai aspek kehidupan masyarakat, termasuk kemudahan bertransaksi secara Online. Namun, di sisi lain, kemajuan ini dimanfaatkan oleh pihak tidak bertanggung jawab untuk melakukan tindak pidana penipuan Online. Data dari berbagai lembaga penegak hukum dan keamanan siber menunjukkan bahwa angka kasus penipuan Online terus meningkat setiap tahunnya. Penipuan ini sering kali memanfaatkan kurangnya literasi digital masyarakat, di mana para pelaku menggunakan berbagai metode untuk menjebak korban. Salah satu modus yang umum digunakan adalah pengiriman undangan atau notifikasi palsu melalui pesan digital, yang ketika diakses korban, memungkinkan pelaku meretas data pribadi atau mencuri identitas.[5]

---

[3] Prasetiyo dan Mukhtar Zuhdy, Penegakan Hukum oleh Aparat Penyidik Cyber Crime dalam Kejahatan Dunia Maya (Cyber Crime) di Wilayah Hukum Polda DIY, Indonesian Journal of Criminal Law and Criminology (IJCLC), Volume 1, No. 2, Juli 2020, Hlm. 80

[4] Puti Priyana, dkk, Alat Bukti Informasi Elektronik Tindak Pidana Penipuan Online dalam Perspektif Hukum Acara Pidana di Indonesia, Jurnal IUS Kajian Hukum dan Keadilan, Volume 9, Issue 1, April 2021, Hlm. 185.

[5] *Ibid*.

Rendahnya kesadaran masyarakat terhadap keamanan digital menjadi faktor utama yang membuat mereka rentan menjadi korban. Kondisi ini menjadi tantangan bagi aparat penegak hukum dalam mengungkap dan menindak pelaku penipuan Online, mengingat kejahatan ini dilakukan secara virtual dan sering kali melibatkan transaksi digital yang sulit dilacak. Oleh karena itu, diperlukan pendekatan efektif dan terintegrasi dalam penyidikan, salah satunya melalui penerapan digital forensik.

Digital forensik memiliki peran penting dalam penyidikan tindak pidana penipuan Online. Dengan teknik dan alat forensik digital, penyidik dapat mengidentifikasi pelaku, melacak aliran transaksi, serta mengumpulkan bukti-bukti digital yang relevan untuk diajukan di pengadilan. Bukti digital seperti jejak email, rekaman transaksi keuangan, dan data dari perangkat elektronik menjadi kunci dalam mengungkap modus operandi pelaku dan memastikan mereka dapat diadili sesuai hukum.

Namun, penerapan digital forensik menghadapi tantangan, seperti pengamanan data yang rentan rusak atau dihapus, serta kesesuaian bukti digital dengan standar pembuktian di pengadilan. Oleh karena itu, penelitian ini penting dilakukan untuk menganalisis peran digital forensik dalam mendukung penyidikan, mulai dari pengumpulan bukti hingga penyusunan laporan forensik yang dapat digunakan sebagai alat bukti di persidangan.

Mengungkap kasus penipuan daring bukanlah perkara mudah dan dipengaruhi oleh beberapa faktor krusial. Pertama, pelaku kejahatan sering kali memanfaatkan ketidaktahuan korban mengenai prosedur spesifik dalam transaksi digital. Kurangnya literasi digital pada sebagian masyarakat menjadi celah yang dieksploitasi oleh para penipu. Kedua, karakteristik unik dari bukti digital dalam kasus penipuan daring menjadikannya rentan terhadap manipulasi, penghapusan, atau bahkan penghilangan secara permanen. Hal ini tentu menyulitkan upaya aparat penegak hukum dalam melacak jejak kejahatan yang telah terjadi. Ketiga, dalam banyak kasus, barang bukti yang berhasil diamankan justru berasal dari pihak ketiga yang tidak terlibat langsung dalam tindak pidana. Situasi ini seringkali menimbulkan perdebatan sengit mengenai keabsahan dan keakuratan bukti tersebut di mata hukum. Lebih lanjut, sifat lintas negara atau transnasional dari penipuan daring menambah lapisan kesulitan tersendiri. Pelaku dapat menjalankan aksinya dari lokasi yang sangat jauh, bahkan melintasi batas-batas negara, sehingga proses identifikasi, pengejaran, dan penangkapan menjadi jauh lebih rumit dan memerlukan kerja sama internasional.

