

PENEGAKAN CYBERLAW TERHADAP DATA FORGERY PADA KASUS PENIPUAN TIKET KONSER DI MEDIA SOSIAL

Ria Enandini, Mega Amalia, Zuhriyah, Yuliani, Angela Vicky Novitasari Damanik

Sistem Informasi, Universitas Bina Sarana Informatika

Jl. Kemanggisan Utama Raya, Palmerah, Jakarta

riaenandini1@gmail.com

ABSTRAK

Media sosial kini tidak hanya berfungsi sebagai sarana komunikasi, tetapi juga menjadi wadah utama aktivitas ekonomi digital. Namun, perkembangan ini turut memunculkan risiko kejahatan siber, salah satunya penipuan tiket konser yang marak terjadi pada 2023–2024 dengan modus *data forgery*. Penelitian ini bertujuan untuk menganalisis penipuan tiket konser sebagai bentuk *cybercrime* serta meninjau efektivitas regulasi hukum, khususnya UU ITE dan UU No. 1 Tahun 2024, dalam memberikan perlindungan bagi korban. Metode yang digunakan adalah studi pustaka (*library research*) dengan pendekatan deskriptif kualitatif melalui analisis literatur, jurnal, berita daring, dan peraturan perundang-undangan yang relevan. Hasil penelitian menunjukkan bahwa meskipun Indonesia telah memiliki dasar hukum yang kuat, implementasi perlindungan hukum masih menghadapi kendala seperti keterbatasan bukti digital, rendahnya literasi digital, dan modus kejahatan yang terus berkembang. Penelitian ini merekomendasikan penguatan kapasitas aparat dalam forensik digital, peningkatan literasi masyarakat, serta kolaborasi lintas sektor untuk menciptakan ekosistem transaksi daring yang lebih aman. Selain itu, regulasi perlu disusun secara adaptif agar mampu merespons dinamika kejahatan siber di masa mendatang.

Kata kunci: *cybercrime, cyberlaw, data forgery, penipuan, media sosial*

1. PENDAHULUAN

Media sosial telah menjadi bagian internal dari kehidupan sehari-hari masyarakat Indonesia. Media sosial merupakan sarana komunikasi yang memungkinkan penggunanya untuk saling berinteraksi, menjalin kerja sama, berbagi informasi, sekaligus menampilkan identitas diri [1]. Selain menjadi sarana komunikasi, media sosial juga berfungsi sebagai tempat berjualan, menyebarkan informasi terkini, bahkan membentuk pandangan publik terhadap suatu produk [2]. Hal ini menunjukkan bahwa media sosial bukan hanya sebagai ruang interaksi, tetapi juga telah menjadi media utama bagi aktivitas ekonomi masyarakat modern.

Seiring meningkatnya aktivitas ekonomi di media sosial, muncul berbagai risiko penyalahgunaan yang merugikan masyarakat. Salah satu bentuk penyalahgunaan yang marak terjadi adalah penipuan tiket konser melalui akun palsu, pemalsuan identitas penjual, hingga pemalsuan bukti transfer atau tiket elektronik. Modus ini dikenal sebagai *data forgery*. *Data forgery* merupakan perilaku memanipulasi atau mengubah informasi secara tidak sah dengan tujuan memperoleh keuntungan pribadi dari pihak lain [3].

Salah satu kasus yang cukup besar terjadi pada November 2023, ketika Polres Jakarta Pusat menerima laporan penipuan 400 tiket konser Coldplay dengan kerugian mencapai Rp1,3 miliar [4]. Di tahun berikutnya penipuan kembali terjadi tepatnya Mei 2024, fans NCT Dream juga menjadi korban penipuan tiket konser dengan kerugian ditaksir lebih dari Rp200 juta [5].

