



Cyber Fraud pada Transaksi Game Online melalui Perantara dalam Perspektif UU ITE

Femanoa Zakia Ayugaez¹, Luthfillah Arrizqi Zainsyah²

¹ Hukum, Universitas Negeri Surabaya, Indonesia

Email: femanoa.23292@mhs.unesa.ac.id

² Hukum, Universitas Negeri Surabaya, Indonesia

Email: luthfillahzainsyah@unesa.ac.id

Artikel info

Artikel history:

Received: 05-10-2025

Revised: 20-11-2025

Accepted: 24-12-2025

Published: 29-12-2025

Keywords:

Online Game

Transactions,

Cyber Fraud,

Illegal Escrow

Services, Normative

Legal Research,

Criminal Liability.

Kata kunci:

Transaksi Game

Online, Penipuan

Siber, Layanan

Escrow Ilegal, Riset

Hukum Normatif,

Tanggung Jawab

Pidana.

Abstract. The development of information technology in the digital age has brought significant changes to people's activities, including in the fields of entertainment and internet-based economic transactions. Online games now serve not only as a medium for recreation, but also as part of the digital economy through the buying and selling of accounts, items, and virtual currencies. This development has encouraged the emergence of third parties as transaction intermediaries, but at the same time has increased vulnerability to cybercrime, particularly cyber fraud, such as fraud in the sale and purchase of Mobile Legends accounts using illegal escrow services. This study applies a normative legal method with a legislative, conceptual, and case study approach, referring to Law Number 1 of 2024 concerning Electronic Information and Transactions and the Criminal Code in analyzing the perpetrator's responsibility. The findings of the study indicate that cyber fraud in online game transactions through illegal intermediaries can be subject to sanctions based on Article 28 paragraph (1) in conjunction with Article 45A paragraph (1) of the ITE Law and Article 378 of the Criminal Code. However, challenges in digital evidence, categorizing cyber activities, and determining the liability of intermediaries remain obstacles in law enforcement. Therefore, strengthening technical regulatory mechanisms, enhancing digital literacy, and adopting more adaptive legal interpretations are necessary to ensure optimal user protection.

Abstrak. Kemajuan teknologi informasi pada era digital mengakomodasi transformasi signifikan pada pola kegiatan masyarakat, termasuk dalam bidang hiburan dan transaksi ekonomi berbasis internet. Game online kini tidak semata-mata berguna untuk media rekreasi, namun turut sebagai bagian dari sistem ekonomi digital melalui praktik jual beli akun, item, maupun mata uang virtual. Perkembangan tersebut turut mendorong hadirnya pihak ketiga sebagai perantara transaksi, namun pada saat yang sama meningkatkan kerawanan terhadap kejahatan siber, khususnya cyber fraud, seperti penipuan dalam transaksi jual beli akun Mobile Legends menggunakan layanan rekber ilegal. Studi ini menerapkan metode hukum normatif melalui pendekatan undang-undang, konseptual, dan studi kasus,

dengan mengacu pada Undang-Undang Nomor 1 Tahun 2024 tentang Informasi dan Transaksi Elektronik serta Kitab Undang-Undang Hukum Pidana dalam menganalisis pertanggungjawaban pelaku. Temuan penelitian menunjukkan bahwa tindakan cyber fraud dalam transaksi game online melalui perantara ilegal dapat dikenai sanksi berdasarkan Pasal 28 ayat (1) jo. Pasal 45A ayat (1) UU ITE serta Pasal 378 KUHP. Namun demikian, kendala dalam pembuktian digital, pengkategorian aktivitas siber, dan penentuan tanggung jawab pihak perantara masih menjadi tantangan dalam penegakan hukum, sehingga diperlukan penguatan mekanisme regulasi teknis, optimalisasi tingkat literasi digital, dan juga interpretasi konstitusional yang lebih adaptif guna memastikan perlindungan pengguna secara optimal.

Corresponden author:

Jalan: Jl. Ketintang, Ketintang, Kec. Gayungan, Surabaya, Jawa Timur 60231

Email: femanoa.23292@mhs.unesa.ac.id



Artikel dengan akses terbuka dibawah licensi CC BY-NC-4.0

PENDAHULUAN

Kemajuan teknologi informasi dan komunikasi di era digital mengakomodasi dampak yang nyata terhadap beragam elemen keseharian manusia. Aktivitas sehari-hari saat ini semakin mengandalkan pada penggunaan internet, contohnya dalam bidang hiburan dan transaksi ekonomi. Salah satu fenomena yang berkembang pesat adalah game online, yang tidak lagi hanya berfungsi sebagai sarana hiburan, melainkan juga telah menjadi bagian dari aktivitas ekonomi digital. Hal ini terlihat dari maraknya praktik jual beli akun, item, maupun mata uang virtual yang memiliki nilai tukar cukup tinggi. Fenomena seperti ini yang membuka peluang bagi para pihak ketiga (*third party*) untuk menjadi perantara dalam transaksi, dengan tujuan mempermudah pengguna dan memperoleh keuntungan.

Dalam *game online*, akun pada *game online* merupakan bentuk identitas digital yang menghubungkan pemain dengan sistem permainan. Pembuatan akun biasanya menjadi syarat utama agar data permainan dan informasi pribadi bisa tersimpan dengan baik. Setiap akun memiliki karakteristik tersendiri karena diatur oleh peraturan serta perjanjian layanan yang berlaku pada platform game tersebut. Selain itu, akun juga berperan dalam menjamin keberlangsungan aktivitas saat bermain serta memberikan akses terhadap berbagai fitur yang disediakan oleh platform (Yunior, 2025).

Di sisi lain, layanan perantara transaksi juga semakin banyak bermunculan, baik dalam bentuk marketplace khusus game seperti *Codashop* maupun forum jual beli di media sosial dan komunitas daring. Kehadiran pihak ketiga memang memberikan kemudahan, namun juga membuka celah terjadinya kejahatan siber (*cyber crime*), khususnya *cyber fraud*. *Cyber fraud* secara umum adalah bentuk kejahatan siber yang dilakukan lewat media elektronik dengan tujuan memperoleh keuntungan secara melawan hukum. Biasanya, pelaku memanfaatkan celah keamanan sistem digital atau kurangnya kewaspadaan pengguna untuk melakukan berbagai bentuk penipuan, seperti pencurian data, manipulasi informasi, atau transaksi palsu. Modus yang sering terjadi di antaranya adalah phishing akun dengan meminta data login korban, bukti transfer palsu untuk menipu penjual, *chargeback fraud* setelah item diterima. Praktik seperti ini sering terlihat pada jual beli akun atau item yang dilakukan lewat perantara tidak resmi (*third party*).