Dalam konteks ini, penggunaan sains dan teknologi, khususnya melalui penerapan digital forensik, menjadi elemen krusial dalam penanganan kejahatan siber. Digital forensik memungkinkan aparat penegak hukum untuk mengidentifikasi tersangka, melacak aktivitas kejahatan, serta mengumpulkan dan mengamankan barang bukti digital yang dapat digunakan dalam proses persidangan. Berbeda dengan pembuktian dalam kejahatan konvensional, pembuktian di dunia maya memiliki karakteristik yang lebih kompleks karena tidak mengenal batas geografis dan dapat dilakukan dari jarak ribuan kilometer. Pelaku penipuan Online sering kali berada selangkah lebih maju dalam melindungi diri mereka dan menghilangkan barang bukti, sehingga peran digital forensik menjadi sangat vital dalam merekonstruksi kejahatan, memastikan integritas barang bukti, dan memberikan kepastian hukum kepada korban.[6]

Dengan penerapan digital forensik yang tepat, aparat penegak hukum dapat meningkatkan efektivitas penyidikan dan pembuktian tindak pidana penipuan Online, yang selama ini sering kali tidak terselesaikan dengan baik. Hal ini diharapkan dapat memperkuat penegakan hukum terhadap kejahatan siber, memberikan perlindungan yang lebih baik bagi masyarakat, serta meningkatkan kepercayaan publik terhadap upaya pemberantasan penipuan Online di Indonesia.

Kebaruan penelitian yang peneliti tulis dari peneliti-peneliti sebelumnya adalah penelitian ini lebih fokus pada tantangan yang dihadapi dalam pengamanan dan penggunaan bukti digital untuk memastikan keabsahannya sesuai dengan undang-undang yang berlaku dan juga peran Negara dalam keilmuan digital forensic sebagai alat penyelesaian hukum khususnya dalam tahap penyidikan.

Berdasarkan isu hukum yang telah diuraikan di atas, penelitian ini bertujuan sebagai berikut :

1. Mengetahui Apa saja tantangan yang dihadapi dalam pengamanan dan penggunaan bukti digital untuk memastikan keabsahannya sesuai dengan peraturan perundang-undangan dalam kasus penipuan *Online*?
2. Bagaimana peran Negara melalui keilmuan Digital Forensik dalam mendorong penyelesaian permasalahan penipuan *Online*?

[6] Monika Elisabet Lamtiur Butar-Butar, dkk, Pembuktian Tindak Pidana Penipuan Melalui Media Online Dilihat dari Perspektif Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik, Diponegoro Law Review, Volume 5, No. 2, Tahun 2016, Hlm. 3.

Penelitian ini diharapkan dapat memberikan kontribusi dalam pengembangan strategi penegakan hukum terhadap tindak pidana penipuan Online di Indonesia serta meningkatkan efektivitas digital forensik sebagai alat utama dalam penyidikan dan pembuktian di pengadilan. Dengan demikian, aparat penegak hukum dapat lebih optimal menangani kasus penipuan Online dan memberikan perlindungan hukum yang lebih baik bagi masyarakat.

## METODE PENELITIAN

Penelitian ini mengadopsi pendekatan yuridis normatif, yang menitikberatkan pada analisis mendalam terhadap data sekunder. Data sekunder ini mencakup berbagai sumber hukum, yaitu bahan hukum primer, sekunder, dan tersier. Sifat penelitian ini adalah deskriptif-analitis, yang bertujuan untuk menggambarkan secara sistematis dan kemudian menganalisis secara mendalam peran penting digital forensik dalam proses penyidikan tindak pidana penipuan daring, dengan berlandaskan pada kerangka hukum yang berlaku di Indonesia.