Dalam perspektif hukum, praktik pemalsuan data dan penipuan daring tersebut termasuk dalam kategori

cybercrime atau kejahatan siber. Istilah *cyber* merujuk pada sesuatu yang bersifat maya, sedangkan *crime* berarti tindakan yang tergolong sebagai kejahatan [6]. Kejahatan siber adalah bentuk kriminalitas yang berlangsung melalui jaringan komputer pada internet [7]. *Cybercrime* sendiri merupakan bentuk pelanggaran hukum yang terjadi melalui jaringan internet [8]. Untuk menanganinya dibutuhkan cyberlaw atau hukum siber. *Cyberlaw* merupakan cabang hukum yang berasal dari istilah *cyberspace law*, dengan cakupan yang meliputi segala hal yang berkaitan dengan individu maupun subjek hukum lain dalam pemanfaatan teknologi internet atau media elektronik, sejak seseorang terhubung “*online*” hingga memasuki dunia maya [9].

Indonesia sendiri telah memiliki dasar hukum untuk menangani dan memberikan sanksi terhadap kejahatan siber. Salah satu aturan tersebut adalah Undang-Undang Informasi Dan Transaksi Elektronik (UU ITE) yang pertama kali ditetapkan melalui UU No. 11 Tahun 2008 dan kemudian diperbarui dengan UU No. 19 Tahun 2016. Kehadiran regulasi ini menjadi konsekuensi dari pesatnya perkembangan ilmu pengetahuan, teknologi, serta arus globalisasi yang mendorong percepatan dalam pengelolaan, akses, dan penyampaian data maupun informasi [10]. Selain itu, hadir pula UU No. 1 Tahun 2024 sebagai perubahan kedua kalinya dari UU No. 11 Tahun 2008 tentang informasi dan transaksi elektronik (ITE) [11]. Regulasi terbaru ini menegaskan kembali sanksi terhadap perbuatan penipuan daring, misalnya pada Pasal 28 ayat (1) yang melarang distribusi atau transmisi informasi menyesatkan yang mengakibatkan kerugian materiil bagi konsumen, dengan ancaman

pidana penjara hingga 6 tahun dan/atau denda maksimal Rp1 miliar sebagaimana diatur dalam Pasal 45A ayat (1) [12].

Kehadiran UU No. 1 Tahun 2024 menunjukkan adanya upaya negara dalam memperkuat kerangka hukum menghadapi dinamika kejahatan digital yang semakin kompleks, termasuk penipuan tiket konser berbasis media sosial. Namun demikian, implementasi regulasi tersebut tetap menghadapi kendala, seperti keterbatasan bukti digital, rendahnya literasi digital masyarakat, serta modus kejahatan yang terus beradaptasi lebih cepat dibandingkan regulasi.

Berdasarkan uraian di atas, penelitian ini bertujuan untuk menganalisis fenomena penipuan tiket konser sebagai bentuk *cybercrime*. Penelitian ini juga ditujukan untuk mengkaji sejauh mana regulasi hukum, khususnya UU ITE dan UU No. 1 Tahun 2024, mampu memberikan perlindungan hukum bagi masyarakat yang menjadi korban penipuan daring.

2. TINJAUAN PUSTAKA

2.1. *Cybercrime*

Cybercrime dapat dipahami sebagai bentuk tindak kejahatan yang berkaitan dengan komputer, yang pada dasarnya mencakup penggunaan perangkat komputer secara tidak sah [13]. *Cybercrime* adalah tindakan kejahatan yang memanfaatkan komputer dan teknologi digital, meliputi akses data tanpa izin, perusakan perangkat elektronik, serta pelanggaran terhadap keamanan dan privasi seperti pencurian PIN dan kata sandi [14]. Secara umum *cybercrime* dibagi menjadi 7 jenis [15].

2.2. *Unauthorized access to computer system and service*

Merupakan tindakan kriminal yang dilakukan dengan cara memasuki suatu jaringan komputer tanpa izin dan tanpa sepengetahuan pemiliknya. Motif pelaku seringkali untuk melakukan sabotase, misalnya mencuri data rahasia, meskipun ada pula pelaku yang hanya bersifat coba-coba atau iseng, ingin menguji kemampuan menembus sistem yang memiliki tingkat proteksi tinggi.