Salah satu contoh nyatanya adalah kasus penipuan jual beli akun *Mobile Legends* yang disertai peretasan email. Peristiwa ini menimpa seorang wanita berinisial SC (21) asal Bogor, yang saat itu menjual akun *Mobile Legends*-nya melalui Facebook. Pelaku menghubungi korban dan mengajaknya bergabung dalam grup “rekening bersama” (*rekber*) dengan dalih mempermudah transaksi. Korban kemudian diminta memberikan alamat email pribadinya serta membayar biaya admin sebesar Rp200.000. Tanpa curiga, korban menuruti permintaan tersebut. Namun, setelah itu akun *Mobile Legends* dan email korban justru diretas, sementara uang serta akunnya hilang. Pelaku juga memutus seluruh komunikasi dengan cara memblokir akun yang berkaitan. Beruntung, setelah melapor kepada pihak berwenang dan layanan dukungan *Mobile Legends*, korban berhasil memulihkan kembali akses ke akun dan emailnya. Kasus ini memperlihatkan kerentanan pengguna ketika melakukan transaksi melalui perantara yang tidak resmi.

Cyber fraud merupakan suatu bentuk ancaman yang serius di tengah pesatnya perkembangan teknologi modern. Para pelaku mempergunakan kecanggihan teknologi informasi dan konektivitas global untuk melakukan penipuan sekaligus merugikan masyarakat dari berbagai lapisan. Kejadian tersebut tidak sekadar merugikan secara finansial yang signifikan, namun turut menghadirkan persoalan hukum yang kompleks karena terjadi di ruang digital yang sulit diawasi (Yarfa Dzardi, 2024). *Cyber fraud* sendiri memunculkan sejumlah isu hukum yang penting untuk dikaji. Pertama, berkaitan dengan penerapan ketentuan sanksi pada pelaku *cyber fraud* pada transaksi game online, mengingat modus yang diperunakan sering kali melibatkan media digital yang sulit dilacak. Kedua, terkait perlindungan hukum bagi pengguna game online sebagai pembeli, yang biasanya pada posisi rentan ketika menjadi korban penipuan. Kedua isu hukum ini menjadi relevan untuk dibahas karena berhubungan erat dengan kepastian hukum, rasa keadilan, serta efektivitas penerapan regulasi untuk menanggulangi kriminalitas berbasis teknologi informasi.

Untuk menghadapi permasalahan tersebut, pemerintah telah menetapkan Undang-Undang Nomor 1 Tahun 2024 tentang Informasi dan Transaksi Elektronik (ITE). Undang-undang ini berfungsi sebagai landasan hukum dalam penyelenggaraan transaksi elektronik sekaligus melindungi publik atas tindak kriminal siber. Aturan di dalamnya mencakup legalitas transaksi, perlindungan data pribadi, hingga sanksi bagi pelaku tindak pidana, termasuk kasus *cyber fraud* dalam transaksi game online. Berdasarkan hal tersebut, sangat menarik jika dilakukan kajian mengenai praktik *cyber fraud* pada transaksi game online melalui perantara (*third party*) dalam perspektif UU No. 1 Tahun 2024 ITE. Kajian ini nanti diharapkan mampu memberikan gambaran mengenai perlindungan hukum bagi pengguna, serta menjadi upaya dalam mencegah dan menanggulangi kejahatan digital di era teknologi yang semakin maju..

METODE

Penelitian ini mempergunakan metode hukum normatif yang terfokus untuk pengkajian regulasi undang-undang beserta berbagai sumber hukum lain yang relevan dengan isu yang diteliti. Pendekatan normatif dipilih karena permasalahan *cyber fraud* pada transaksi game online merupakan isu hukum yang perlu dianalisis melalui norma dan aturan yang berlaku, diantaranya Undang-Undang Nomor 1 Tahun 2024 tentang ITE dan Kitab Undang – Undang Hukum Pidana (KUHP) pendekatan statute approach, juga menggunakan pendekatan konseptual dan pendekatan kasus. Melalui pemanfaatan perundang – undangan sebagai bahan hukum primer yang menjadi dasar analisis.

HASIL DAN PEMBAHASAN

1. Ketentuan pidana terhadap pelaku *cyber fraud* pada transaksi game online melalui perantara (*third party*)?

Penipuan siber dalam transaksi permainan daring termasuk dalam kategori kejahatan siber yang terkait dengan kemajuan teknologi digital dan meningkatnya ekonomi berbasis online. Fenomena

ini muncul seiring meningkatnya nilai ekonomi dari aset virtual, seperti akun, item langka, maupun mata uang digital dalam sebuah permainan. Pelaku umumnya memanfaatkan celah dari penggunaan perantara (*third party*) yang tidak resmi sebagai sarana untuk melancarkan aksi penipuan. Modus yang digunakan bervariasi, mulai dari phishing akun dengan meminta data login korban, penggelapan dana melalui rekening bersama palsu, hingga manipulasi transaksi elektronik seperti penggunaan bukti transfer fiktif atau praktik *chargeback fraud*.

Kejahatan ini menjadi semakin kompleks karena dilakukan di ruang siber yang tidak memiliki batas. Hal tersebut membuat upaya penegakan hukum tidak mudah, mengingat pembuktian tindak pidana di dunia digital sering kali menghadapi kendala, baik dari segi identifikasi pelaku, pelacakan aliran dana, maupun pembuktian elektronik di pengadilan. Di sisi lain, posisi korban, yang dalam konteks ini merupakan pemain atau konsumen game online, cenderung lemah karena tidak memiliki perlindungan yang memadai ketika bertransaksi melalui pihak ketiga yang tidak resmi.

Ketentuan pidana terhadap pelaku *cyber fraud*, khususnya pada persoalan transaksi game online yang melibatkan perantara, sangat diatur dalam beberapa undang-undang di Indonesia, terutama dalam UU ITE serta KUHP. *Cyber fraud* dalam transaksi game online sering berupa tindakan menipu ketika bertransaksi akun game di mana pelaku memanipulasi informasi elektronik guna mendapatkan untung melalui perlawanan regulasi dengan merugikan korban. Modus operasi yang umum ditemukan adalah pelaku mempergunakan identitas palsu, menjual akun game yang tidak ada, atau melakukan tindakan “hackback” setelah pembayaran dilakukan melalui perantara, sehingga korban kehilangan uang tanpa mendapatkan akun yang dijanjikan (Ashari et al., 2025).

Menurut Ashari (2025), tanggung jawab pidana bagi pelaku dalam kasus ini perlu memiliki unsur kesengajaan dan unsur kerugian yang nyata bagi korban. Pasal-pasal yang mampu dipergunakan untuk landasan konstitusi guna menjerat pelaku adalah Pasal 28 ayat (1) UU ITE yang memuat aturan larangan menyebar berita elektronik yang menyesatkan, dan Pasal 378 KUHP tentang penipuan secara umum. Selain itu, adanya unsur pemanfaatan perantara dalam transaksi digital turut memperumit kasus, namun tidak menghilangkan pertanggungjawaban pelaku karena tetap terjadi tindak penipuan elektronik yang diproses secara pidana (Ashari, 2025). Dengan demikian, pelaku bisa diancam hukuman penjara paling lama 6 tahun dan/atau denda hingga Rp1 miliar berdasarkan ketentuan UU ITE.