Proses pengumpulan data dalam penelitian ini dilakukan melalui studi kepustakaan. Metode ini melibatkan penelusuran dan pengkajian berbagai bahan hukum. Bahan hukum primer yang menjadi fokus utama adalah peraturan perundang-undangan yang berkaitan erat dengan tindak pidana siber. Selain itu, bahan hukum sekunder, seperti buku-buku ilmiah, makalah akademis, pendapat para ahli di bidang hukum dan teknologi, serta hasil-hasil penelitian terdahulu yang relevan dengan topik ini, juga menjadi sumber informasi penting. Sebagai pelengkap, bahan hukum tersier seperti kamus hukum dan ensiklopedia digunakan untuk memberikan klarifikasi terhadap konsep-konsep dan istilah-istilah hukum yang mungkin memerlukan pemahaman lebih mendalam.[7]

Data yang terkumpul dianalisis menggunakan metode deskriptif. Tujuan dari analisis ini adalah untuk memaparkan dan menguraikan secara jelas ketentuan-ketentuan hukum yang berkaitan dengan pemanfaatan digital forensik dalam proses penyidikan kasus penipuan daring. Selain itu, analisis ini juga didukung oleh teori-teori hukum yang relevan. Penerapan teori-teori ini bertujuan untuk mengevaluasi sejauh mana efektivitas digital forensik sebagai salah satu instrumen penting dalam proses pembuktian di hadapan hukum. Dengan demikian, diharapkan dapat diperoleh pemahaman yang

[7] Peter Mahmud Marzuki, *Penelitian Hukum*, (Jakarta: Kencana Prenanda Media Group, 2014), hlm.133

komprehensif mengenai kontribusi digital forensik dalam penegakan hukum terhadap kejahatan penipuan daring.

## HASIL DAN PEMBAHASAN

### 1. Analisis Peraturan dalam Penyidikan terhadap Tindak Pidana Penipuan Online

#### a. Landasan Hukum Penanganan Penipuan Online di Indonesia

Keberadaan regulasi yang mengatur penipuan daring memegang peranan krusial dalam memberikan perlindungan kepada masyarakat yang melakukan transaksi melalui internet. Tindakan penipuan yang terjadi dalam transaksi daring dapat mengakibatkan kerugian finansial bagi konsumen sekaligus memberikan keuntungan ilegal kepada pelaku kejahatan. Penipuan daring dikategorikan sebagai *illegal content*, yang merujuk pada penyalahgunaan teknologi informasi melalui penyisipan data atau informasi yang tidak benar ke dalam ranah internet. Informasi yang disebarkan dalam konteks ini seringkali tidak sesuai dengan etika, melanggar ketentuan hukum yang berlaku, atau mengganggu ketertiban umum..

Praktik penipuan daring memanfaatkan berbagai media internet, seperti ruang obrolan (*chat room*), surat elektronik (*email*), atau situs web, dalam rangka melancarkan transaksi penipuan. Tak jarang, penipuan ini melibatkan institusi keuangan seperti bank atau lembaga lain yang memiliki hubungan tertentu dengan calon korban. Para pelaku kejahatan siber ini memanfaatkan perangkat lunak dan akses internet untuk mengakali korban demi keuntungan pribadi mereka.[8]

Undang-Undang Nomor 19 Tahun 2016 tentang Perubahan atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE) memang tidak secara eksplisit menyebutkan tindak pidana penipuan daring. Kendati demikian, Pasal 28 ayat (1) UU ITE secara tegas melarang penyebaran berita bohong dan informasi yang menyesatkan yang berpotensi menimbulkan kerugian bagi konsumen dalam konteks transaksi elektronik.[9] eskipun istilah "penipuan" tidak digunakan secara langsung, pasal ini memiliki relevansi yang

[8] Masukun dan Wiwik Meilararti. 2017. *Aspek Hukum Penipuan Berbasis Internet*. Bandung: Keni Media. Hlm. 30
[9] Suseno, Sigid. 2012. *Yuridiksi Tindak Pidana Siber*. Bandung: Refika Aditama. Hlm. 18.

signifikan dalam memberikan perlindungan kepada konsumen dari praktik penipuan yang terjadi dalam ranah transaksi daring.