2.3. *Illegal contents*

Merupakan bentuk kejahatan siber yang dilakukan dengan menyebarkan data atau informasi di internet yang bersifat tidak etis atau menyesatkan dan berpotensi mengganggu ketertiban publik. Contohnya, penyebaran informasi palsu mengenai rahasia negara untuk menimbulkan propaganda terhadap pemerintah, atau mempublikasikan konten berisi fitnah maupun pornografi yang merendahkan kehormatan seseorang.

2.4. *Data forgery*

Merupakan kejahatan yang dilakukan dengan memalsukan data pada dokumen penting yang tersimpan dalam bentuk *scriptless document* melalui jaringan internet. Jenis kejahatan ini sering menyasar sistem *e-commerce*, di mana pelaku memanipulasi

data agar tampak seolah terjadi kesalahan penulisan, padahal tindakan tersebut dilakukan untuk memperoleh keuntungan pribadi dari pihak yang dirugikan.

2.5. *Cyber espionage*

Merupakan bentuk kejahatan yang dilakukan dengan cara memata-matai individu atau pihak lain melalui pemanfaatan jaringan internet dalam sistem jaringan komputer. Umumnya, kejahatan ini menyasar pesaing bisnis dengan tujuan memperoleh akses terhadap dokumen atau data penting yang tersimpan dalam sistem komputer mereka. Jika informasi yang berhasil diperoleh tergolong rahasia, pelaku dapat melanjutkan aksinya dengan melakukan pemerasan, misalnya melalui ancaman lewat e-mail, untuk menekan korban agar menuruti kehendaknya.

2.6. *Cyber sabotage and extortion atau cyber terrorism*

Merupakan perbuatan kriminal ini dilakukan dengan membuat perangkat lunak berbahaya, misalnya virus, *worm*, *trojan*, *adware* atau *browser hijacker* yang bertujuan mengganggu, merusak, atau menghancurkan data serta program pada komputer yang tersambung ke internet. Pelaku sering menyisipkan *logic bomb* atau jenis *malware* lain sehingga sistem operasi dan aplikasi tidak lagi berfungsi sebagaimana mestinya; alih-alih bekerja normal, komputer tersebut dikendalikan dari jarak jauh sesuai kehendak pelaku.

2.7. *Offense against intellectual property*

Merupakan bentuk pelanggaran di dunia maya yang berkaitan dengan kepemilikan Hak Atas Kekayaan Intelektual (HAKI). Tindakan ini dapat berupa peniruan tampilan situs web milik orang lain secara ilegal tanpa izin dari pemilik aslinya, meskipun situs tersebut telah memiliki perlindungan hukum atas hak cipta. Selain itu, pelanggaran juga bisa terjadi melalui penyebaran informasi rahasia dagang milik pihak lain di internet. Perbuatan tersebut dapat merugikan reputasi perusahaan atau individu, terutama jika dilakukan melalui media sosial seperti WhatsApp, Facebook, Twitter, Instagram, Skype, Camfrog, MIRC, atau melalui penyebaran email massal yang mengungkap informasi rahasia perusahaan kepada publik.

2.8. *Infringements of privacy*

Merupakan tindak kejahatan yang melanggar kerahasiaan data pribadi seseorang yang tersimpan dalam sistem komputer. Jika data tersebut bocor dan diketahui oleh pihak yang tidak berwenang, korban dapat mengalami kerugian baik secara materiil maupun nonmateriil. Contoh data pribadi yang termasuk kategori rahasia di antaranya adalah nomor kartu kredit, PIN ATM, hingga informasi medis yang bersifat pribadi.