Penelitian oleh (Oktareza, 2024) menegaskan bahwa pihak ketiga atau perantara yang digunakan dalam transaksi online tidak serta merta bebas dari pertanggungjawaban pidana apabila terbukti membantu atau bersekongkol dengan pelaku utama dalam menjalankan penipuan. Dalam praktiknya, penyidikan biasanya memfokuskan pada bentuk-bentuk manipulasi informasi elektronik yang dilakukan pelaku, baik secara langsung maupun melalui perantara, yang menyebabkan kerugian materiil bagi korban. Raodia juga menyoroti pentingnya literasi hukum digital bagi masyarakat agar konsumen dapat lebih waspada dan mengetahui langkah perlindungan hukum yang dapat ditempuh ketika menjadi korban penipuan dalam transaksi *game online*.

Berdasar pada pendapat ahli yang disebutkan, diperoleh kesimpulan bahwasanya ketentuan pidana terhadap pelaku *cyber fraud* pada transaksi game online melalui perantara di Indonesia mengacu pada UU ITE dan KUHP, dengan fokus pada unsur kesengajaan dan kerugian yang dialami korban. Pelaku dapat dikenai proses pidana dengan ancaman hukuman yang cukup berat, dan peranan perantara juga dapat menjadi objek penegakan hukum jika terbukti berperan aktif membantu kejahatan tersebut.

UU No. 1 Tahun 2024 lahir untuk menyempurnakan kerangka hukum siber di Indonesia. Secara formal, regulasi ini adalah Perubahan Kedua atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik. Pembentukannya dilatarbelakangi oleh kebutuhan mendesak untuk menyelaraskan regulasi hukum dengan pesatnya kemajuan teknologi digital, terutama dalam konteks meningkatnya aktivitas ekonomi berbasis daring. Di samping itu, perubahan ini

turut sebagai jawaban atas berbagai persoalan hukum yang selama ini menimbulkan perdebatan dan penafsiran ganda, termasuk kritik terhadap keberadaan “pasal karet” yang sebelumnya dianggap berpotensi disalahgunakan dalam penanganan delik tertentu, seperti kasus pencemaran nama baik (Raranta et al., 2025).

Pembaruan dalam regulasi ini berfokus pada upaya penyesuaian dengan prinsip-prinsip hukum pidana umum serta peningkatan kepastian hukum dalam sistem peradilan Indonesia. Dalam konteks ekonomi digital, keberadaan UU No.1 Tahun 2024 tentang ITE menjadi sangat signifikan karena menyediakan landasan konstitusi yang kuat untuk menghadapi beragam bentuk kejahatan siber. Undang-undang ini juga menyesuaikan diri dengan kompleksitas transaksi digital masa kini, mencakup aspek perlindungan data pribadi hingga penguatan mekanisme pembuktian dalam proses peradilan.

Dalam konteks ini, *cyber fraud* bisa dipahami suatu tindak kriminal yang melibatkan penyebaran berita elektronik yang menyesatkan untuk mendapatkan keuntungan pribadi, sebagaimana yang dimuat dalam Pasal 28 ayat (1) UU ITE 2024. Meski pasal ini jadi acuan utama untuk menjerat pelaku penipuan digital, ada kaitan erat juga dengan Pasal 27 ayat (2) yang membahas soal perjudian. Dalam praktiknya, kejahatan siber semacam ini sering memanfaatkan zona abu-abu hukum, di mana transaksi aset virtual dalam game online kadang menyerupai skema investasi atau bahkan praktik perjudian terselubung. Situasi ini membuat penegak hukum sering kesulitan membedakan mana yang benar-benar penipuan, dan mana yang masuk kategori pelanggaran terkait konten perjudian terutama karena beberapa game memang punya sistem yang mirip online gambling. Karena itu, hukum siber perlu menetapkan batas yang jelas supaya penegakan hukumnya bisa tegas, tanpa menimbulkan tafsir yang membingungkan (Pradika et al., 2024).

Salah satu poin penting yang diperkuat dalam UU No.1 Tahun 2024 tentang ITE adalah penegasan soal kedudukan alat bukti elektronik. Dalam Pasal 5 ayat (1) dan (2) disebutkan secara jelas bahwa Informasi Elektronik dan Dokumen Elektronik, termasuk hasil cetak, disahkan sebagai alat pembuktian hukum yang resmi di Indonesia. Ketentuan ini memperluas jenis alat bukti yang diakui dalam sistem hukum acara pidana (KUHP), sehingga aspek pembuktian dalam kasus-kasus digital kini punya dasar hukum yang lebih kuat (*Undang-Undang Republik Indonesia Nomor 1 Tahun 2024 tentang Perubahan Kedua atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik*).

Pengakuan ini punya dampak besar dalam praktik penegakan hukum siber. Bukti digital yang dulu sering diperdebatkan keabsahannya seperti riwayat transaksi online, tangkapan layar percakapan, metadata, atau log aktivitas pengguna sekarang sudah punya posisi hukum yang lebih kuat di pengadilan. Ini jadi langkah maju karena sebelumnya, pembuktian kasus siber sering terbentur anggapan bahwa data digital mudah dimanipulasi dan sulit diverifikasi.

Selain itu, Pasal 5 UU No.1 Tahun 2024 ITE menegaskan bahwa bukti elektronik dianggap sah hanya jika dihasilkan melalui sistem elektronik yang sesuai dengan ketentuan undang-undang. Ketentuan ini penting karena menggeser fokus pembuktian, dari sekadar “ada atau tidaknya” dokumen digital, menjadi soal keandalan sistem yang memproduksi atau menyimpannya. Artinya, penegak hukum sekarang punya landasan yang lebih jelas dan kuat untuk membuktikan kejahatan siber, terutama dalam kasus *cyber fraud* yang datanya cepat berubah atau mudah hilang.

Selain penguatan dari sisi pembuktian, dalam UU No.1 Tahun 2024 tentang ITE juga mempertegas aspek otentikasi digital lewat Pasal 13A. Dalam pasal ini dijelaskan bahwa Penyelenggara Sertifikasi Elektronik (PSE) berwenang melayani mencakup tanda tangan elektronik, segel elektronik, dan identitas digital.

Kalau dikaitkan dengan transaksi game online, identitas digital yang tersertifikasi ini punya peran penting banget sebagai bentuk verifikasi. Setiap aktivitas—mulai dari login, pembelian item virtual, sampai transfer aset antar pengguna bisa dilacak dengan lebih akurat dan aman. Dengan begitu,

risiko penyalahgunaan identitas (*spoofing*) atau manipulasi data bisa ditekan, yang selama ini sering jadi celah utama dalam kasus *cyber fraud*.