Pasal 28 ayat (1) UU ITE seringkali dikaitkan dengan ayat (2) yang mengatur mengenai penyebaran ujaran kebencian yang berlandaskan pada isu SARA (Suku, Agama, Ras, dan Antargolongan). Kedua ayat ini dianggap memiliki tujuan untuk menjaga ketertiban umum. Namun, analisis akademis terhadap UU ITE belum sepenuhnya memberikan kejelasan mengenai keterkaitan antara kedua ayat tersebut, sehingga penelitian lebih lanjut diperlukan untuk memahami relasinya secara lebih mendalam.[10]

Meskipun demikian, Pasal 28 ayat (1) UU ITE tetap memiliki potensi untuk diterapkan dalam kasus-kasus di mana konsumen individu mengalami kerugian akibat penipuan daring. Pasal ini mendukung interpretasi hukum yang tidak hanya terpaku pada maksud pembuat undang-undang (*legislative intent*) semata, tetapi juga mempertimbangkan prinsip-prinsip fundamental dalam hukum pidana.

Pasal 28 ayat (1) UU ITE memiliki elemen-elemen yang menunjukkan kemiripan dengan tindak pidana penipuan konvensional yang diatur dalam Pasal 378 Kitab Undang-Undang Hukum Pidana (KUHP). Keunggulan yang ditawarkan oleh UU ITE terletak pada pengakuan terhadap validitas bukti elektronik dan perluasan cakupan yurisdiksi. Selain itu, pasal ini juga memiliki keterkaitan yang erat dengan Undang-Undang Nomor 8 Tahun 1999 tentang Perlindungan Konsumen, yang bertujuan untuk meningkatkan kesadaran konsumen akan hak-hak mereka, memberikan kepastian hukum dalam transaksi, serta mempermudah akses terhadap informasi yang relevan.

Dalam konteks Undang-Undang Perlindungan Konsumen, definisi konsumen merujuk pada pengguna akhir barang atau jasa untuk kepentingan pribadi, keluarga, atau makhluk hidup lainnya, dan tidak mencakup konsumen perantara seperti pedagang eceran atau pemasok. Pasal 28 ayat (1) UU ITE termasuk dalam kategori delik materiil, yang berarti bahwa timbulnya kerugian pada konsumen akibat

[10] *Ibid*.

penyebaran berita bohong dan informasi yang menyesatkan merupakan esensi dari pelanggaran pasal ini.[11]

Ancaman pidana bagi pelanggar Pasal 28 ayat (1) UU ITE tercantum dalam Pasal 45A ayat (1) UU ITE, yaitu berupa pidana penjara maksimal enam tahun dan/atau denda maksimal satu miliar rupiah. Perbedaan mendasar antara Pasal 378 KUHP dan Pasal 28 ayat (1) UU ITE adalah tidak adanya unsur "menguntungkan diri sendiri atau orang lain secara melawan hukum" dalam Pasal 28 ayat (1). Meskipun demikian, dalam praktik penegakan hukum, penyidik memiliki kewenangan untuk menerapkan kedua pasal ini secara bersamaan apabila seluruh unsur-unsur dalam masing-masing pasal terpenuhi.

Keberadaan UU ITE, terutama setelah mengalami revisi melalui Undang-Undang Nomor 19 Tahun 2016, memberikan dampak positif bagi perlindungan konsumen dengan meminimalisir potensi kejahatan melalui media elektronik serta menjamin hak-hak konsumen dalam transaksi daring..

**b. Tantangan dalam Pengumpulan dan Pembuktian Bukti Digital**

Dalam proses penyidikan, bukti digital memiliki sifat yang unik dibandingkan dengan bukti konvensional. Bukti ini dapat berupa rekaman transaksi, log komunikasi, atau metadata perangkat elektronik, yang rentan terhadap manipulasi, penghapusan, atau kerusakan. Berdasarkan Pasal 5 ayat (1) UU ITE, informasi elektronik dan/atau dokumen elektronik dapat dijadikan alat bukti hukum yang sah, asalkan memenuhi persyaratan validitas dan integritas data sesuai dengan Pasal 6 UU ITE. Namun, penegak hukum sering kali menghadapi kendala teknis dalam mengumpulkan, menganalisis, dan menyajikan bukti digital agar dapat diterima di pengadilan.

