

Artikel Penelitian

## Penanggulangan Kejahatan Penipuan Online (Studi Kasus di Wilayah Hukum Polres Metro Jakarta Barat)

*Raihan Ramadhan<sup>\*</sup>, Idris Wasahua**Fakultas Hukum Universitas Esa Unggul, Jakarta Barat, DKI Jakarta, Indonesia*

### INFORMASI ARTIKEL

Diterima Redaksi: 28 Desember 2025

Revisi Akhir: 10 Januari 2025

Diterbitkan Online: 15 Februari 2026

### KATA KUNCI

Cyber Crime

Penipuan

Undang-Undang ITE

### KORESPONDENSI (\*)

E-mail: [raihanramdhn07012000@gmail.com](mailto:raihanramdhn07012000@gmail.com)

### A B S T R A K

Tujuan penelitian ini adalah untuk mengetahui: bagaimana Modus Operandi para pelaku Penipuan online di wilayah Polres Jakarta Barat, Dan bagaimana Penanggulangan tindak Pidana Penipuan Online di Wilayah Hukum Polres Metro Jakarta Barat. Penelitian ini menggunakan Metode Empiris. Hasil penelitian ini menunjukkan bahwa upaya atau upaya penanggulangan hukum dalam menangani kejahatan siber dapat berupa upaya preventif, upaya preventif, dan upaya represif. Berbagai modus operandi yang semakin beragam seperti Phising meretas aplikasi mobile banking, Money Mule jenis penipuan yang meminta korban untuk menerima sejumlah uang ke rekening, Pharming penipuan daring yang melibatkan kode, social engineering atau rekayasa sosial, sniffing tindakan penyadapan, upaya penanggulangan kejahatan penipuan yaitu upaya penanggulangan kejahatan melalui jalur nonpenal Upaya penanggulangan kejahatan perlu ditempuh dengan pendekatan kebijakan secara terpadu (integral), dimana terdapat keterpaduan antara kebijakan kriminal dengan kebijakan sosial juga penanggulangan dengan sarana penal dan non-penal. Penelitian ini mengupas mengenai Modus dan cara penanggulangan Kejahatan Penipuan Online.

## PENDAHULUAN

Perkembangan kecanggihan teknologi memudahkan setiap orang untuk berkomunikasi bahkan bertransaksi satu dengan yang lainnya, membantu masyarakat untuk mencari informasi dan melakukan berbagai aktivitas transaksi bisnis atau transaksi jual beli melalui online shop. Internet pun telah memberikan kontribusi yang demikian besar bagi masyarakat, perusahaan atau industri maupun pemerintah (Imamah et al).

Teknologi informasi telah membuka mata dunia akan sebuah dunia baru, interaksi baru, dan sebuah jaringan bisnis dunia yang tanpa batas. Disadari betul bahwa perkembangan teknologi yang disebut internet, telah mengubah pola interaksi masyarakat, yaitu interaksi bisnis, ekonomi (Janaloka & 2022), sosial, dan budaya. Internet telah memberikan kontribusi yang demikian besar pada masyarakat, industri, maupun pemerintah. Internet seakan sudah menjadi kebutuhan primer bagi masyarakat, khususnya daerah perkotaan, Internet bukan hanya konsumsi golongan tertentu saja seperti tahun-tahun sebelumnya, namun sudah merambah ke masyarakat golongan menengah kebawah. Masyarakat dapat dengan mudah berkomunikasi tanpa ada batas jarak, ruang, dan waktu dilakukan tanpa meninggalkan tempat atau komunitas dimana ia berada dan aktivitas ini bisa dilakukan dimana dan kapan saja. Interaksi sosial tidak lagi terbatas dalam sekat-sekat teritorial suatu negara.

Seiring kemajuan teknologi informasi (internet) dan segala bentuk manfaat di dalamnya membawa konsekuensi negatif tersendiri, dimana semakin mudahnya para penjahat untuk melakukan aksinya yang semakin meresahkan masyarakat. Kejahatan tersebut perlu mendapatkan tindakan yang tegas dengan dikeluarkan undang-undang terhadap kejahatan maya yaitu dengan diberlakukan Undang-undang nomor 1 Tahun 2024 (R. I.-A. L. Journal & 2024) Tentang Perubahan Kedua atas Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik, yang merupakan usaha untuk memberikan kepastian hukum tentang kerugian akibat cybercrime tersebut (Efektifitas et al).

Undang-undang ini, akibat dari lemahnya penanggulangan yang digunakan sebelumnya yang mengacu pada Kitab Undang-Undang Hukum Pidana (KUHP) dan peraturan perundangan lainnya. Tujuan hukum adalah menciptakan nilai keadilan dalam tatanan masyarakat. Selain nilai keadilan, hukum juga bertujuan untuk menciptakan ketertiban dalam masyarakat. Kejahatan adalah suatu nama atau cap yang diberikan orang untuk menilai perbuatan-perbuatan tertentu, sebagai perbuatan jahat, dengan demikian maka si pelaku disebut sebagai penjahat (Firdaus et al., 2019)

Pada dasarnya setiap teknologi diciptakan untuk memenuhi suatu kebutuhan tertentu manusia, setelah diciptakan teknologi dikembangkan agar semakin efisien dan efektif, untuk memenuhi kebutuhan yang dimaksud. Di era digital seperti sekarang, banyak kejahatan-kejahatan yang terjadi dengan menggunakan sarana teknologi informasi. Salah satunya adalah perbuatan membuat akun media sosial palsu (R. D.-T. M. L. Journal & 2020, 2020). Akun palsu termasuk dalam golongan cyber bullying, cybercrime. Dalam cyber bullying, akun palsu termasuk dalam jenis fraping, profil palsu dan catfishing. Fraping adalah tindakan mencuri, masuk ke akun media sosial korban dan mem-posting konten tak pantas, seakan-akan si korban yang melakukan, profil palsu biasanya diciptakan seseorang yang menyembunyikan identitasnya dengan tujuan mem-bully korbannya. Akun palsu biasanya digunakan untuk memantau aktivitas seseorang/kelompok, dibuat untuk tujuan bisnis, dibuat untuk menggiring opini publik, dibuat untuk menjatuhkan seseorang/kelompok (Kajian & 2020). Selain itu juga, untuk mengelabui sasarannya untuk berkenalan dan melancarkan aksinya untuk meraup keuntungan. Hal inilah yang menjadi dasar pemerintah perlu mendukung pengembangan teknologi informasi melalui infrastruktur hukum dan pengaturannya, sehingga pemanfaatan teknologi informasi dilakukan secara aman untuk mencegah penyalahgunaannya dengan memperhatikan nilai-nilai agama dan sosial budaya masyarakat Indonesia (Nusantara & 2022).