Menariknya, ada hubungan langsung antara Pasal 13A dan Pasal 5 UU No.1 Tahun 2024 tentang ITE. Mekanisme sertifikasi elektronik yang meningkatkan keakuratan identitas dan transaksi otomatis juga memperkuat keabsahan alat bukti elektronik. Transaksi yang sudah terverifikasi lewat sertifikat digital punya bobot hukum yang kokoh, sehingga membantu aparat dalam membuktikan niat dan tindakan pelaku penipuan. Pada akhirnya, regulasi ini mendorong terciptanya sistem transaksi elektronik lebih terjamin keamanan dan transparansi, dan bisa dipertanggungjawabkan.

Pasal 28 ayat (1) UU No. 1 Tahun 2024 tetap menjadi landasan utama untuk menjerat pelaku *cyber fraud* yang menyebarkan informasi menyesatkan. Teks pasal tersebut berbunyi:

“Setiap orang yang dengan sengaja dan tanpa hak menyebarkan berita bohong dan menyesatkan yang mengakibatkan kerugian konsumen dalam transaksi elektronik dipidana dengan pidana penjara paling lama 6 (enam) tahun dan/atau denda paling banyak Rp1.000.000.000,00 (satu miliar rupiah).”

Kutipan pasal dan sanksi yang digunakan dalam analisis ini sudah sesuai. Perlu diperhatikan bahwa ketentuan pidana berupa hukuman penjara maksimal enam tahun dan denda hingga Rp1.000.000.000,00 tercantum dalam Pasal 45A ayat (1) Undang-Undang Nomor 1 Tahun 2024 tentang Perubahan Kedua atas Undang-Undang Nomor 11 Tahun 2008 mengenai Informasi dan Transaksi Elektronik, yang merupakan ketentuan pidana korelatif terhadap pelanggaran Pasal 28 ayat (1) (Prayoga, 2024).

Pasal tersebut memuat unsur pidana yang menuntut adanya unsur kesengajaan (*mens rea*) serta tindakan tanpa kewenangan untuk menyampaikan berita hoax atau bersifat menyesatkan (*actus reus*), yang pada akhirnya merugikan pembeli pada pelaksanaan jual beli digital.

Pasal ini punya kaitan kuat dengan praktik penipuan digital yang kerap terjadi dalam praktik global game online. Modus yang dipakai pelaku umumnya berupa manipulasi informasi elektronik misalnya memakai bukti transfer palsu untuk mengaku sudah membayar top-up, membuat akun fiktif untuk menjual aset virtual yang sebenarnya tidak ada, atau menjalankan layanan perantara ilegal demi menipu pemain lain. Semua bentuk tindakan yang disebutkan tergolong penyebaran informasi digital yang menyesatkan pada aktivitas jual beli digital (Haya et al., 2025). Dengan dasar hukum ini, pelaku yang terbukti dengan kesengajaan melakukan penipuan pengguna demi menguntungkan diri sendiri bisa dikenai sanksi pidana berat, yang diharapkan bisa menimbulkan efek jera.

UU No. 1 Tahun 2024 tentang menegaskan yang lebih rinci sekaligus memperluas tanggung jawab Penyelenggara Sistem Elektronik (PSE), baik bagi platform game resmi maupun pihak ketiga yang menjadi perantara dalam transaksi digital.

Dalam Pasal 16, PSE diwajibkan untuk menjamin keandalan serta keamanan sistem elektronik yang mereka kelola. Tanggung jawab ini mencakup aspek teknis, seperti memastikan sistem berjalan dengan stabil, terlindungi dari celah keamanan, dan tidak mudah dieksploitasi untuk tindakan kejahatan siber misalnya penyalahgunaan *bug* untuk menggandakan item (*duping*) atau pencurian akun pengguna.

Sementara itu, Pasal 16A menekankan pentingnya perlindungan terhadap konsumen. PSE harus menjaga keamanan data pribadi pengguna agar tidak bocor atau disalahgunakan, serta menyediakan mekanisme perlindungan hukum jika terjadi pelanggaran. Ketentuan ini sangat relevan dengan industri game online, mengingat banyak penggunanya berasal dari kelompok rentan seperti anak-anak, yang kerap menjadi sasaran empuk penipuan digital. Selain itu, aturan teknis mengenai pendaftaran dan tata kelola operasional PSE diatur lebih rinci dalam Peraturan

Menteri Komunikasi dan Informatika Nomor 5 Tahun 2020 (*Peraturan Menteri Komunikasi dan Informatika Republik Indonesia Nomor 5 Tahun 2020 tentang Penyelenggara Sistem Elektronik Lingkup Privat*).

Banyak kasus *cyber fraud* dalam game online melibatkan pihak perantara, seperti jasa *top-up* ilegal atau *marketplace* aset *virtual* yang tidak resmi. Dalam hal ini, UU No.1 Tahun 2024 tentang ITE menegaskan bahwa pihak ketiga yang menyediakan layanan perantara dalam transaksi digital apabila memenuhi kriteria tertentu juga tergolong sebagai PSE dan wajib mematuhi ketentuan yang tercantum dalam Pasal 16 dan Pasal 16A.

Konsep kelalaian dan keterlibatan langsung menjadi hal yang krusial pada topik ini. Kewajiban PSE tidak semata-mata terbatas pada pengelolaan sistem internalnya, namun juga mencakup kewajiban untuk mencegah sistem tersebut dimanfaatkan sebagai sarana tindak kejahatan siber. Jika PSE utama terbukti lalai dalam menerapkan standar keamanan yang memadai, atau tidak mengambil tindakan terhadap aktivitas ilegal di platformnya seperti penyebaran tautan phishing atau penipuan digital maka mereka tetap dapat dimintai pertanggungjawaban.

Dalam situasi di mana kelalaian tersebut dapat dibuktikan, pertanggungjawaban hukum dapat dituntut baik secara perdata maupun pidana, mengacu pada asas penyertaan dalam tindak pidana. Ketentuan ini pada akhirnya menjadi dorongan bagi setiap PSE untuk lebih serius berinvestasi dalam keamanan sistem serta memastikan kepatuhan terhadap regulasi yang berlaku.

Untuk menjamin kepatuhan PSE terhadap Pasal 16A, UU No. 1 Tahun 2024 tentang Perubahan Kedua atas UU No. 11 Tahun 2008 tentang ITE menambahkan Pasal 16B yang memuat ketentuan terkait sanksi administratif. Jika PSE melanggar kewajiban yang telah ditetapkan, maka dapat disanksi dengan peringatan tertulis, sanksi denda administratif, dan penangguhan sementara layanan, atau bahkan pemutusan akses.