Indonesia telah berupaya menyesuaikan regulasi penanganan cyber crime dengan standar internasional, seperti Konvensi Budapest tentang Kejahatan Siber. Meskipun belum menjadi anggota resmi, beberapa prinsip dari konvensi ini telah diadopsi, termasuk pentingnya kerja sama internasional dalam menangani kejahatan lintas batas. Hal ini mencakup pengaturan tentang ekstradisi, pertukaran informasi,

[11] Sitompul, Josua. 2012. *Cyberspace Cybercrime Cyberlaw Tinjauan Aspek Hukum Pidana*. Jakarta: Tatanusa. Hlm. 61.

dan pemulihan aset. Namun, pengaturan yang lebih spesifik terkait yurisdiksi dan prosedur pelacakan lintas negara masih perlu diperkuat untuk meningkatkan efektivitas penyidikan.

Digital forensik memiliki peran sentral dalam mendukung penyidikan terhadap tindak pidana penipuan online. UU ITE memberikan dasar hukum untuk menggunakan bukti digital, tetapi penerapan forensik digital memerlukan prosedur ketat untuk memastikan validitas bukti di pengadilan. Dalam praktiknya, standar operasi forensik digital, seperti ISO/IEC 27037 (Panduan untuk Identifikasi, Pengumpulan, Akuisisi, dan Pemeliharaan Bukti Digital), perlu diterapkan secara konsisten oleh aparat penegak hukum. Selain itu, koordinasi antar lembaga, termasuk Polri, Badan Siber dan Sandi Negara (BSSN), serta lembaga peradilan, menjadi kunci dalam memastikan integritas proses penyidikan.[12]

## 2. Upaya Penanggulangan Tindak Pidana Penipuan Online melalui Pendekatan Digital Forensik

Menurut pandangan Syahrul N. Nur, penanggulangan kejahatan penipuan daring dapat ditempuh melalui dua strategi utama, yaitu langkah pencegahan (preventif) dan penindakan setelah kejadian (represif).[13] Langkah preventif berfokus pada upaya untuk menghindarkan terjadinya tindak pidana sebelum benar-benar terjadi. Pendekatan ini melibatkan kegiatan sosialisasi atau penyebaran informasi melalui berbagai kanal media massa serta koordinasi yang solid antar berbagai lembaga terkait dalam rangka merumuskan kerangka penegakan hukum yang efektif. Lebih lanjut, media juga dapat dimanfaatkan sebagai sarana edukasi yang bertujuan untuk meningkatkan pemahaman masyarakat mengenai aspek hukum yang berkaitan dengan Informasi dan Transaksi Elektronik (ITE). Dengan peningkatan pemahaman ini, diharapkan masyarakat akan lebih mampu mengenali dan menghindari potensi risiko penipuan daring.

Di sisi lain, langkah represif menitikberatkan pada tindakan yang diambil setelah tindak pidana penipuan daring terjadi. Langkah ini mencakup proses penyelidikan secara menyeluruh terhadap laporan kasus penipuan daring serta penerapan sanksi hukum yang

[12] Noor Rahmad. "KAJIAN HUKUM TERHADAP TINDAK PIDANA PENIPUAN SECARA ONLINE", Jurnal Hukum Ekonomi Syariah Magister Ilmu Hukum Universitas Muhammadiyah Yogyakarta. Vol. 3, No.2, Juli-Desember 2019. Hlm.105.
[13] Waluyo, Bambang. 2017. Viktimologi Perlindungan Korban & Saksi. Jakarta: Sinar Grafika. Hlm. 34.

tegas sesuai dengan pasal-pasal peraturan perundang-undangan yang relevan. Tujuan dari langkah represif ini adalah untuk memberikan efek jera kepada pelaku kejahatan sekaligus menegakkan keadilan di tengah masyarakat.