Secara yuridis formal tindak kejahatan merupakan bentuk tingkah laku yang melanggar undang-undang harus dihindari dan barangsiapa yang melanggarnya, maka akan dikenakan pidana. Jadi larangan-larangan dan kewajiban-kewajiban tertentu yang harus ditaati oleh setiap warga Negara wajib dicantumkan dalam undang-undang maupun peraturan-peraturan pemerintah, baik ditingkat pusat maupun tingkat daerah (Laminating 1996) (Bastian et al.). Tindak pidana berarti suatu perbuatan yang pelakunya dapat dikenai hukum pidana, dan pelaku-pelaku ini dapat dikatakan sebagai "subjek" tindak pidana. Peristiwa pidana itu adalah suatu perbuatan atau rangkaian perbuatan manusia, yang bertentangan dengan undang-undang atau peraturan perundangundangan lainnya, terhadap perbuatan mana diadakan tindakan penghukuman" (Chazawi 2014). Perbuatan yang dapat dikenakan pidana dibagi menjadi dua yakni perbuatan yang dilarang oleh undang-undang dan orang yang melanggar larangan itu. Secara idealnya dapat dikatakan tidak ada suatu perkara pidana dapat diadili dengan serta merta ketika seseorang dianggap melanggar ketentuan hukum pidana.

Tindak pidana merupakan suatu dasar yang pokok dalam menjatuhkan pidana pada orang yang telah melakukan perbuatan pidana atas dasar pertanggung jawaban seseorang atas perbuatan yang telah dilakukannya, tapi sebelum itu mengenai dilarang dan diancamnya suatu perbuatan yaitu mengenai perbuatan pidananya sendiri, yaitu sebagaimana yang tercantum dalam Pasal 1 ayat (1) Kitab Undang-Undang Hukum Pidana (KUHP) bahwa tiada suatu perbuatan boleh dihukum, melainkan atas kekuatan ketentuan pidana dalam undang-undang yang ada terdahulu dari pada perbuatan itu. Penipuan secara online pada prinsipnya sama dengan penipuan konvensional, yang membedakan hanyalah pada sarana perbuatannya yakni menggunakan Sistem Elektronik (komputer, internet, perangkat telekomunikasi). Berdasarkan data awal yang diperoleh penulis dari Polres Metro Jakarta Barat, terdapat 500 kasus penipuan secara online dengan rentang waktu dari Januari – Mei 2024.

Salah satu kasus yang sudah di tangani oleh Unit Cyber Polres Jakarta Barat yang di terangkan oleh Beripka Yogi seperti kasus penipuan berikut. Tim Cyber Crime melakukan pengejar dan penangkapan hasil laporan dari salah satu tempat hiburan di wilayah Taman Sari, Jakarta Barat terduga pelaku penipuan dapat ditangkap oleh unit Cyber Crime Polres Metro Jakarta Barat. Bripka Yogi, mengungkapkan modus operandi pelaku adalah memasukan foto-foto wanita sexy kedalam akun instagram beserta tarifnya dan apabila korban berminat maka korban akan disuruh transfer uang ke rekening pelaku".

Sementara Polisi mengamankan tiga orang terduga pelaku yaitu AK yang di tangkap di bekasi, kemudian Polisi mengembangkannya lagi dan terungkap bahwa ada lagi pelaku lain yang berada di dalam lapas. Bripka Yogi mengatkan bahwa Kasat Reskrim Polres Metro Jakarta Barat berkordinasi dengan Ka Lapas untuk meminta keterangan dari pelaku yang berinisial MBS dan NF. Dari keterangan AK bahwa penipuan di kendalikan oleh NF untuk membuat rekening Bank dan mendaftarkan nomor handphone yang dimiliki untuk sarana M Banking kemudian NF memberikan handphone tersebut kepada MBS yang juga berada dalam lapas. Kemudian MBS membuat akun instagram palsu berinisial GCS dengan menampilkan foto-foto wanita-wanita painu bisa di Booking Out (BO) dengan tarif Rp.3.8 juta untuk LC bias dan Rp.4.7 juta untuk LC premium. Pelaku sudah menjalankan aksinya sekitar awal januari 2018 dengan hasil penipuan ini pelaku meraup Omzet 25 juta per minggu dan di bagi tiga

Subnit Cyber Crime Satuan Reserse Kriminal Polres Metro Jakarta Barat membongkar praktek penyebaran konten video pornografi melalui aplikasi dream live yang mempertontonkan secara live streaming. Akibat aksi tidak

senonoh tersebut polisi mengamankan Dua perempuan berinisial LS (21) dan PP (19) Keduanya berperan sebagai host di bawah agensi bernama INFINITY 4EVER yang dikepalai oleh DSP (33). Dimana kasus tersebut terbongkar saat anggota cyber melakukan patroli siber dan menemukan beberapa akun diantaranya akun @upil dan @yayang melalui aplikasi dream live melakukan siaran langsung konten pornografi.

Kasat Reserse Kriminal Polres Metro Jakarta Barat Kompol Andri Kurniawan mengatakan, dari pengungkapan tersebut kami mengamankan 3 orang pelaku "Ke 3 orang pelaku tersebut memiliki peran berbeda-beda diantaranya, PP als Upil (sebagai Host), LS als Yayang (sebagai Host) dan DSP (33) sebagai agency," ujar Kasat Reskrim Polres Metro Jakarta Barat Kompol Andri Kurniawan saat press conference dimapolres, Selasa, 14/3/2023.

Andri menjelaskan, pihaknya lantas melakukan pengembangan dan berhasil meringkus dua host tersebut di tempat berbeda.

Diketahui, pemilik akun @upil adalah PP. Ia ditangkap di daerah Jalan H. Som, Pondok Pucung, Pondok Aren Kota, Tangerang Selatan. Sementara pemilik @yayang adalah LS. Ia ditangkap di Jalan Raya Kebayoran Lama, Jakarta Selatan. Adapun pemilik agensi berinisial DSP, ditangkap di Jalan Cipinang Kebembem, Pisangan Timur, Pulogadung, Jakarta Timur. "Dari aplikasi tersebut, Kepolisian Resort Jakarta Barat melakukan pengungkapan dan akhirnya diamankan tiga orang pelaku. Tiga pelaku itu kami amankan di beberapa tempat berbeda. "Ada 14 barang bukti, mulai dari pakaian yang digunakan pada saat live, kemudian handphone, buku, serta hasil screenshot pornografi, aksi ketiganya itu sudah berlangsung selama lebih dari tiga bulan. Dari hasil live tersebut, ketiganya mendapat keuntungan sebesar Rp 6 juta sampai Rp 15 juta.

## TINJAUAN PUSTAKA

### 1. Pengertian Kejahatan Penipuan Online

Kejahatan penipuan online merupakan suatu tindakan ilegal yang dilakukan dengan memanfaatkan teknologi informasi dan komunikasi, khususnya internet, untuk menipu korban dengan tujuan mendapatkan keuntungan secara melawan hukum. Kejahatan ini bisa berbentuk scam, phishing, jual beli barang palsu, investasi bodong, dan modus lainnya yang memanfaatkan kepercayaan korban terhadap media digital.