Sanksi administratif ini punya dua peran penting. Pertama, berfungsi sebagai langkah pencegahan dini (*deterrent*) yang bisa diterapkan tanpa perlu melalui proses pidana yang panjang, sehingga mendorong PSE untuk segera memperbaiki sistemnya. Kedua, ancaman sanksi paling berat berupa pemutusan akses menjadi dorongan kuat bagi PSE termasuk yang beroperasi di luar negeri agar mematuhi aturan terkait keamanan dan perlindungan konsumen di Indonesia [\(Puspitalova, 2025\)](#). Aturan lanjut yang memuat terkait penerapan sanksi administratif ini akan dicantumkan melalui Peraturan Pemerintah, yang berarti pelaksanaannya secara detail masih menunggu pengaturan pada tingkat peraturan turunan.

Dengan diberlakukannya UU No. 1 Tahun 2024 tentang Perubahan Kedua atas UU No. 11 Tahun 2008 tentang ITE, aparat penegak hukum kini terdapat landasan konstitusi lebih kokoh dan legitimasi yang lebih jelas dalam menangani kasus *cyber fraud*. Penguatan tersebut membantu aparat hukum menelusuri jejak digital pelaku dengan lebih akurat, terutama karena prosesnya kini didukung oleh sistem otentikasi identitas digital sebagaimana diatur dalam Pasal 13A.

Meski kerangka hukumnya sudah semakin kuat, persoalan pembuktian masih jadi tantangan utama, terutama dalam hal klasifikasi aktivitas digital. Salah satu masalah besar dalam penegakan hukum siber adalah bagaimana membedakan dengan jelas antara *game online* legal yang mungkin rawan penipuan dan dapat dijerat lewat Pasal 28 dengan *game* yang mengandung unsur perjudian atau menyerupai praktik judi daring, yang termasuk pelanggaran Pasal 27 ayat (2) UU No. 1 Tahun 2024 tentang Perubahan Kedua atas UU No. 11 Tahun 2008 tentang ITE.

Karena beberapa *game online* yang melibatkan transaksi finansial memiliki sistem yang menyerupai perjudian, diperlukan batas definisi yang sangat jelas dari pemerintah untuk menghindari ambiguitas penegakan hukum. Tanpa demarkasi yang jelas, penegak hukum kesulitan menerapkan sanksi pidana secara konsisten dan tepat.

Selain itu, dalam kasus penipuan yang melibatkan pihak perantara, proses penegakan hukum perlu benar-benar hati-hati dalam membuktikan adanya penyertaan pidana. Penting untuk dipastikan apakah pihak perantara atau bahkan platform utamanya berperan sebagai pelaku utama penipuan, hanya menyediakan sarana yang digunakan untuk tindak ilegal, atau justru terlibat karena kelalaian sistem yang serius. Kompleksitas pembuktian semacam ini menuntut kemampuan forensik digital yang kuat serta pemahaman hukum yang mendalam mengenai tanggung jawab korporasi di ranah siber.

Konsep Tindak Pidana *Cyber Fraud* pada Transaksi Game Online

Tindak pidana *cyber fraud* dalam transaksi game online ialah suatu wujud kejahatan siber (*cyber crime*) yang memanfaatkan sistem elektronik atau jaringan internet untuk melakukan tindakan penipuan dengan tujuan memperoleh keuntungan finansial secara melawan hukum. Modus ini umumnya terjadi melalui praktik *Real Money Trading* (RMT), yaitu transaksi yang melibatkan pertukaran aset virtual seperti item, mata uang dalam game, atau akun game dengan uang nyata (Safitri et al., n.d.). Kejahatan tersebut dipandang sebagai ancaman serius dan termasuk dalam kategori *online business crime*.

1. Modus Operandi Utama (*Modus Operandi Typology*)

Kejahatan penipuan dalam sektor game online memiliki tipologi *modus operandi* yang terencana, dengan memanfaatkan kelecmanan pada aspek kepercayaan serta rendahnya tingkat literasi digital para korbannya:

A. Penipuan Jual Beli Akun (*Account Selling Fraud*)

Modus ini berlangsung ketika pelaku menawarkan penjualan akun game misalnya akun *Valorant* dan menerima pembayaran dari pembeli. Setelah transaksi diselesaikan dan dana diterima, pelaku memanfaatkan data pemulihan akun yang masih dikuasainya untuk mengambil kembali akun tersebut (*reclaiming fraud*). Akibatnya, pembeli mengalami kerugian ganda karena kehilangan uang sekaligus akun yang telah dibeli. Tindakan ini memenuhi unsur penipuan konvensional karena mengandung unsur tipu muslihat dalam proses transaksi (Herrenauw et al., 2022).

B. *Top-Up* Ilegal dan Penipuan Pihak Ketiga

Pelaku menawarkan layanan *top-up* mata uang atau item virtual dengan harga yang jauh di bawah standar resmi, yang termasuk dalam bentuk penyebaran informasi menyesatkan. Setelah korban melakukan transfer dana, barang atau layanan yang dijanjikan tidak pernah disampaikan. Selain itu, sejumlah situs pihak ketiga ilegal sering meminta korban untuk memasukkan nama pengguna dan kata sandi akun mereka sebagai syarat proses *top-up*, yang pada akhirnya mengarah pada praktik *phishing* atau pencurian data akun. Aksi ini bisa dikualifikasikan sebagai ketidakpatuhan pada ketentuan akses ilegal seperti yang dicantumkan dalam UU ITE (Haya et al., 2025).

C. Teknik Rekayasa Sosial (*Social Engineering*)

Pelaku penipuan memanfaatkan manipulasi psikologis serta strategi retorik untuk mempercepat proses transfer dana oleh korban (Juanda, 2023). Dalam praktiknya, mereka sering menggunakan identitas palsu, membuat iklan fiktif, atau menawarkan harga yang tidak wajar sebagai upaya menarik perhatian dan membangun kepercayaan korban. Kajian komunikasi menunjukkan bahwa pola interaksi tersebut didominasi oleh tindak tutur direktif seperti perintah atau desakan yang bertujuan mengendalikan perilaku korban.

2. Status Hukum Aset Virtual sebagai Objek Pidana

Dalam konteks penegakan hukum, permasalahan utama terletak pada penetapan status hukum terhadap aset virtual seperti item, mata uang, atau akun game yang menjadi objek penipuan.

Meskipun tidak memiliki wujud fisik, kajian hukum menegaskan bahwa aset virtual dapat diperlakukan layaknya barang (*goods*) karena memiliki nilai ekonomi yang dapat diukur.

Pengakuan terhadap status tersebut menjadi krusial, mengingat aksi pelanggaran hukum dengan menipu diharuskan memadai unsur “kerugian konsumen.” Dengan ditetapkannya aset virtual sebagai objek bernilai ekonomi, kerugian finansial yang dialami korban dapat dihitung secara konkret, yang selanjutnya menjadi dasar yuridis untuk menjerat pelaku berdasarkan Pasal 28 Ayat (1) UU ITE (Direktorat Jenderal Kekayaan Negara (DJKN), Kementerian Keuangan. Ketentuan terkait Penipuan. (Artikel resmi yang menjelaskan komparasi Pasal 492 UU 1/2023 dan Pasal 28 Ayat (1) UU ITE).