2.9. Cyberlaw

Upaya menanggulangi kejahatan siber memerlukan paying hukum khusus di ranah digital, yang sering disebut *cyberlaw* atau hukum siber [16]. Istilah hukum siber berakar dari kata *cyberlaw*, yang kini secara global dipahami sebagai cabang hukum yang membahas penggunaan serta penerapan teknologi informasi. Selain itu, istilah ini juga sering disebut dengan beberapa nama lain seperti Hukum Teknologi Informasi (*Law of Information Technology*), Hukum Dunia Maya (*Virtual World Law*), maupun Hukum Mayantara [17]. *Cyberlaw* berasal dari kata *Cyberspace Law*. Hukum ini diperkirakan akan memiliki peran penting di masa mendatang, mengingat hampir seluruh aspek kehidupan manusia kini telah tersentuh oleh perkembangan teknologi. Oleh karena itu, dibutuhkan seperangkat aturan yang mampu mengatur berbagai aktivitas dalam ruang digital tersebut [18].

2.10. Penelitian Terdahulu

Beberapa penelitian terdahulu yang membahas mengenai kejahatan siber (*cybercrime*) dan penerapan hukum siber (*cyberlaw*).

Penelitian dalam [19] membahas maraknya kejahatan siber berupa pemalsuan akun dan manipulasi data pada platform *e-commerce*. Permasalahan yang diangkat yaitu lemahnya penegakan hukum terhadap pelaku fake account yang memanfaatkan sistem digital untuk memperoleh keuntungan ilegal melalui modus penipuan dan *data forgery*. Hasil penelitian menunjukkan bahwa tindakan tersebut termasuk pelanggaran Pasal 35 jo. Pasal 51 ayat (1) Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE) dengan ancaman pidana penjara paling lama 12 tahun dan denda maksimal Rp12 miliar. Penelitian ini menegaskan bahwa penegakan *cyberlaw* perlu diperkuat melalui kolaborasi antara aparat penegak hukum dan penyelenggara platform digital agar pelaku kejahatan siber, khususnya yang berkaitan dengan pemalsuan data di ruang digital seperti media sosial, dapat ditindak secara efektif.

Selanjutnya, penelitian [20] membahas mengenai meningkatnya tindak pidana siber sebagai dampak dari perkembangan teknologi informasi. Masalah utama yang dikaji adalah munculnya berbagai bentuk kejahatan digital seperti *phishing*, *carding*, *ransomware*, *data forgery*, hingga *cyber terrorism* yang semakin sering terjadi di masyarakat. Hasil penelitian menunjukkan bahwa upaya penanggulangan kejahatan siber di Indonesia telah diatur dalam beberapa ketentuan KUHP, antara lain Pasal 362 tentang pencurian, Pasal 378 tentang penipuan, dan Pasal 263 tentang pemalsuan identitas, serta diperkuat dengan ketentuan dalam UU ITE.

Penelitian pada sumber [21] juga membahas mengenai maraknya kasus pemalsuan data (*data forgery*) di era digital akibat kemajuan teknologi informasi. Permasalahan yang diangkat berfokus pada

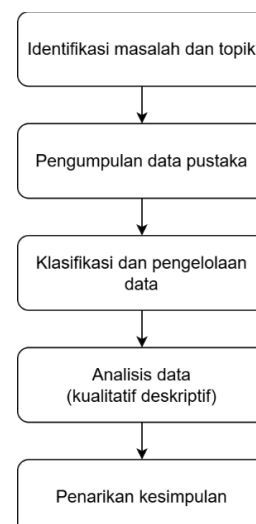
meningkatnya tindak pidana pemalsuan data yang melibatkan manipulasi dokumen elektronik serta lemahnya perlindungan hukum terhadap korban. Hasil penelitian menunjukkan bahwa pemalsuan data merupakan kejahatan serius yang diatur dalam KUHP dan UU ITE, dengan ancaman pidana berupa penjara dan denda. Penelitian tersebut menekankan pentingnya kerja sama antarinstitusi serta penguatan kerangka hukum untuk mencegah dan menanggulangi tindak pidana pemalsuan data di Indonesia.