Menurut Clarke & Cornish (1985), kejahatan online merupakan fenomena baru dalam kriminologi yang muncul seiring perkembangan teknologi informasi dan globalisasi, sehingga memerlukan pendekatan penanggulangan khusus. (sesuaikan referensi jika perlu) Beberapa peneliti menyatakan bahwa kejahatan penipuan online mempunyai karakteristik berbeda dengan kejahatan konvensional, karena bersifat lintas negara, cepat, anonim, dan sulit dilacak tanpa dukungan teknologi forensik digital (Wall, 2007; McGuire, 2012)(Solim et al.).

### 2. Teori Kejahatan dan Teknologi Informasi

Dalam analisis kejahatan penipuan online, Routine Activity Theory menyatakan bahwa kejahatan terjadi ketika ada pelaku yang termotivasi, target yang rentan, dan tidak adanya penjagaan yang efektif (Cohen & Felson, 1979). Dalam konteks penipuan online, pelaku menggunakan medium internet sebagai alat untuk menghubungi korban (target) yang rentan karena kurangnya pemahaman akan risiko digital, sementara pengawasan (guardianship) menjadi rendah karena keterbatasan sistem keamanan digital dan penegakan hukum.

Sementara itu, Crime Pattern Theory menjelaskan bahwa perkembangan teknologi menciptakan peluang baru yang secara geografis tidak terbatas sehingga mempengaruhi pola terjadinya kejahatan. Penipuan online dapat terjadi kapan saja dan di mana saja tanpa batas wilayah hukum tradisional, kecuali melalui koordinasi aparat penegak hukum (Brantingham & Brantingham, 1984).

### 3. Perkembangan Kejahatan Penipuan Online di Indonesia

Data Kepolisian Republik Indonesia mencatat peningkatan signifikan laporan kasus penipuan yang melibatkan media digital dalam beberapa tahun terakhir. Penyidik di berbagai Polda dan Polres, termasuk Unit Siber, membentuk strategi penanggulangan khusus melalui penyelidikan digital forensik, cyber patrol, dan kerja sama dengan penyedia layanan teknologi. Dalam studi yang dilakukan oleh Putra (2020), disimpulkan bahwa kurangnya edukasi masyarakat dan keterbatasan sumber daya penyidik menjadi kendala utama dalam menanggulangi kejahatan ini.

Menurut laporan terbaru tahun 2024, Direktorat Tindak Pidana Siber Bareskrim Polri mencatat ratusan ribu laporan penipuan online dengan kerugian masyarakat mencapai angka miliaran rupiah. Banyak modus seperti investment scam, penipuan jual beli online, serta penipuan melalui aplikasi pesan instan menjadi sorotan utama.

#### 4. Konsep Penanggulangan Kejahatan Online

Penanggulangan kejahatan penipuan online dilakukan melalui beberapa pendekatan:

##### 4.1. Kebijakan dan Regulasi

Undang-Undang Informasi dan Transaksi Elektronik No. 11 Tahun 2008 jo. UU 19 Tahun 2016 (ITE) menjadi dasar hukum utama dalam menangani kejahatan siber di Indonesia. Pasal-pasal dalam UU ITE memberikan landasan untuk mengusut tindakan penipuan yang dilakukan melalui fasilitas elektronik.

Selain itu, Kitab Undang-Undang Hukum Pidana (KUHP) dan UU Perlindungan Konsumen juga dimanfaatkan sebagai alat hukum pelengkap dalam penegakan kasus penipuan online (Hidayat, 2021).

##### 4.2. Penegakan Hukum dan Penyidikan Digital

Penegakan hukum terhadap penipuan online membutuhkan kompetensi penyidik dalam investigasi digital forensik, pengumpulan bukti elektronik, kerja sama dengan platform digital dan lembaga internasional, serta pengembangan teknologi pelacakan IP, open-source intelligence (OSINT), dan lain-lain. Menurut Susanto (2019), keberhasilan penyidikan sangat dipengaruhi oleh kemampuan aparat dalam mengintegrasikan bukti digital ke dalam proses hukum secara sah dan meyakinkan.

##### 4.3. Pencegahan Melalui Edukasi

Pencegahan kejahatan ini juga memerlukan edukasi masyarakat untuk meningkatkan literasi digital, identifikasi modus penipuan, serta pemahaman hak dan kewajiban saat bertransaksi online. Literasi digital yang rendah seringkali menyebabkan masyarakat menjadi korban penipuan online (Rahmawati, 2022)..

## METODOLOGI

1. Metode penelitian yang digunakan oleh penulis adalah penelitian hukum empiris. Penelitian hukum empiris adalah pengumpulan data yang didapat dari lapangan melalui cara wawancara atau interview dengan pihak-pihak yang berhubungan seperti Unit Cybr Crime Polres Metro Jakarta Barat (Soekanto 1984).

2. Jenis dan Sumber Data

##### a) Data Primer

Data primer ialah merupakan data yang diambil dengan cara interview yang merupakan wawancara dan tanya jawab dengan narasumber secara langsung yaitu dari Unit Cyber Polres Metro Jakarta Barat.

##### b) Data Sekunder

Data sekunder adalah data yang diperoleh dari bahan Pustaka dengan menelaah literatur dan dokumen terkait Penipuan Berbasis Online (Sunggono 1997). Data yang diperoleh secara tidak langsung yang dapat

Untuk mengumpulkan data sekunder, juga memperoleh data dengan studi literatur dan sumber-sumber yang berkorelasi dengan penelitian, studi ini dimaksudkan untuk mendapatkan landasan teori yang cukup, guna mendukung analisis penelitian. Data sekunder diperoleh dengan membaca berbagai literatur yang berhubungan dengan penelitian, serta penelusuran situs internet untuk mencari data-data yang terkait dengan penelitian yang akan dilakukan.

### Kerangka Teori

Kerangka teori ini berisi teori-teori hukum yang relevan untuk digunakan membahas dan menganalisis masalah hukum dalam penelitian ini, teori tersebut ialah sebagai berikut:

1. Teori Kriminologi tentang Modus Kejahatan

Modus operandi merupakan salah satu aspek kriminologi yang mempelajari tingkah laku kejahatan manusia. Tingkah laku ini disebabkan pula oleh beberapa faktor seperti sosial, ekonomi, dan psikologis, yang membentuk pilihan pribadi seseorang berdasarkan apa yang mereka inginkan. Menurut Martin L. Haskell dan Lewis Yablonsky menulis bahwa kriminologi sebagai salah satu studi ilmiah kejahatan dan penjahat mencakupi analisa-analisa tentang:

- a) Sifat dan luas kejahatan
- b) Sebab-sebab kejahatan
- c) Perkembangan Hukum
- d) Pidana dan pelaksanaan peradilan pidana
- e) Ciri-ciri penjahat serta modus kejahatan
- f) Pola kriminalitas dan
- g) Akibat kejahatan atas perbuatan

Modus operandi berasal dari bahasa Latin, artinya prosedur atau cara bergerak atau berbuat sesuatu. Istilah modus operandi diartikan sebagai cara atau teknik yang berciri khusus dari seorang atau kelompok penjahat dalam melakukan perbuatan jahatnya yang melanggar hukum dan merugikan orang lain, baik sebelum, ketika, dan sesudah perbuatan kriminal tersebut dilakukan. Secara leksikal istilah modus operandi diartikan sebagai cara atau teknik yang berciri khusus dari seorang atau kelompok penjahat dalam melakukan perbuatan jahatnya yang melanggar hukum dan merugikan orang lain, baik sebelum, ketika, dan sesudah perbuatan kriminal tersebut dilakuka

Menurut para subjek penelitian dan info dari informan, penipuan dengan memasukan foto-foto sexy kedalam akun isntagram beserta tarifnya ini terjadi akibat faktor ekonomi, faktor lingkungan, ataupun faktor pengaruh dari sosial media Instagram yang membuat informasi tersebar dengan cepat sehingga timbul suatu kejahatan yaitu penipuan (Takanjanji 2021).