A. Perlindungan Hukum Korban *Cyber Fraud*: Komparasi UU No. 1 Tahun 2024 ITE dengan Regulasi Singapura

UU No. 1 Tahun 2024 ITE hadir guna pembaruan dari aturan terdahulu dengan tujuan memperkuat jaminan hukum masyarakat di era digital, khususnya dalam menghadapi kejahatan siber seperti *cyber fraud*. Revisi ini menegaskan kembali komitmen pemerintah untuk membangun ruang digital yang pasti akan keamanan, etis, dan terbebas dari penyalahgunaan teknologi informasi. Salah satu ketentuan penting dalam perundangan ini tercantum pada Pasal 28, yang memuat aturan melarang menyebarkan berita dan menyesatkan yang bisa menjadikan kerugian oleh pembeli, yang mana diancam pidana penjara hingga enam tahun dan denda sebesar Rp1 miliar. Ketentuan tersebut diharapkan mampu menekan angka kejahatan daring yang kian meningkat, terutama penipuan berbasis media sosial dan transaksi elektronik. Namun, efektivitas penerapannya masih menghadapi sejumlah kendala. Menurut Bastian (2025), “UU ITE bertujuan memperkuat mekanisme penegakan hukum terhadap kejahatan berbasis digital, tetapi pelaksanaannya menemui tantangan, salah satunya terkait tumpang tindih kewenangan dan kurangnya literasi digital masyarakat”. Pernyataan ini menggambarkan bahwa meskipun regulasi sudah diperkuat, tantangan nyata masih terletak pada kapasitas institusi penegak hukum dan tingkat kesadaran masyarakat terhadap ancaman dunia digital.

Selain aspek pidana, UU ITE juga memberikan tanggung jawab besar kepada PSE untuk memastikan keamanan sistem, menjaga privasi pengguna, serta menyediakan jaminan hukum bagi kelompok rentan, misalnya anak-anak dan remaja. Kondisi tersebut mengindikasikan bahwasanya regulasi ini tidak sekadar bersifat represif, namun juga preventif, dengan mendorong peran aktif pelaku industri digital dalam membangun lingkungan daring yang pasti akan keamanan dan pertanggung jawabannya. Perlindungan hukum yang diatur tidak hanya mencakup sanksi terhadap pelaku, tetapi juga penegakan hak-hak korban melalui mekanisme hukum pidana maupun perdata. Pendekatan ini menandai dinamika paradigma dari sekadar penegakan hukum menuju pembangunan ekosistem digital yang beretika dan berorientasi pada hak asasi manusia.

Jika dibandingkan dengan Singapura, pendekatan hukum Indonesia masih cenderung berbasis pelaporan dan penindakan setelah terjadi pelanggaran. Di Singapura, regulasi mengenai kejahatan siber diatur melalui *Cybersecurity Act* dan *Online Criminal Harms Act (OCHA)* yang diberlakukan sejak tahun 2023. Kedua regulasi ini tidak hanya menitikberatkan pada penindakan, namun turut mengedepankan langkah-langkah pencegahan melalui kerja sama erat antara pemerintah, lembaga keamanan digital, dan penyedia layanan daring. Otoritas Singapura diberi kewenangan untuk melakukan tindakan proaktif seperti pemblokiran situs, penghapusan tautan penipuan, dan penghentian akses ke akun yang dicurigai melakukan aktivitas ilegal bahkan sebelum adanya laporan korban. Menurut penelitian Rencana (2025), “Singapura menerapkan pendekatan preventif dengan kerjasama ketat antara pemerintah dan penyedia layanan digital, sehingga mampu melakukan tindakan cepat terhadap ancaman *cyber fraud*.” Pendekatan yang lebih adaptif dan responsif ini menyatakan bagaimana kebijakan hukum mampu disinergikan dengan teknologi untuk menyediakan perlindungan yang lebih kuat bagi masyarakat.

Selain itu, infrastruktur hukum di Singapura mendukung mekanisme pengawasan aktif dengan mewajibkan platform digital untuk melakukan deteksi dini terhadap aktivitas mencurigakan, melaporkan ancaman kepada otoritas, dan menerapkan sistem keamanan tingkat tinggi seperti otentikasi digital dan enkripsi data. Regulasi ini mencerminkan kesadaran bahwa keamanan siber bukan hanya tanggung jawab pemerintah, melainkan juga bagian dari tata kelola teknologi yang harus dijalankan oleh seluruh pelaku ekosistem digital.

Perbandingan antara kedua negara menunjukkan adanya perbedaan signifikan dalam orientasi kebijakan dan implementasi hukum. Indonesia lebih menekankan pada aspek penegakan hukum dan pemberian sanksi setelah tindak pidana terjadi, sementara Singapura menitikberatkan pada pencegahan, deteksi dini, dan intervensi cepat melalui kolaborasi lintas sektor. Dalam konteks perlindungan korban, Indonesia berfokus pada pemberian sanksi dan penguatan sistem keamanan, sedangkan Singapura melibatkan upaya pencegahan dengan penghapusan konten berbahaya dan penerapan sistem keamanan teknis secara real time. Peran penyedia layanan digital pun berbeda; di Indonesia mereka diwajibkan mendukung keamanan sistem, sedangkan di Singapura mereka memiliki tanggung jawab aktif untuk mendeteksi dan memblokir aktivitas penipuan.

Melalui perbandingan itu, dapat disimpulkan bahwa pendekatan hukum di Indonesia masih memerlukan penguatan dalam aspek koordinasi lintas lembaga, peningkatan literasi digital masyarakat, dan penerapan sistem pengawasan siber berbasis teknologi yang lebih responsif. Indonesia dapat mengambil pelajaran dari model Singapura yang berhasil memadukan regulasi hukum dengan inovasi teknologi serta membangun hubungan kerja sama yang terpadu antara pemerintah dan kalangan swasta. Melalui kombinasi pendekatan preventif, penerapan hukum yang tegas serta pengembangan kesadaran masyarakat publik, diharapkan penjaminan hukum terhadap tindak kriminal siber di Indonesia dapat lebih optimal dan adaptif terhadap perkembangan dunia digital yang semakin kompleks.