Sejalan dengan pemikiran tersebut, Kristian Hutasoit berpendapat bahwa penanggulangan tindak pidana penipuan daring memiliki keterkaitan yang erat dengan konsep politik kriminal. Pembentukan Undang-Undang ITE dilatarbelakangi oleh tujuan untuk mendukung terciptanya kesejahteraan sosial dan memberikan perlindungan kepada masyarakat di era digital ini. Dalam konteks kebijakan kriminal, Hutasoit menekankan bahwa upaya penanggulangan kejahatan tidak dapat hanya mengandalkan instrumen hukum pidana (pendekatan penal), melainkan memerlukan pendekatan yang lebih integral dan sistematis.[14]

Mengingat penipuan daring merupakan jenis kejahatan yang berbasis pada teknologi, Kristian Hutasoit juga menggarisbawahi pentingnya pendekatan pencegahan yang berbasis teknologi (*techno prevention*), di samping pendekatan budaya, edukasi, serta kerja sama internasional yangSolid. Upaya penanggulangan melalui kebijakan hukum pidana mencakup kriminalisasi terhadap perbuatan-perbuatan tertentu, sebagaimana yang tertuang dalam Pasal 28 ayat (1) UU ITE. Pasal ini secara spesifik mengatur mengenai perbuatan menyebarkan berita bohong dan informasi yang menyesatkan yang mengakibatkan kerugian bagi konsumen dalam transaksi daring. Pelanggaran terhadap ketentuan Pasal 28 ayat (1) UU ITE akan dikenai sanksi pidana sebagaimana diatur dalam Pasal 45 ayat (2) UU ITE, yaitu pidana penjara paling lama enam tahun dan/atau denda maksimal sebesar satu miliar rupiah.

Pemanfaatan hukum pidana sebagai alat untuk mencegah dan menanggulangi kejahatan siber menjadi sangat relevan mengingat dampak negatif dan kerugian yang ditimbulkan oleh semakin masifnya penggunaan teknologi informasi. Dengan memberlakukan hukum pidana, potensi kerugian yang dialami masyarakat akibat kejahatan siber diharapkan dapat diminimalkan, sekaligus mencegah terjadinya hambatan dalam upaya pembangunan kesejahteraan masyarakat secara keseluruhan.

Selain melalui kebijakan penal, upaya penanggulangan kejahatan daring juga dilakukan melalui kebijakan non-penal. Kebijakan ini lebih menekankan pada tindakan

[14] Hutasoit, Kristian. “Tinjauan Yuridis terhadap Tindak Pidana Penipuan Secara Online dalam Perspektif Hukum Pidana di Indonesia”. Jurnal Fakultas Hukum Universitas Umatera Utara (Januari, 2018). Hlm. 10

pencegahan yang meliputi perbaikan kondisi ekonomi nasional, peningkatan kualitas pendidikan moral baik melalui jalur formal maupun informal, penguatan sistem kesehatan mental masyarakat, serta peningkatan efektivitas kerja sama internasional dalam memberantas kejahatan siber (Barda Nawawi Arief, 2007:46).[15] Langkah-langkah lain yang termasuk dalam kebijakan non-penal meliputi penguatan sistem keamanan teknologi informasi dan komputer, serta peningkatan efektivitas hukum administrasi dan perdata yang berkaitan dengan sistem dan jaringan internet.[16]

Dalam konteks penanggulangan penipuan daring di Indonesia, telah diimplementasikan upaya melalui pembentukan badan pengawas lalu lintas data, yaitu Id-SIRTII/CC (Indonesian Security Incident Response Team on Internet and Infrastructure/Coordination Center). Lembaga ini memiliki tugas utama untuk mengawasi keamanan jaringan telekomunikasi yang berbasis protokol internet, memberikan sosialisasi terkait pentingnya keamanan teknologi informasi kepada masyarakat, serta melakukan pemantauan dini terhadap berbagai potensi ancaman terhadap jaringan telekomunikasi, baik yang berasal dari dalam negeri maupun luar negeri.