## 2. Teori Penanggulangan Kejahatan

Pada prinsipnya kebijakan kriminal merupakan kajian yang luas yang terdiri dari kebijakan penal dan kebijakan nonpenal. Hal ini merujuk pada upaya penanggulangan kejahatan menurut G P. Hoefnagels , yaitu (Nawawi Arief 2002) penerapan hukum pidana (criminal law application);

- a) Pencegahan tanpa pidana (prevention without punishment);
- b) Mempengaruhi pandangan masyarakat tentang kejahatan dan pemidanaan melalui media masa (influencing views of society on crime and mass media)

Sehingga, penanggulangan kejahatan pada intinya terdiri dari dua hal pokok, yaitu pendekatan penal dan pendekatan non penal. Jika pendekatan pertama yang ditempuh, maka ini berarti bahwa penanggulangan suatu kejahatan dilakukan dengan menggunakan hukum pidana yang difungsikan sebagai sarana pengendali sosial, yaitu dengan sanksinya yang berupa pidana untuk dijadikan sarana menanggulangi kejahatan. Dengan demikian diharapkan norma-norma sosial dapat ditegakkan dengan sanksi yang dimiliki hukum pidana terhadap seseorang yang berperilaku tidak sesuai dengan norma-norma tersebut.

Secara umum, substansi hukum penal dalam wujudnya sebagai peraturan perundang-undangan, telah diterima sebagai instrument resmi yang memperoleh aspirasi untuk dikembangkan, yang diorientasikan secara pragmatis untuk menghadapi masalah-masalah sosial (kejahatan) yang kontemporer. Hukum demikian dinamakan hukum responsif yang menampakkan ciri bahwa hukum ada bukan demi hukum itu sendiri, bukan demi kepentingan praktisi hukum, juga bukan untuk membuat pemerintah senang, melainkan hukum ada demi kepentingan rakyat di dalam masyarakat.

Kebijakan penal sebagai salah satu sarana penanggulangan kejahatan memiliki keterbatasan- keterbatasan. Sehingga, diperlukan upaya lain yang dilakukan untuk menanggulangi kejahatan. Upaya lain selain hukum pidana yang berusaha menanggulangi kejahatan inilah kemudian dapat dikatakan sebagai upaya “non penal”, yaitu suatu upaya rasional dalam menanggulangi kejahatan dengan upaya-upaya lain selain hukum pidana (penal). Oleh karena itu dilihat dari kebijakan kriminal sebaiknya ditempuh dengan pendekatan kebijakan integral, baik dengan menggunakan “penal” maupun dengan sarana “non- penal”.

## HASIL DAN PEMBAHASAN

### **Modus-modus operandi para pelaku Kejahatan Penipuan online di wilayah hukum Polres Jakarta Barat.**

Modus kejahatan dalam cybercrime terutama mengenai penipuan online sulit dimengerti oleh orang-orang yang tidak menguasai pengetahuan teknologi informasi. Sebab, salah satu karakter pokok penipuan online adalah penggunaan sarana teknologi informasi dalam modus operandinya. Sifat inilah yang membuat penipuan online berbeda dengan tindak pidana lainnya (konvensional).

Pengertian Modus Operandi dalam ruang lingkup kejahatan yaitu operasi cara atau Teknik yang berciri khusus dari seorang penjahat dalam melakukan perbuatan jahatnya. Modus operandi berasal dari Bahasa latin yang berarti prosedur atau cara bergerak atau berbuat sesuatu. Dalam hukum pidana tradisional, seseorang dikatakan sebagai penjahat atau pelaku kejahatan apabila orang tersebut telah melakukan kejahatan yang dapat dihukum dimasa lampau. Pada umumnya dari sudut pandang Masyarakat, kita lebih berkepentingan melindungi Masyarakat dari Tindakan-tindakan dimasa depan daripada membalas dendam kepada penjahat bagi tindakan-tindakannya dimasa lampau.

Perhatian orang lebih terarah pada kemungkinan timbulnya bahaya dimasa depan daripada kejahatan yang telah lewat. Dalam pandangan hukum sendiri penjahat atau pelaku kejahatan adalah seseorang yang dianggap telah melanggar kaidah-kaidah hukum dan perlu dijatuhi hukuman. Namun perlu diketahui pula tentang ukuran-ukuran yang menentukan apakah seseorang dapat diperlakukan sebagai penjahat atau tidak. Kriminalitas berasal dari kata “crimen” yang berarti kejahatan. Pengertian tindak kriminalitas menurut bahasa adalah sama dengan kejahatan yaitu perkara kejahatan yang

dapat dihukum menurut Undang- Undang, sedangkan pengertian kriminalitas menurut istilah diartikan sebagai suatu kejahatan yang tergolong dalam pelanggaran hukum positif (hukum yang berlaku disuatu Negara).

Pengertian kejahatan sebagai unsur tindak kriminalitas secara sosiologis mempunyai 2 unsur (Bripka Yogi), yaitu: Kejahatan ialah perbuatan yang merugikan secara ekonomis dan merugikan secara psikologis dan melukai perasaan susila dari suatu segerombolan manusia, dimana orang-orang itu berhak melahirkan celaan. Dengan demikian, pengertian kriminalitas adalah segala macam bentuk tindakan dan perbuatan yang merugikan secara ekonomis dan psikologis yang melanggar hukum yang berlaku dalam Negara Indonesia serta noma- norma sosial dan agama.

Pengertian modus operandi adalah teknik cara- cara beroperasi yang dipakai oleh penjahat. Berdasarkan pada data di lapangan dapat diketahui bahwa modus operandi pelaku tindak pidana penipuan online bervariasi karena modus yang digunakan berbeda-beda bergantung pada lokasi yang akan digunakan sebagai sasaran menjalankan perbuatann. Kejahatan yang berhubungan erat dengan penggunaan teknologi yang berbasis komputer dan jaringan telekomunikasi yaitu cybercrime dikelompokkan dalam beberapa bentuk sesuai modus operandi yang ada.