3. METODE PENELITIAN

Metode penelitian yang digunakan dalam penulisan ini adalah studi pustaka (*library research*). Studi pustaka merupakan metode penelitian yang dilakukan dengan cara menelaah dan mengkaji berbagai sumber pustaka yang relevan dengan topik penelitian. Proses ini mencakup kegiatan mengidentifikasi, mengumpulkan, membaca, mencatat, serta menganalisis berbagai literatur yang memiliki keterkaitan dengan permasalahan yang diteliti [22].

Sumber data yang digunakan dalam penelitian ini berupa data sekunder, yang diperoleh dari jurnal ilmiah, artikel akademik, berita daring, serta peraturan perundang-undangan yang membahas tentang kejahatan siber (*cybercrime*), hukum siber (*cyberlaw*) dan kasus penipuan tiket konser di media sosial. Pemilihan sumber dilakukan secara selektif dengan memperhatikan relevansi, validitas dan kredibilitas informasi yang dikutip.

Penelitian ini menggunakan pendekatan kualitatif deskriptif, yaitu penelitian yang dilakukan melalui pengolahan data yang berkarakter deskriptif [23]. Secara umum, penelitian ini dilakukan melalui beberapa tahapan yang dijelaskan pada Gambar 1 berikut:



Gambar 1. Tahapan penelitian

Adapun penjelasan dari gambar di atas adalah sebagai berikut:

- a. Identifikasi masalah dan topik penelitian dilakukan dengan menentukan fokus kajian yaitu

kejahatan siber dalam bentuk pemalsuan data dan penipuan tiket konser.

- b. Pengumpulan data pustaka dilakukan dengan menelusuri berbagai referensi dari sumber ilmiah dan dokumen hukum yang relevan.
- c. Klasifikasi dan pengelolaan data mencakup proses pemilahan literatur berdasarkan tema dan tingkat kredibilitas.
- d. Analisis data kualitatif deskriptif digunakan untuk menggambarkan dan menjelaskan hasil telaah pustaka secara sistematis
- e. Penarikan kesimpulan merupakan tahap akhir yang merangkum hasil analisis dan memberikan gambaran menyeluruh mengenai penerapan hukum siber terhadap kasus yang dibahas.

4. HASIL DAN PEMBAHASAN

Fenomena penipuan tiket konser yang marak di Indonesia dalam kurun 2023-2024 memperlihatkan bagaimana media sosial tidak hanya menjadi sarana interaksi, tetapi juga ruang yang rawan dimanfaatkan untuk tindak kejahatan siber. Kasus penipuan 400 tiket konser Coldplay pada November 2023 dengan kerugian mencapai Rp1,3 miliar, serta penipuan yang menimpa penggemar NCT Dream pada Mei 2024 dengan kerugian lebih dari Rp200 juta, menjadi bukti nyata bahwa transaksi daring memiliki risiko tinggi. Modus utama yang digunakan pelaku adalah data forgery, yaitu pemalsuan data atau informasi digital dengan tujuan menipu calon pembeli. Pemalsuan tersebut biasanya berupa akun media sosial palsu, bukti pemesanan tiket yang dimanipulasi, hingga e-tiket palsu yang menyerupai tiket asli.

Praktik ini menunjukkan karakteristik *cybercrime* sebagaimana dijelaskan oleh para ahli, yakni tindakan kriminal yang dilakukan melalui jaringan internet dengan memanfaatkan manipulasi data untuk keuntungan pribadi. Oleh karena itu, penipuan tiket konser melalui media sosial dapat dipandang sebagai bentuk nyata kejahatan siber yang merugikan masyarakat.