Selain Id-SIRTII/CC, Kepolisian Republik Indonesia juga memiliki divisi khusus yang secara spesifik menangani berbagai jenis kejahatan siber. Namun, keberadaan tim *cybercrime* ini saat ini masih terkonsentrasi di kota-kota besar dan belum menjangkau seluruh wilayah Indonesia secara merata. Oleh karena itu, peran aktif serta partisipasi dari seluruh elemen masyarakat menjadi sangat penting dalam menghadapi ancaman kejahatan siber, termasuk di dalamnya adalah penipuan daring. Beberapa tindakan konkret yang dapat dilakukan oleh masyarakat dalam upaya ini meliputi:[17]

a. Meningkatkan kesadaran organisasi terhadap ancaman siber;
b. Menerapkan standar keamanan informasi secara menyeluruh;
c. Melatih sumber daya manusia dalam pengamanan siber secara berkelanjutan;
d. Menggunakan sistem dan layanan yang aman serta melakukan pembaruan berkala;
e. Mengembangkan kemampuan pencegahan, mitigasi, dan audit keamanan.

[15] Barda Nawawi Arief, *Masalah Kebijakan Hukum Pidana dalam Penanggulangan Kejahatan* (Bandung: Citra Aditya Bakti, 2007), hlm. 46.
[16] Widodo. 2011. Aspek Hukum Pidana Kejahatan Mayantara. Yogyakarta: Aswaja Pressindo. Hlm. 191.
[17] Op. Cit. Noor Rahmad. Hlm. 110.

Penting untuk dicatat bahwa dalam konteks penanggulangan kejahatan siber, termasuk penipuan daring, digital forensik memegang peranan yang semakin krusial. Digital forensik merupakan cabang ilmu forensik yang berfokus pada identifikasi, pengumpulan, pelestarian, analisis, dan penyajian bukti digital yang dapat digunakan dalam proses hukum.[18] Dalam kasus penipuan daring, digital forensik dapat membantu dalam melacak jejak pelaku, mengidentifikasi alat dan metode yang digunakan, serta memulihkan bukti-bukti penting yang mungkin telah dihapus atau disembunyikan.[19] Penerapan teknik-teknik digital forensik yang efektif memerlukan pemahaman mendalam mengenai teknologi yang digunakan dalam kejahatan tersebut serta kemampuan untuk menganalisis data digital secara akurat dan sesuai dengan standar hukum yang berlaku.

## KESIMPULAN

Tantangan utama dalam mengamankan dan memanfaatkan bukti digital dalam kasus penipuan daring di Indonesia melibatkan risiko kerusakan atau penghapusan bukti, manipulasi data, serta validitas bukti di mata hukum sesuai peraturan perundang-undangan yang berlaku. Mengatasi kompleksitas ini memerlukan penguatan keilmuan digital forensik oleh negara untuk pengumpulan dan analisis bukti yang akurat, sehingga memperkuat proses penyidikan dan pembuktian kejahatan siber dalam sistem penegakan hukum di Indonesia.

Untuk itu, diperlukan pengembangan kebijakan komprehensif terkait bukti digital yang selaras dengan standar pembuktian di pengadilan Indonesia, peningkatan kapasitas aparat penegak hukum dalam digital forensik melalui pelatihan berkelanjutan dan kerja sama lintas lembaga (baik nasional maupun internasional), serta pembangunan infrastruktur digital forensik yang memadai di seluruh wilayah Indonesia, termasuk pusat data nasional yang aman. Peningkatan literasi digital masyarakat Indonesia dan kerja sama internasional dalam pertukaran informasi serta teknologi juga krusial untuk mendukung upaya penegakan hukum yang efektif. Pengembangan sistem monitoring berbasis kecerdasan buatan untuk deteksi dini aktivitas mencurigakan dapat melengkapi upaya ini dan memberikan peringatan kepada aparat penegak hukum. Implementasi