Beripka Yogi menerangkan bahwa Dalam periode Januari – Mei 2024 terjadi 500 kasus kejahatan dunia maya yang masuk kedalam catatan Polres Metro Jakarta Barat, modus-modus tersebut antara lain sebagai berikut:

No	Jenis	Modus Operandi	Jumlah
1	Phising	Pelaku dalam menjalankan aksinya memanfaatkan korban dengan menggunakan email, sms tautan, atau website palsu yang dibuat semirip mungkin dengan situs resminya. Dengan begitu, korban akan menjadi lebih percaya.  Tujuan daru pshising Adalah mencuri data pribadi, meliputi password, nomer kartu kredit, atau OTP. Data yang didapat dimanfaatkan pelaku untuk kepentingan pribadi	90
2	Mony Mule	Modus money mule merujuk pada Tindakan mentransfer uang kepada pelaku. Cara yang digunakan Adalah dengan membuat korban tergiur dengan penawaran yang diajukan. Setelahnya, korban akan berhasil masuk dalam perangkap dengan mengirimkan sejumlah uang sesuai yang diminta pelaku. Target dari modus ini ialah pelajar, pencari kerja, hingga pengguna aplikasi kencan online.	59
3	Pharming	Pharming tidak dilakukan dengan mengirim link palsu melalui email atau media social. Melainkan, pelaku menggunakan modifikasi domain name system (DNS) dengan mengirim malware mengacu pada program yang diciptkan secara khusus untuk masuk kedalam sebuah system tanpa diketahui pemiliknya. Malware tersebut akan memanipulasi domain Perusahaan. Ketika korban hendak mengunjungi website tertentu, korban secara tanpa sadar akan diarahkan kepada website palsu yang didesain semirip mungkin dengan aslinya untuk mengambil data pribadi.	60
4	Social Engineering	Modus Pelaku dalam jenis ini mereke memanfaatkan orang terdekat. Pelaku akan mengaku-ngaku sebagai seseorang yang korban ini kenal atau percaya. Dengan begitu, korban dapat menjadi lebih percaya dan berkenan untuk membagikan data pribadi hingga sejumlah uang kepada pelaku	102
5	Sniffing	Merupaka Tindakan kejahatan penyadapan yang dilakukan pelaku penyadapan jaringan internet dengan tujuan utama mencuri data dan informasi penting seperti username dan password m-banking kata sandi email dan data-data penting lainnya. Tindakan ini pelaku kejahatan	44

		ini mengincar pengguna internet ditempat public, seperti kafe, mall, atau bandara. Para pelaku dengan sengaja memasang sinyal internset tersebut sebagai pancingan. Saat korban menautkan gawainya keinternet tersebut, pelaku dapat dengan mudah mencuri berbagai data pribadinya.	
6	Pornografi	Dengan menyebarkanluarkan foto sexy di social media	145

Penipuan online termasuk kedalam kejahatan cybercrime kelompok data forgery, artinya kejahatan tersebut bekerja dengan memalsukan data pada dokumen-dokumen penting yang tersimpan sebagai scripless document melalui Internet. Beberapa pasal dalam UnadngUndang ITE untuk menjerat pelaku tindak pidana cybercrime akan ditampilkan ke dalam bentuk tabel dibawah ini:

Teknologi Infromasi sebagai objek		Teknologi Informasi sebagai Fasilitas	
Pasal	Muatan	Pasal	Muatan
Ps 46 Jo Ps 30	Mengakses sistem orang lain	Ps 45 Jo Ps 27	<b>Pelanggaran asusila, perjudiam, penghinaan atau pencemaran nama baik.</b>
Ps 47 Jo PS 31	Melakukan intersepsi atau penyadapan (Illegal Interception)	Ps 45 ayat (2) Jo PS 28	<b>Penipuan menyebarkan informasi yang menyesatkan</b>
PS 48jo Ps 32	Perbuatan melawan hukum terhadap sistem/dokumen elektronik (data interference)	PS 45 ayat (3) jo Ps 29	<b>Pengancamaan kekerasan</b>
Ps 49 jo Ps 33	<b>Terganggunya sistem komputer</b>	Ps 51 ayat (1) jo Ps 35	<b>Pemalsuan Informasi/dokumen elektronik</b>

Penipuan online diatur dalam Pasal 28 ayat (1) Undang-Undang ITE yang berbunyi, “Setiap Orang dengan sengaja dan tanpa hak menyebarkan berita bohong dan menyesatkan yang mengakibatkan kerugian konsumen dalam Transaksi Elektronik” dengan ancaman pidana enam tahun dan/atau denda paling banyak Rp. 1 Miliar (Pasal 45 ayat (2) UU ITE). Apabila tindak pidana penipuan tersebut dilakukan tidak menggunakan media teknologi informasi maka menggunakan Pasal 378 KUHP yang dirumuskan sebagai berikut “Barangsiapa dengan maksud untuk menguntungkan diri sendiri atau orang lain atau orang lain secara melawan hukum, dengan memakai nama palsu atau martabat palsu, dengan tipu muslihat, ataupun rangkaian kebohongan, membujuk orang lain untuk menyerahkan barang sesuatu kepadanya, ata supaya memberi utang atau menghapuskan piutang, diancam karena penipuan dengan pidana penjara paling lama empat tahun.” Oleh karena itu, penegak hukum harus jeli apakah kasus tersebut dijerat dengan Undang-Undang ITE atau dengan KUHP, sebab perbedaannya sangatlah tipis mengingat saat ini teknologi informasi semakin berkembang dan menjadi kebutuhan sehari-hari. Alat bukti juga diperlukan untuk menentukan apakah laporan tersebut memenuhi syarat pidana terhadap Undang-Undang ITE atau termasuk ke dalam hukum pidana biasa.

### Bagaimana Penanggulangan Kejahatan Penipuan Online di Wilayah Hukum Polres Metro Jakarta Barat

Tindak pidana penipuan yang dilakukan secara online secara khusus diatur dalam dalam undang- undang nomor 19 tahun 2016 tentang perubahan atas undang-undang 11 tahun 2008 tentang Informasi dan Transaksi elektronik. Dalam hal ini, UU ITE ini tidak secara rinci menyatakan adanya tindak pidana penipuan, tetapi secara implisit terdapat unsur yang hampir sama dengan tindak pidana penipuan yang diatur secara umum dalam Pasal 378 Kitab Undang- Undang Hukum Pidana (KUHP) (Maskun 2002).

Dengan demikian, sekiranya kebijakan penanggulangan kejahatan (politik kriminal) dilakukan dengan menggunakan saran pena; (hukum pidana), maka kebijakan hukum pidana, khususnya pada tahap kebijakan yudikatif/aplikatif harus mempehatikan dan mengarah pada tercapainya tujuan dari kebijakan sosial ini, berupa social-welfare dan social-defence (Prasteyo 2014).

Dalan wawancara pada tanggal 07 Mei 2024, pukul 14.00 WIB dengan narasumber Bapak Yogi selaku Satuan Reserse Kriminal Polres Metro Jakarta Barat telah menerima 500 (lima ratus) laporan berkenaan dengan kasus cybercrime dari awal tahun 2024 sampai bulan mei 2024. Kasat Reskrim Polres Metro Jakarta Barat AKBP Edi Suranta Sitepu. SIK,

mengungkapkan Modus yang dilakukan oleh pelaku memasukan foto- foto wanita sexy kedalam akun instgram beserta tarifnya dan apabila korban berminat maka korban akan disuruh transfer uang ke rekening pelaku,”ungkap AKBP Edi Suranta Sitepu. SIK. Polisi mengamankan tiga orang terduga pelaku yaitu AK yang di tangkap di bekasi, kemudian Polisi mengembangkannya lagi dan terungkap bahwa ada lagi pelaku lain yang berada di dalam lapas,”tutur Kasat AKBP Edi Suranta Sitepu. SIK.