2. Perlindungan Hukum Pengguna *Game Online* terhadap Fenomena *Cyber Fraud*

Kemajuan teknologi digital telah menghasilkan transformasi signifikan dalam pola komunikasi dan kegiatan transaksi masyarakat. Salah satu dampak dari kemajuan tersebut adalah meningkatnya aktivitas ekonomi di ranah digital, termasuk dalam ekosistem game online. Transaksi yang melibatkan aset virtual seperti item, mata uang digital dalam game, maupun akun telah melahirkan bentuk ekonomi baru yang dikenal sebagai *virtual economy*.¹ Akan tetapi, sisi lain peluang ekonomi tersebut, disertai kemunculan risiko serius berbentuk tindak kriminalitas *cyber fraud* yang memanfaatkan celah hukum serta rendahnya kesadaran hukum para pengguna.

Kejahatan *cyber fraud* dalam konteks game online umumnya dilakukan melalui modus *Real Money Trading* (RMT), yaitu transaksi antar pemain dengan menggunakan uang nyata untuk memperoleh item atau akun virtual. Salah satu bentuk yang paling sering terjadi adalah *reclaiming fraud*, di mana pelaku menjual akun kepada korban, namun setelah pembayaran diterima, pelaku mengambil kembali akun tersebut dengan memanfaatkan data pemulihan yang masih dikuasainya. Imbasnya, korban harus menanggung kerugian ganda berupa hilangnya uang dan akun yang telah dibeli. Fenomena semacam ini umumnya terjadi melalui berbagai platform digital, seperti media sosial, forum komunitas, maupun *marketplace* yang tidak memiliki sistem pengawasan yang memadai (Rizky, 2023).

Urgensi Perlindungan Hukum bagi Pengguna *Game Online*

Perlindungan hukum bagi pengguna game online menjadi suatu kebutuhan yang mendesak, mengingat aktivitas dalam game kini memiliki dampak ekonomi yang nyata. Aset virtual dikategorikan sebagai aset tidak berwujud (*intangible assets*) yang memiliki nilai tukar serta dapat dijadikan objek transaksi (Sebakas & Santoso, 2024). Oleh karena itu, ketika terjadi tindak

penipuan, kerugian yang dialami pengguna bersifat konkret dan terukur. Namun demikian, kerangka hukum di Indonesia masih menghadapi kendala, karena aset virtual belum secara tegas diakui atau diatur sebagai “barang” dalam sistem hukum pidana konvensional.

Dalam perspektif hukum positif, jaminan hukum terhadap pengguna game online dapat merujuk pada UU No. 1 Tahun 2024 tentang ITE, yang berperan sebagai *lex specialis* terhadap KUHP. Tindak penipuan yang terjadi di ranah digital dapat dikenai sanksi berdasarkan Pasal 28 ayat (1) UU ITE 2024, yang melarang penyebaran informasi palsu atau menyesatkan yang menimbulkan kerugian bagi konsumen dalam transaksi elektronik (Zahra et al., n.d.). Ancaman pidana bagi pelaku diatur dalam Pasal 45A ayat (1) UU ITE 2024, berupa hukuman penjara paling lama enam tahun dan/atau denda maksimal sebesar Rp1 miliar. Selain itu, Pasal 378 KUHP tentang penipuan juga dapat diterapkan secara kumulatif sebagai *lex generalis* apabila unsur-unsur tindak pidana konvensional terpenuhi. Dengan demikian, secara substansial, Indonesia telah memiliki landasan hukum yang memadai untuk menjerat pelaku *cyber fraud*, meskipun dalam praktiknya masih terdapat berbagai kendala teknis dan hambatan dalam pembuktian (Afinda Wahyu Nur Sholikhah; Hanifah Febriani S.H., 2021).

Bentuk Perlindungan Hukum: Preventif dan Represif

a. Perlindungan Preventif

Perlindungan hukum preventif bertujuan untuk mencegah terjadinya tindak kejahatan sejak tahap awal. Dalam konteks ini, tanggung jawab tidak hanya berada pada pengguna, tetapi juga pada pengembang game (*developer*) serta pemerintah. Pengembang game, selaku Penyelenggara Sistem Elektronik (PSE), berdasarkan ketentuan Pasal 16A Undang-Undang Nomor 1 Tahun 2024 tentang Informasi dan Transaksi Elektronik (UU ITE 2024), memiliki kewajiban untuk memberikan perlindungan kepada pengguna, antara lain melalui peningkatan keamanan sistem akun dan penyediaan fitur pemulihan yang aman.

Selain itu, diperlukan upaya edukasi digital kepada masyarakat agar memiliki pemahaman yang lebih baik mengenai risiko transaksi di luar platform resmi. Pemerintah pun berperan penting dalam memperkuat regulasi yang mengatur status hukum aset virtual serta memastikan efektivitas pelaksanaan penegakan hukum di ranah digital.

b. Perlindungan Represif

Perlindungan hukum represif merupakan langkah yang ditempuh setelah terjadinya tindak kejahatan, dengan tujuan memberikan efek jera bagi pelaku serta pemulihan hak bagi korban. Korban dapat mengajukan laporan kepada aparat penegak hukum dengan berlandaskan pada ketentuan yang terdapat dalam Undang-Undang Nomor 1 Tahun 2024 tentang Informasi dan Transaksi Elektronik (UU ITE 2024) maupun Kitab Undang-Undang Hukum Pidana (KUHP). Namun, tantangan utama dalam proses penegakan hukum terletak pada aspek pembuktian, khususnya dalam membuktikan unsur kesengajaan atau *mens rea* serta keabsahan bukti digital yang diajukan (Rizky, 2023).

Keberhasilan proses penuntutan sangat ditentukan oleh kualitas dan validitas bukti digital. Oleh karena itu, peningkatan kapasitas aparat penegak hukum terutama pada unit khusus kejahatan siber menjadi hal yang krusial. Selain itu, bukti elektronik perlu diperkuat dengan keterangan ahli digital forensik agar dapat diakui sebagai alat bukti yang sah dalam proses persidangan (Gymnastiar et al., 2024).

SIMPULAN DAN SARAN

Kejahatan *cyber fraud* dalam transaksi game online melalui pihak ketiga (*third party*) merupakan salah satu bentuk kejahatan siber yang berkembang seiring meningkatnya aktivitas ekonomi digital di sektor hiburan daring. Modus yang dilakukan pelaku, seperti *phishing*, *reclaiming fraud*, hingga penggunaan perantara palsu, menunjukkan bahwa ruang digital masih memiliki celah besar terhadap praktik manipulasi dan penyalahgunaan data pengguna. Secara hukum, tindakan tersebut dapat dikategorikan sebagai penyebaran informasi elektronik yang menyesatkan sebagaimana diatur dalam Pasal 28 ayat (1) Undang-Undang Nomor 1 Tahun 2024 tentang Informasi dan Transaksi Elektronik (ITE), dengan ancaman pidana paling lama enam tahun penjara dan/atau denda paling banyak Rp1 miliar sesuai dengan Pasal 45A ayat (1).