Dalam perspektif hukum, Indonesia telah memiliki instrument regulasi melalui Undang-Undang Informasi Dan Transaksi Elektronik (UU ITE) yang pertama kali disahkan pada tahun 2008, kemudian diperbarui dengan UU No.19 Tahun 2016 dan terakhir melalui UU No. 1 Tahun 2024. Regulasi terbaru tersebut memperkuat perlindungan hukum dengan menegaskan larangan distribusi atau transmisi informasi menyesatkan yang merugikan konsumen sebagaimana diatur dalam Pasal 28 ayat (1), serta menetapkan ancaman pidana penjara hingga enam tahun dan/atau denda maksimal Rp1 miliar pada Pasal 45A ayat (1). Kehadiran aturan ini pada dasarnya memberikan dasar hukum yang lebih jelas dalam menindak pelaku penipuan daring, termasuk penipuan tiket konser.

Namun, efektivitas perlindungan hukum tersebut belum sepenuhnya tercapai. Aparat penegak hukum masih menghadapi kendala dalam pembuktian digital,

terutama ketika pelaku menggunakan identitas anonim atau akun media sosial palsu. Di sisi lain literasi digital masyarakat masih rendah, sehingga banyak korban mudah percaya pada penjual tanpa melakukan verifikasi keaslian tiket atau identitas penjual. Perkembangan modus kejahatan yang sangat cepat juga menambah kompleksitas, sebab regulasi hukum kerap tertinggal dari inovasi pelaku kejahatan siber.

Analisis ini menunjukkan bahwa meskipun UU ITE dan UU No.1 Tahun 2024 sudah memberikan kerangka hukum yang lebih kuat, namun implementasinya masih terbatas. Perlindungan hukum akan lebih efektif apabila diiringi dengan penguatan kapasitas aparat dalam bidang forensik digital, peningkatan literasi digital masyarakat, serta kolaborasi antara pemerintah, penyelenggara konser, platform media sosial dan lembaga perbankan. Kerjasama lintas sektor dapat memperkecil ruang gerak pelaku, misalnya dengan menciptakan sistem verifikasi penjualan tiket yang lebih aman dan transparan.

Selain itu pembaruan regulasi perlu dilakukan secara adaptif agar mampu merespons bentuk-bentuk *cybercrime* yang terus berkembang. Penambahan pengaturan khusus mengenai penipuan tiket daring, misalnya, dapat menjadi salah satu opsi untuk mempertegas perlindungan hukum bagi masyarakat. Dengan demikian, hasil penelitian ini menegaskan bahwa penipuan tiket konser melalui media sosial bukan hanya sekadar tindak kriminal, tetapi juga tantangan bagi sistem hukum Indonesia dalam menyeimbangkan perkembangan teknologi digital dengan perlindungan hukum yang efektif.

5. KESIMPULAN DAN SARAN

Berdasarkan hasil penelitian, dapat disimpulkan bahwa penipuan tiket konser melalui media sosial merupakan salah satu bentuk kejahatan siber (*cybercrime*) dengan modus *data forgery* atau pemalsuan data digital untuk memperoleh keuntungan pribadi. Meskipun Indonesia telah memiliki dasar hukum melalui UU ITE dan UU No. 1 Tahun 2024 yang memperkuat perlindungan terhadap masyarakat dari kejahatan daring, implementasinya masih menghadapi berbagai kendala seperti keterbatasan bukti digital, rendahnya literasi digital masyarakat, serta perkembangan modus kejahatan yang semakin kompleks. Oleh karena itu, diperlukan peningkatan kapasitas aparat penegak hukum dalam bidang forensik digital, penguatan kerja sama lintas sektor antara pemerintah, platform media sosial, penyelenggara konser, dan lembaga keuangan, serta edukasi masyarakat untuk meningkatkan kewaspadaan terhadap penipuan daring. Sebagai rekomendasi untuk penelitian berikutnya, kajian dapat difokuskan pada pendekatan komparatif mengenai regulasi *cybercrime* di berbagai negara guna menemukan model perlindungan hukum yang lebih efektif. Penelitian lanjutan juga dapat diarahkan pada aspek teknologi, seperti pengembangan sistem keamanan digital