Dalam menanggulangi terjadinya kejahatan cyber, pihak kepolisian Polres Jakarta Barat telah melakukan berbagai upaya seperti memberikan himbauan ke masyarakat melalui media elektronik maupun media sosial dengan menyebarkan broadcast berupa himbauanhimbau terkait cybercrime untuk di forward ke masyarakat luas. Selain itu dilakukan juga penerangan ke masyarakat melalui media surat kabar dan radio, serta pada saat mengisi acara talkshow pihak kepolisian tidak henti-hentinya memberikan himbauan kemasyarakat.

Melihat dari data kasus tindak pidana penipuan di dunia maya yang terjadi di wilayah Polres Metro Jakarta Barat, adapun upaya yang dilakukan pihak Polres Metro Jakarta Barat dalam mencegah dan menanggulangi tindak pidana penipuan didunia maya tersebut sesuai dengan aturan yang berlaku :

- a) Upaya preventif (pencegahan): upaya yang dilakukan Polres Metro Jakarta Barat dengan cara melakukan pencegahan melalui penyuluhan ke masyarakat. Tugas ini dilakukan oleh Unit Satbimas (Satuan Bimbingan Masyarakat) yang bertugas melakukan pembinaan kepada masyarakat.
- b) Upaya represif: upaya Polres Metro Jakarta Barat dalam menangani tindak pidana yang telah terjadi dengan cara melakukan tindakan berupa proses lidik dan sidik. Proses lidik seperti menerima laporan pengaduan dari masyarakat yang kemudian akan dilakukan penanganan lebih lanjut oleh Unit Tipiter. Proses sidik seperti laporan pengaduan yang telah diterima, akan dikoordinasikan dengan Unit Opsnal, berikut ini akan dipaparkan beberapa kasus cyer crime yang telah ditangani oleh Kepolisian Polres Jakarta Barat 2024:

No	Jenis	Ketentuan Pidana	Jumlah
1	Phising	Pasal 30	90
2	Mony Mule	Pasal 27 ayat 4 dan pasal 29	59
3	Pharming	Pasal 30	60
4	Social engineering	Pasal 28 ayat 1	102
5	Sniffing	Pasal 30	44
6	<b>Pornografi</b>	<b>Pasal 27 ayat 1</b>	<b>145</b>

Berdasarkan hasil wawancara dengan Reskrimsus Polres Jakarta Barat, urutan dari penanggulangan hukum terhadap Cyber Crime laporan polisinya kebanyakan menggunakan model B, sebagaimana dimaksud pada pasal 5 ayat (1) huruf b Peraturan Kapolri Nomor 14 Tahun 2012 tentang Manajemen Pendidikan Tindak Pidana yaitu adalah Laporan Polisi yang dibuat oleh anggota Polri atas laporan/pengaduan yang diterima dari masyarakat

- c) untuk memeriksa laporan korban apakah bisa dilakukan penanganan lebih lanjut atau tidak, jika bisa maka penyidik akan terjun langsung kelapangan untuk melakukan penindakan sesuai prosedur penyidik kepolisian.
- d) Upaya penanggulangan melalui kebijakan hukum pidana dilaksanakan melalui kriminalisasi hukum pidana yaitu dengan pembentukan undang-undang yang secara khusus mengatur perbuatan yang dilarang tersebut. Upaya penanggulangan tindak pidana siber (cybercrime) melalui sarana penal tercantum dalam Undang-Undang Nomor 19 Tahun 2016 tentang perubahan atas Undang- Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik. Upaya penanggulangan tindak pidana penipuan yang dilakukan secara online melalui sarana penal diatur pada Pasal 28 ayat (1) UU ITE. Penyebaran berita bohong dan penyesatan merupakan padanan kata yang semakna dengan penipuan. Penipuan dapat dilakukan dengan motivasi, yaitu untuk menguntungkan dirinya dan merugikan orang lain secara sekaligus. Dengan motivasi-motivasi tersebut, maka penyebaran berita bohong dan penyesatan dapat dikategorikan sebagai penipuan. Secara umum penipuan itu telah diatur sebagai tindak pidana dalam Pasal 378 KUHP (Suhariyanto 2013).
- e) Upaya atau kebijakan untuk melakukan pencegahan dan penanggulangan kejahatan yang merupakan bagian kebijakan kriminal ini, tidak terlepas dari kebijakan yang lebih luas, yaitu kebijakan sosial (social policy) yang terdiri dari kebijakan/upaya-upaya untuk kesejahteraan social dan kebijakan upaya- upaya untuk perlindungan masyarakat (Martuli T. Situmeang 2020).
- f) Kasus penipuan online atau kasus-kasus cyber crime di Jakarta Barat ini dari tahun ke tahun semakin meningkat. Maka dari itu perlu adanya kerjasama dari masyarakat untuk melaporkan setiap kejahatan yang dialaminya ke Polres Metro Jakarta Barat. Polres Metro Jakarta Barat sementara memberikan penyuluhan- penyuluhan kepada masyarakat tentang dampak bertransaksi lewat media online dan bagaimana mencegah atau menanggulangi kejahatan penipuan online.

Untuk mengatasi masalah penipuan di dunia maya yang masih banyak terjadi, penting untuk meningkatkan dan mengkonsolidasikan regulasi yang jelas, komprehensif, dan tegas terkait dengan penipuan di dunia maya. Ini harus disertai dengan upaya penanggulangan yang efektif dan pengawasan yang lebih ketat di lingkungan digital. Selain itu, kerja sama internasional juga penting untuk mengatasi penipuan di dunia maya yang melintasi batas negara. Penanggulangan hukum menuntut polisi harus berada di atas supremasi hukum, pada sisi lain polisi menjalankan tugas sosial kemasyarakatan yang harus memperhatikan nilai-nilai yang hidup dalam masyarakat. Kedua hal tersebut menimbulkan kesenjangan dalam implementasinya karena di satu sisi terdapat ketentuan hukum yang berlaku bagi polisi untuk menjalankan tugasnya seperti menerima laporan kasus hukum, melaksanakan penyelidikan dan penyidikan kasus. Keterbatasan alat-alat khusus cybercrime yang dimiliki oleh Polres Metro Jakarta Barat untuk menunjang sarana prasarana penyidik dalam mengungkap tindak pidana penipuan online. Maka dari itu penyidik berupaya menanggulangnya dengan cara:

- a. Meningkatkan kerjasama antar lembaga bank secara bilateral dalam upaya penanganan cybercrime, antara lain melalui perjanjian yang telah ditentukan oleh kedua belah pihak.
- b. Meningkatkan kerjasama dengan operator selular atau internet service provider dan tidak membatasi penyidik dalam membuka identitas pelaku. Memberikan saran kepada penyedia layanan operator selular dan internet untuk meningkatkan system pengamanan jaringan komputer nasional sesuai standar nasional.
- c. Meningkatkan kinerja POLRI untuk lebih mengayomi masyarakat, meningkatkan penyuluhan dan berperan aktif membina masyarakat tentang pengetahuan masalah kejahatan konvensional maupun kejahatan modus baru, serta pentingnya mencegah kejahatan tersebut terjadi lagi.