[18] Carrier, Brian D. 2005. "A Hypothesis-Based Framework for Digital Investigations." *Digital Investigation*, 2(1), 24–35.
[19] Reith, Harald, Julian Carr, and Gregg Gunsch. 2002. "An Examination of Digital Forensic Models." *International Journal of Digital Evidence*, 1(3), 1–12.

rekomendasi ini diharapkan dapat mengatasi kendala dalam penggunaan bukti digital, mengoptimalkan peran digital forensik sebagai instrumen penting dalam penyelesaian kasus penipuan daring di Indonesia, memperkuat penegakan hukum secara keseluruhan, dan meningkatkan perlindungan hukum bagi masyarakat Indonesia.

## DAFTAR PUSTAKA

Arief, Barda Nawawi. 2007. Masalah Kebijakan Hukum Pidana dalam Penanggulangan Kejahatan. Bandung: Citra Aditya Bakti.

Marzuki, Peter Mahmud. 2014. Penelitian Hukum. Jakarta: Kencana Prenanda Media Group.

Masukun dan Wiwik Meilararti. 2017. Aspek Hukum Penipuan Berbasis Internet. Bandung: Keni Media.

Sitompul, Josua. 2012. Cyberspace Cybercrime Cyberlaw Tinjauan Aspek Hukum Pidana. Jakarta: Tatanusa.

Suseno, Sigid. 2012. Yuridiksi Tindak Pidana Siber. Bandung: Refika Aditama.

Waluyo, Bambang. 2017. Viktimologi Perlindungan Korban & Saksi. Jakarta: Sinar Grafika.

Widodo. 2011. Aspek Hukum Pidana Kejahatan Mayantara. Yogyakarta: Aswaja Pressindo..

Beebe, Nicole L., and Jonathan G. Clark. 2005. “A Formal Definition of Digital Forensics.” International Journal of Digital Evidence, 4(1), 1–22.

Butar-Butar, Monika Elisabet Lamtiur, dkk. 2016. “Pembuktian Tindak Pidana Penipuan Melalui Media Online Dilihat dari Perspektif Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik.” Diponegoro Law Review, 5(2), 1–14.

Carrier, Brian D. 2005. “A Hypothesis-Based Framework for Digital Investigations.” Digital Investigation, 2(1), 24–35.

Darwis, Nurlely. 2019. “Kriminology pada Bidang Kebijakan ‘Cyber Security’.” Jurnal Ilmiah Hukum Dirgantara, 9(2), 18–29.

Hutasoit, Kristian. 2018. “Tinjauan Yuridis terhadap Tindak Pidana Penipuan Secara Online dalam Perspektif Hukum Pidana di Indonesia.” Jurnal Fakultas Hukum Universitas Sumatera Utara, (Januari), 1–14.

Noor Rahmad. 2019. "KAJIAN HUKUM TERHADAP TINDAK PIDANA PENIPUAN SECARA ONLINE." Jurnal Hukum Ekonomi Syariah Magister Ilmu Hukum Universitas Muhammadiyah Yogyakarta, 3(2), 105–116.

Prasetiyo dan Mukhtar Zuhdy. 2020. "Penegakan Hukum oleh Aparat Penyidik Cyber Crime dalam Kejahatan Dunia Maya (Cyber Crime) di Wilayah Hukum Polda DIY." Indonesian Journal of Criminal Law and Criminology (IJCLC), 1(2), 75–84.

Priyana, Puti, dkk. 2021. "Alat Bukti Informasi Elektronik Tindak Pidana Penipuan Online dalam Perspektif Hukum Acara Pidana di Indonesia." Jurnal IUS Kajian Hukum dan Keadilan, 9(1), 181–196.

Reith, Harald, Julian Carr, and Gregg Gunsch. 2002. "An Examination of Digital Forensic Models." International Journal of Digital Evidence, 1(3), 1–12.

Syaza Dyah Utami, dkk. 2021. "Analisis Live Forensic pada Whatsapp Web untuk Pembuktian Kasus Penipuan Transaksi Elektronik." Cyber Security dan Forensik Digital, 4(1), 23–30.