berbasis verifikasi identitas, maupun aspek sosial berupa peningkatan literasi digital masyarakat agar lebih waspada terhadap praktik kejahatan siber. Dengan demikian, penelitian ini tidak hanya memberikan gambaran mengenai kondisi saat ini, tetapi juga membuka peluang bagi studi lanjutan dalam memperkuat perlindungan hukum dan keamanan transaksi digital di masa mendatang.

DAFTAR PUSTAKA

- [1] C. S. Feroza and D. Misnawati, "Penggunaan media sosial instagram pada akun@yhoophii_official sebagai media komunikasi dengan pelanggan," *Jurnal Inovasi*, vol. 14, no. 1, pp. 32–41, 2020.
- [2] D. N. Refilia and N. Pahlawi, "Pemanfaatan media sosial dalam pemasaran produk bank syariah indonesia," *Jurnal Manajemen Dan Bisnis (JMB)*, vol. 4, no. 1, pp. 11–18, 2023.
- [3] G. Nurmansyah, "Perlindungan Hukum Bagi Korban Cybercrime Data Forgery Pada Sektor Perbankan Melalui Internet (E-Banking)," *PERDATA*, vol. 1, no. 3, p. 96, 2023.
- [4] Antara News, "Polres Jakpus Terima Laporan Penipuan 400 Tiket Coldplay, Kerugian Rp 1,3 M." Accessed: Oct. 03, 2025. [Online]. Available: <https://news.detik.com/berita/d-7039154/polres-jakpus-terima-laporan-penipuan-400-tiket-coldplay-kerugian-rp-1-3-m>
- [5] Tasya Natalia, "Penipuan Tiket Konser Terjadi Lagi, Fans NCT Dream Korban Ratusan Juta," *CNBC Indonesia*. Accessed: Oct. 03, 2025. [Online]. Available: https://www.cnbcindonesia.com/research/20240521131024-128-540105/penipuan-tiket-konser-terjadi-lagi-fans-nct-dream-korban-ratusan-juta?utm_source=chatgpt.com
- [6] M. Jubaidi and N. Fadilla, "Pengaruh fenomena cyberbullying sebagai cyber-crime di Instagram dan dampak negatifnya," *Shaut Al-Maktabah: Jurnal Perpustakaan, Arsip dan Dokumentasi*, vol. 12, no. 2, pp. 117–134, 2020.
- [7] A. Suhaemin and M. Muslih, "Karakteristik cybercrime di indonesia," *EduLaw: Journal of Islamic Law and Jurisprudence*, vol. 2, no. 1, pp. 15–26, 2021.
- [8] C. H. Ratulangi, "Tindak pidana cyber crime dalam kegiatan perbankan," *Lex Privatum*, vol. 9, no. 5, 2021.
- [9] Z. Hasan, M. R. Alfath, A. Mahardika, and R. Rizaldi, "Peranan cyber law dalam penanganan tindak pidana di Indonesia," *Jurnal Komunikasi*, vol. 2, no. 5, pp. 337–345, 2024.
- [10] N. Aida, M. Sulaiman, and M. R. Plamesti, "Peningkatan pemahaman peserta didik Madrasah Aliyah Negeri dan Swasta terhadap pemanfaatan teknologi informasi dalam perspektif UU No. 11 tahun 2008 jo UU No. 19 tahun 2016 tentang informasi dan transaksi elektronik," *Journal Of Human And Education (JAHE)*, vol. 3, no. 4, pp. 273–283, 2023.