Di sisi lain kasus hukum yang dilaporkan oleh masyarakat sering bertentangan dengan nilai agama dan nilai sosial, sehingga dapat menimbulkan masalah yang membuat dilema antara tugasnya sebagai penegak hukum dan fungsinya sebagai pelindung dan pengayom masyarakat yang dijiwai dengan nilai moral, agama, dan budaya yang berbeda di setiap daerah. Pengembangan kemampuan dan kekuatan Polri dikelola sedemikian rupa agar dapat mendukung pelaksanaan tugas dan tanggungjawab Polri sebagai lembaga yang bertugas melindungi keamanan dalam negara

## KESIMPULAN DAN SARAN

Berdasarkan hasil penelitian dan pembahasan mengenai langkah Kepolisian Metro Jakarta Barat dalam menanggulangi tindak penipuan perdagangan online dapat dikemukakan kesimpulan sebagai berikut:

1. Modus Operandi Para pelaku Kejahatan Penipuan online di wilayah hukum Polres Metro Jakarta Barat dengan berbagai macam bentuk yaitu;
  - a) Phising,( meretas aplikasi mobile banking) Modus Phising menjadi jurus penipuan klasik. Kendati demikian, masih banyak masyarakat yang lengah dalam penipuan jenis ini. Phising memanfaatkan korban dengan menggunakan email, SMS, tautan, atau website palsu yang dibuat semirip mungkin dengan dengan situs resminya.
  - b) Money mule, (penipuan yang meminta korban untuk menerima sejumlah uang ke rekening) Selain phising, money mule diketahui sebagai tipe penipuan kedua yang sering terjadi di wilayah Hukum Polres Jakarta Barat. Kejadian ini memiliki dampak signifikan pada institusi finansial di Indonesia. Pasalnya, modus money mule merujuk pada tindakan mentransfer uang kepada pelaku. Cara yang digunakan adalah dengan membuat korban tergiur dengan penawaran yang diajukan.
  - c) Pharming, (penipuan daring yang melibatkan kode) Istilah pharming terdiri atas dua kata, yakni phising dan farming. Sedikit berbeda dengan modus phising sebelumnya, pharming tidak dilakukan dengan mengirim link palsu melalui email atau media sosial. Melainkan, pelaku menggunakan modifikasi domain name system (DNS) dengan mengirim malware ke gawai korban.
  - d) Social engineering, (rekayasa sosial) Penipuan jenis social engineering umumnya memanfaatkan orang terdekat. Pelaku akan mengaku sebagai seseorang yang korban kenal atau percaya.
  - e) Snifing, (tindakan penyadapan) Merupakan Tindakan kejahatan penyadapan yang dilakukan pelaku penyadapan jaringan internet dengan tujuan utama mencuri data dan informasi penting seperti username dan password m-banking kata sandi email dan data-data penting lainnya.
2. Penanggulangan Kejahatan Penipuan Online di Wilayah Hukum Polres Metro Jakarta Barat Menurut Bpk Bripka Yogi dilakukan melalui berbagai cara penanggulangan menurut beberapa uraian kasus sebagai berikut
  - a) Phising dan Pharming

Upaya penanggulangan dapat ditempuh dengan 1) Penerapan hukum pidana; 2) Pencegahan tanpa pidana; dan 3) Mempengaruhi pandangan masyarakat tentang kejahatan dan pemidanaan melalui media masa. Untuk kategori pertama dikelompokkan ke dalam upaya penanggulangan kejahatan lewat jalur penal, sedangkan kedua dan ketiga termasuk upaya penanggulangan kejahatan melalui jalur nonpenal. Upaya melalui jalur penal merupakan upaya represif yang dalam pelaksanaannya mengandung keterbatasan sehingga perlu diimbangi dengan pendekatan non-penal yang cenderung merupakan upaya preventif

b) *Mony Mule*, *Social Engineering* dan *Snifing*

Upaya penanggulangan kejahatan perlu ditempuh dengan pendekatan kebijakan secara terpadu (integral), dimana terdapat keterpaduan antara kebijakan kriminal dengan kebijakan sosial juga penanggulangan dengan sarana penal dan non-penal. Selanjutnya kebijakan hukum pidana berkaitan dengan masalah kriminalisasi yaitu perbuatan apa yang akan dijadikan tindak pidana dan penalisasi, yaitu sanksi apa yang sebaiknya dikenakan kepada si pelanggar.

Kepolisian Jakarta Barat melakukan upaya penanggulangan tindak pidana dengan Melakukan penyuluhan atau sosialisasi Penyuluhan atau sosialisasi yang dilakukan oleh kepolisian Jakarta Barat yaitu sosialisasi dan penyuluhan kepada masyarakat baik itu merupakan pelajar, remaja, karang taruna, instansi, organisasi wanita, dan lain-lain. Sosialisasi dan penyuluhan tersebut berkaitan dengan segi hukum yaitu meliputi sanksi pengaturan mengenai tindak pidana penipuan online, moral dan kesusilaan akan bahaya serta dampak dari pornografi.

Unit Satreskrim (Satuan Reserse Kriminal) Polres Metro Jakarta Barat bertanggung jawab untuk menangani kasus-kasus kriminal, termasuk tindak pidana penipuan di dunia maya. Terdapat beberapa upaya yang telah dilakukan oleh Unit Satreskrim dalam mencegah tindak pidana penipuan di dunia maya:

- a. Penyelidikan dan penindakan,
- b. Kerjasama dengan Unit PPA dan lembaga terkait,
- c. Kerjasama dengan platform online dan penyedia layanan internet,
- d. Pengawasandunia maya atau cyberpatrol.

Kombinasi penggunaan alat teknis, pendidikan, komunikasi terbuka, dan pengawasan aktif oleh orang tua atau pengawas merupakan pendekatan yang lebih efektif dalam mempromosikan penggunaan internet yang aman bagi anak-anak. Pencegahan tindak pidana penipuan membutuhkan pendekatan yang komprehensif dari berbagai unit kepolisian, lembaga pemerintah, dan masyarakat. Kerjasama, edukasi, dan penanggulangan yang kuat menjadi kunci dalam upaya pencegahan ini.

Dalam upaya penanggulangan kejahatan dan perlindungan hukum terhadap tindak pidana cyber penipuan di dunia maya di wilayah Polres Metro Jakarta Barat yang berpedoman pada pasal 2 undang- undang No. 2 Tahun 2002 tentang kepolisian Republik Indonesia, Undang-Undnag No 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik, Undang- Undnag No. 40 tahun 1999 Tentang Pers, Undang- Undang tentang Perlindungan Saksi dan Korban.