Undang-undang tersebut menjadi dasar penting bagi pemberian perlindungan hukum terhadap pengguna game online, sekaligus memperkuat kapasitas aparat penegak hukum dalam menangani kejahatan siber. Pembaruan dalam UU ITE 2024, seperti pengakuan terhadap alat bukti elektronik (Pasal 5), pengaturan mengenai otentikasi digital dan sertifikasi elektronik (Pasal 13A), serta kewajiban Penyelenggara Sistem Elektronik (PSE) untuk menjamin keamanan sistem dan melindungi konsumen (Pasal 16, 16A, dan 16B), menunjukkan peningkatan perhatian negara terhadap keamanan dan akuntabilitas dalam aktivitas digital. Jika dibandingkan dengan regulasi di Singapura yang menitikberatkan pada deteksi dini, intervensi cepat, serta kerja sama lintas sektor, sistem hukum di Indonesia masih lebih berorientasi pada penindakan setelah pelanggaran terjadi. Oleh karena itu, diperlukan sinkronisasi kebijakan, pembaruan sistem pengawasan berbasis teknologi, serta peningkatan kapasitas forensik digital agar penegakan hukum terhadap kejahatan siber menjadi lebih efektif, adaptif, dan responsif terhadap perkembangan teknologi.

Dengan demikian, penerapan Undang-Undang Nomor 1 Tahun 2024 tentang Informasi dan Transaksi Elektronik merupakan langkah progresif dalam memperkuat landasan hukum siber di Indonesia. Namun, efektivitasnya sangat bergantung pada sinergi antara aparat penegak hukum, penyelenggara sistem digital, dan masyarakat pengguna sebagai bagian dari ekosistem game online yang semakin kompleks dan dinamis.

DAFTAR RUJUKAN

- Afinda Wahyu Nur Sholikhah; Hanifah Febriani S.H., L. L. . (2021). *Perlindungan Hukum Terhadap Korban Tindak Pidana Penipuan Di Sosial Media*. 167–186.
- Ashari, F. M., Parmono, B., & Hidayati, R. (2025). *Perlindungan Hukum Terhadap Pembeli Dalam Penipuan Transaksi Jual Beli Akun Game Melalui Media Sosial*. 193, 13328–13343.
- Bastian, M. (2025). Evaluasi Efektivitas Undang-Undang No. 1 Tahun 2024 Tentang Ite. *Jurnal Hukum Dan Masyarakat*, 25 (1), 15–29.
- Gymnastiar, I. R., Rahman, M. K., & Alauddin, M. R. F. (2024). *Interdisciplinary Explorations In Research Analisis Efektifitas Undang-Undang Nomor 1 Tahun 2024 Di Pasal 27 Mengenai Judi Online Di Kota*. 2(1), 694–703.
- Haya, F., Susetio, W., Rizka, A., Azis, H., Saragih, A., Bertha, J., Arjuna, U. N., & Jeruk, K. (2025). *Perlindungan Konsumen Terhadap Pelanggaran Dalam Transaksi Top-Up Game Online*. 22(1).
- Herrenauw, J. M., Alfaramona, J., Titahelu, S., & Saimima, J. M. (2022). *Kajian Hukum Pidana Dalam Penipuan Jual Beli Akun Permainan Online Melalui Media Sosial Teknologi Yang Sangat Membantu Dan Memudahkan Dalam Memenuhi Kebutuhan Sehari-hari*. 2(3), 252–261.

- Juanda, M. R. (2023). *Analisis Penipuan Transaksi Daring : Studi Kasus Penjualan Akun Game Online (Gim Daring)* [Universitas Pendidikan Indonesia Bandung]. [Http://Repository.Upi.Edu/101654/](http://Repository.Upi.Edu/101654/)
- Nomor, U. R. I., Kedua, P., Nomor, U., Elektronik, T., & Statistik, B. P. (2024). *No Title*. 2022, 1–19.
- Oktareza, M. I. (2024). *Aspek Tindak Pidana Dalam Kasus Penipuan Jual Beli Akun Game Online Valorant Berdasarkan Undang-Undang Nomor 1 Tahun 2024 Tentang Ite*.
- Pradika, M. F., Taufik, L., Hidayat, T., Habib, A., Prakoso, D., & Khan, A. A. (2024). Implementation Of Violations Of The Ite Law Article 27 Verse (2) Of 2016 Concerning Promotion Of Online Gambling By Influencers In Indonesia. *Jurnal Komunikasi Indonesia*, 13(2). <https://doi.org/10.7454/Jkmi.V13i2.1227>
- Prayoga, A. (2024). *Sanksi Tindak Pidana Penipuan Transaksi Elektronik Dalam Pasal 28 Ayat (1) Undang-Undang Informasi Dan Transaksi Elektronik Perspektif Hukum Pidana Islam*. Uin Sunan Gunung Djati Bandung.
- Puspitalova, A. T. (2025). *Terancam Sanksi, Ini Poin Poin Aturan Komdigi Tentang Pse Privat*. Tempo.
- Raranta, E. A., Mamengko, R. S., & Karamoy, R. V. (2025). *Jurnal Fakultas Hukum Unsrat Lex Privatum Vol.14 N0 5 Jan 2025*. 14.
- Rencana, S. (2025). Eranan Regulasi Cybersecurity Act Dan Online Criminal Harms Act Di Singapura. *Journal Of Cybersecurity Polic*, 8 (2), 101–115.
- Rizky, M. (2023). Legal Protection For Victims Of Cyber Crime Hacking Through Online Games According To Indonesian Regulations. *Recidive : Jurnal Hukum Pidana Dan Penanggulangan Kejahatan*, 12(1), 120. <https://doi.org/10.20961/Recidive.V12i1.69292>
- Safitri, N. E., B, M. T. M., & Phahlevy, R. R. (N.D.). *Virtual Objects Trading In Indonesia : Legal* (Vol. 1). Atlantis Press Sarl. <https://doi.org/10.2991/978-2-38476-052-7>
- Sebakas, K., & Santoso, B. (2024). Analisa Yuridis Keabsahan Jual Beli Akun Permainan Daring Secara Backdoor Antara Para Gamers (Pemain Daring). *Notarius*, 17(2), 695–710.
- Yarfa Dzardi. (2024). Analisis Cyber Fraud Pada Platform Jual Beli Game Online. *Doktrin: Jurnal Dunia Ilmu Hukum Dan Politik*, 2(2), 57–76. <https://doi.org/10.59581/doktrin.v2i2.2546>
- Yunior. (2025). *Perlindungan Hukum Terhadap Korban Penipuan Transaksi Penjualan Akun Game Online*. 1–15. <http://repository.unars.ac.id/id/eprint/3273%0A>
- Zahra, A. M., Pawennai, M., & Tjolleng, A. (n.d.). *Legal Dialogica Akibat Hukum Bagi Pelaku Tindak Pidana Penipuan Online di Media Sosial Elektronik dan semakin canggih . Tidak hanya penipuan saja yang variatif, berbagai macam*. 1(1), 1–17.