- [11] Z. Zainal Abidin, Z. Azize, Q. Shodiqah, and R. Rois, "Analisis Penegakan Hukum Terhadap Tindak Pidana Perjudian Online Menurut Undang-Undang Nomor 1 Tahun 2024 Tentang Perubahan Kedua Atas Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik," *Analisis Penegakan Hukum Terhadap Tindak Pidana Perjudian Online Menurut Undang-Undang Nomor 1 Tahun 2024 Tentang Perubahan Kedua Atas Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik*, May 2025.
- [12] Pemerintah Republik Indonesia, "Undang-undang (UU) Nomor 1 Tahun 2024 tentang Perubahan Kedua atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik," *Lembaran Negara Republik Indonesia*. Accessed: Oct. 04, 2025. [Online]. Available: <https://peraturan.bpk.go.id/details/274494/uu-no-1-tahun-2024>
- [13] A. Angkasa and R. Windiasih, "Cybercrime di era industri 4.0 dan masyarakat 5.0 dalam perspektif viktimologi," *Journal Justiciabelen (Jj)*, vol. 2, no. 02, pp. 104–119, 2022.
- [14] N. Setiawan and I. Wahyudi, "Pencegahan fraud pada kejahatan siber perbankan," *Kabillah: Journal of Social Community*, vol. 8, no. 1, pp. 508–518, 2023.
- [15] H. Gunawan, "Tindak Kejahatan Cyber Crime Dalam Perspektif Fikih Jinayah," *Jurnal El-Qanuniy: Jurnal Ilmu-Ilmu Kesyariahan Dan Pranata Sosial*, vol. 6, no. 1, pp. 96–110, 2020.
- [16] S. N. Fitri, "Politik Hukum Pembentukan Cyber Law Undang-Undang Informasi dan Transaksi Elektronik di Indonesia," *Jurnal Justisia: Jurnal Ilmu Hukum, Perundang-Undangan Dan Pranata Sosial*, vol. 7, no. 1, pp. 104–124, 2022.
- [17] A. Rahmadina and R. Faslah, "Perlindungan Hak Cipta Di Era Digital Dalam Perspektif Cyber Law," *Jurnal Ekonomi dan Bisnis Digital*, vol. 2, no. 4, pp. 2251–2257, 2025.
- [18] T. S. Ramli, A. M. Ramli, R. R. Permata, T. Wahyuningsih, and D. Mutiara, "Aspek Hukum Atas Konten Hak Cipta Dikaitkan Dengan Undang-Undang Nomor 19 Tahun 2016 Tentang Informasi Dan Transaksi Elektronik," *Jurnal Legislasi Indonesia*, vol. 17, no. 1, pp. 62–69, 2020.
- [19] A. W. Winarno and A. C. Isradjuningtias, "Perlindungan Hukum Pelaku Usaha E-Commerce Terhadap Pelaku Pemalsuan Akun Konsumen Dalam Perspektif Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik," *Bus. LJ*, vol. 16, p. 261, 2022.

- [20] D. F. T. Popal, "Upaya Penanggulangan Tindak Pidana Mayantara (Cyber Crime)," *Lex Administratum*, vol. 11, no. 5, 2023.
- [21] M. Z. Rizaldi and A. U. Hosnah, "Analisis yuridis terhadap tindak pidana pemalsuan dokumen," *Indonesian Journal of Islamic Jurisprudence, Economic and Legal Theory*, vol. 2, no. 1, pp. 339–349, 2024.
- [22] D. Aprilia and N. Y. A. Apriliyani, "Dina Kajian Psikolinguistik Dalam Pembelajaran Bahasa (Studi Pustaka)," *PENTAS: Jurnal Ilmiah Pendidikan Bahasa dan Sastra Indonesia*, vol. 9, no. 2, pp. 15–22, 2023.
- [23] S. Hanyfah, G. R. Fernandes, and I. Budiarmo, "Penerapan metode kualitatif deskriptif untuk aplikasi pengolahan data pelanggan pada car wash," in *Seminar Nasional Riset dan Inovasi Teknologi (SEMNAS RISTEK)*, 2022