## SARAN

1. Pihak kepolisian Polres Metro Jakarta Barat perlu meningkatkan kinerjanya dalam melakukan terhadap tindak penipuan online baik secara preventif, pre-emptif, dan represif yang di dukung dengan pemberdayaan sumber daya manusia terutama kepada personel kepolisian untuk diberikan pembekalan mengenai ilmu cyber yang didukung dengan sarana prasarana yang memadai dibidang teknologi agar dapat secara tegas menangani kasus cybercrime terutama dalam kasus penipuan online yang marak terjadi.
2. Masyarakat hendaknya lebih berhati-hati dan meningkatkan kewaspadaan dengan berbagai cara dari tindak pidana penipuan online yang terjadi akhir-akhir ini menunjukkan tingkat kualitas yang lebih canggih dan kadang-kadang tidak masuk akal.

## DAFTAR PUSTAKA

- Bastian, M., Sutanto, R., Mimar, R. B.-J. H., & 2025, undefined. (). Evaluasi Efektivitas Undang-Undang No. 1 Tahun 2024 Tentang Informasi dan Transaksi Elektronik dalam Pencegahan Cyberterrorism. *Jurnal.Unsur.Ac.Id*. Retrieved December 28, 2025, from <https://jurnal.unsur.ac.id/jhmj/article/view/4997>
- Chazawi, Adam. 2014. *Pelajaran Hukum Pidana Bagian I*. Jakarta.
- Dirgantara, Ryan. 2020. "Analisis Kejahatan Begal Dengan Motivasi Perampokan Di Kota

- Palu.” *Tadulako Master Law Journal* 4(2).
- Efektifitas, A., Nomor, U.-U., 2024, T., Pasal, D., Judi, M., Di, O., Banjarmasin, K., Rizkan Gymnastiar, I., Rahman, M. K., Rizky, M., Alauddin, F., Syaifullah, H. D., Islam, U., & Banjarmasin, N. A. (). Analisis Efektifitas Undang-Undang Nomor 1 Tahun 2024 Di Pasal 27 Mengenai Judi Online Di Kota Banjarmasin. *Shariajournal.Com*, 2, 694–703. Retrieved December 28, 2025, from <http://www.shariajournal.com/index.php/IERJ/article/view/529>
- Firdaus, F., Negeri, K., & Abstrak, P. (2019). Analisis Ketentuan Masa Waktu Penyidikan Terkait Dengan Hak Asasi Tersangka Dalam Proses Peradilan Pidana. *103.245.72.41F FirdausTadulako Master Law Journal*, 2019•103.245.72.41. <http://103.245.72.41/index.php/TMLJ/article/view/184>
- Imamah, S., Anomie, S. J.-, & 2023, undefined. (). ANALISIS RATIONAL CHOICE THEORY DALAM PENIPUAN JUAL BELI ONLINE (STUDI KASUS PENIPUAN TIKET KONSER DI MEDIA SOSIAL TWITTER). *Jom.Fisip.Budiluhur.Ac.IdS Imamah, S JuliantiAnomie, 2023•jom.Fisip.Budiluhur.Ac.Id*, 5, 183–192. Retrieved December 28, 2025, from <https://jom.fisip.budiluhur.ac.id/anomie/article/view/426>
- Janaloka, H. R.-, & 2022, undefined. (). Penanggulangan Kejahatan Penipuan Belanja Online Di Wilayah Kepolisian Daerah Jawa Timur. *Janalokajournal.Id*. Retrieved December 28, 2025, from <https://janalokajournal.id/index.php/jnk/article/view/16>
- Journal, R. D.-T. M. L., & 2020, undefined. (2020). Analisis kejahatan begal dengan motivasi perampokan di Kota Palu. *103.245.72.41R DirgantaraTadulako Master Law Journal*, 2020•103.245.72.41, 2. <http://103.245.72.41/index.php/TMLJ/article/view/199>
- Journal, R. I.-A. L., & 2024, undefined. (). Tindak Pidana Informasi Elektronik dan Transaksi Elektronik Berdasarkan Undang-Undang Nomor 1 Tahun 2024. *Journal.Andrewlawcenter.or.Id*. Retrieved December 28, 2025, from <http://journal.andrewlawcenter.or.id/index.php/ALJ/article/view/35>
- Kajian, J. T.-W. P. H. J., & 2020, undefined. (). Merefleksi Penegakan Hukum Tindak Pidana Penipuan Online. *Ejournal.Widyamataram.Ac.Id*. Retrieved December 28, 2025, from <http://ejournal.widyamataram.ac.id/index.php/pranata/article/view/260>
- Indonesia. *Undang-Undang Noor 1 Tahun 2004 Tentang Perubahan Kedua Atas Undang- Undang Nomor 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik ( Tambahan Lembar Negara Republik Indonesia Nomor 6905*
- Laminating, P. A 1996. *Dasar-Dasar Hukum Pidana Indonesia*. Bandung: PT. Citra Aditya Bakti.
- Martuli T. Situmeang, Sahat. 2020. *Cyber Law*. Bandung: Cv. Cakara.
- Maskun. 2002. *Kejahatan Siber (Cyber Crime): Suatu Pengantar*. Jakarta: Prenada Media.
- Nawawi Arief, Barda. 2002. *Bunga Rampai Kebijakan Hukum Pidana*. Bandung.
- NUSANTARA, S. S.-T., & 2022, undefined. (). Optimalisasi Hukum Siber (cyber law) dalam Penanggulangan Kejahatan Penipuan melalui Internet dalam Menyelamatkan Kehidupan Masyarakat. *Ojs.Uninus.Ac.Id*. Retrieved December 28, 2025, from <https://ojs.uninus.ac.id/index.php/TEKNOLOGINUSANTARA/article/view/2420>
- Prasteyo, Teguh. 2014. *Hukum Pidana Edisi Revisi*. 2014: Grafindo Persada.
- Solim, J., Septian Rumapea, M., Wijaya, A., Monica Manurung, B., & Lionggodinata, W. (). Upaya Penanggulangan Tindak Pidana Penipuan Situs Jual Beli Online Di Indonesia. *Ejurnalunsam.Id*. Retrieved December 28, 2025, from <https://ejurnalunsam.id/index.php/jhsk/article/view/1157>
- Sitompul, Josua. 2012. *Cyberspace Cybercrime Cyberlaw Tinjauan Aspek Hukum Pidana*. Jakarta: Tatanusa.
- Soekanto, Soerjono. 1984. *Pengantar Metode Penelitian Hukum*. Jakarta.
- Suhariyanto, Budi. 2013. *Tindak Pidana Teknologi Informasi (CyberCrime) UrgensiPengaturan Dan Celah Hukumnya*. Jakarta: Raja Grafindo Persada.
- Sunggono, Bangbang. 1997. *Metode Penelitian Hukum*. Jakarta: Raja Grafindo Persada.
- Takanjanji, Jefri. 2021. “Merefleksi Penegakan Hukum Tindak Pidana Penipuan Online.” *Widya Pranata Hukum : Jurnal Kajian Dan Penelitian Hukum* 2(2). doi: 10.37631/widyapranata.v2i2.260.