



Kualifikasi Tindak Pidana terhadap Penggunaan Identitas Orang Lain dalam Transaksi *Paylater* oleh Anak di Bawah Umur

Aryn Nabel Budiono¹, Dewi Muti'ah^{2*}, Yusaq Djunarto³

¹⁻² Fakultas Hukum, Program Studi Ilmu Hukum, Universitas Trunodjoyo Madura, Indonesia

³ Seksi Intelijen, Kejaksaan Negeri Kota Mojokerto, Indonesia

*Penulis Korespondensi: dewi.muti'ah@trunodjoyo.ac.id

Abstract. *The rapid development of Buy Now Pay Later (PayLater) services has facilitated access to digital financing while simultaneously increasing the misuse of other people's identities by minors to obtain credit facilities. Such conduct raises legal issues regarding the proper criminal qualification, as it involves unauthorized use of personal data, manipulation of electronic information, identity forgery, and fraud. This study aims to analyze the criminal qualification of using another person's identity in PayLater transactions committed by minors under Indonesian criminal law. This research employs a normative legal method using statutory and conceptual approaches. Legal materials were analyzed qualitatively using a prescriptive method. The findings reveal that the unauthorized use of another person's identity in PayLater transactions is more appropriately classified as the criminal offense of fraud because the perpetrator intentionally uses another person's identity from the outset to unlawfully obtain credit facilities through deceitful conduct. Violations of the Personal Data Protection Law, the Electronic Information and Transactions Law, and the provisions on forgery under the Indonesian Criminal Code constitute accompanying offenses that reinforce the legal construction of fraud in PayLater transactions. Therefore, determining the appropriate criminal qualification requires a comprehensive approach that considers the characteristics of digital crime and the interrelationship among relevant legal regulations*

Keywords: Criminal Qualification; Fraud; Identity Misuse; Minors; Paylater.

Abstrak. Perkembangan layanan Buy Now Pay Later (PayLater) telah memberikan kemudahan akses pembiayaan digital, namun di sisi lain memunculkan penyalahgunaan identitas oleh anak di bawah umur untuk memperoleh fasilitas kredit menggunakan data pribadi milik orang lain. Perbuatan tersebut menimbulkan persoalan mengenai kualifikasi tindak pidana yang tepat karena berkaitan dengan penyalahgunaan data pribadi, manipulasi informasi elektronik, pemalsuan identitas, dan penipuan. Penelitian ini bertujuan untuk menganalisis kualifikasi tindak pidana terhadap penggunaan identitas orang lain dalam transaksi PayLater yang dilakukan oleh anak di bawah umur berdasarkan hukum pidana di Indonesia. Penelitian ini merupakan penelitian hukum normatif dengan menggunakan pendekatan perundang-undangan dan pendekatan konseptual. Bahan hukum dianalisis secara kualitatif melalui metode preskriptif. Hasil penelitian menunjukkan bahwa penggunaan identitas orang lain dalam transaksi PayLater lebih tepat dikualifikasikan sebagai tindak pidana penipuan karena sejak awal pelaku menggunakan identitas pihak lain untuk memperoleh fasilitas pembiayaan secara melawan hukum melalui rangkaian tipu muslihat. Adapun penyalahgunaan data pribadi sebagaimana diatur dalam Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi, manipulasi informasi elektronik dalam Undang-Undang Informasi dan Transaksi Elektronik, serta pemalsuan sebagaimana diatur dalam Kitab Undang-Undang Hukum Pidana merupakan tindak pidana yang menyertai dan memperkuat konstruksi penipuan dalam transaksi PayLater. Oleh karena itu, penentuan kualifikasi tindak pidana harus dilakukan secara komprehensif dengan memperhatikan karakteristik kejahatan digital dan keterkaitan antarperaturan perundang-undangan.

Kata Kunci: Anak di Bawah Umur; Kualifikasi Kriminal; Pembayaran Terlambat; Penipuan; Penyalahgunaan Identitas.

1. LATAR BELAKANG

Teknologi dan internet memiliki peran yang begitu besar dalam menunjang segala aktivitas kehidupan manusia sehingga berdampak bagi beberapa sektor, seperti pada sektor bisnis atau industri bisnis yang kemudian perkembangan dalam industri perdagangan dan industri keuangan di Indonesia (Putri & Miru, 2020). Seiring dengan perkembangan teknologi telah memunculkan berbagai inovasi digital, salah satu bentuk inovasi tersebut

adalah inovasi pada industri keuangan yaitu inovasi yang berupa *financial technology* yang selanjutnya disebut dengan *fintech* (Panjalu, 2022).

Data OJK menunjukkan pengguna *PayLater* di Indonesia melonjak drastis, dengan jumlah kontrak mencapai 79,92 juta pada 2023 dan total utang BNPL (*Buy Now Pay Later*) perbankan mencapai Rp24,33 triliun per Agustus 2025, tumbuh 32,35% *year on year* (2025). Dalam mendukung pengembangan dan pengawasan *fintech*, Undang-Undang No. 4 Tahun 2023 tentang Pengembangan dan Penguatan Sektor Keuangan (P2SK) menjadi instrumen utama. Undang-Undang ini memberikan landasan hukum yang jelas untuk regulasi *fintech*, mencakup berbagai aspek dari operasional hingga perlindungan konsumen. UU P2SK bertujuan untuk menyesuaikan regulasi keuangan dengan perkembangan pesat di dunia teknologi finansial (Prasanti & Munandar, 2024).

Kemudahan verifikasi, akses cepat, dan promosi layanan masif menyebabkan ini digunakan oleh berbagai kelompok usia, termasuk anak-anak di bawah umur. Kondisi tersebut menimbulkan kerentanan, terutama ketika anak mengakses layanan *PayLater* melalui identitas pihak ketiga, misalnya menggunakan KTP orang tua, kerabat, atau bahkan identitas orang lain tanpa izin. Penggunaan data identitas tanpa hak untuk memperoleh fasilitas kredit digital telah diidentifikasi sebagai salah satu bentuk pelanggaran yang berpotensi menimbulkan pertanggungjawaban pidana.

Dalam konteks kejahatan digital, penggunaan identitas orang lain tanpa izin termasuk ke dalam bentuk pencurian atau pemalsuan identitas yang dapat dipidana berdasarkan ketentuan hukum positif di Indonesia. Menjelaskan bahwa tindak pidana pencurian identitas kini semakin berkembang seiring kemudahan teknologi, sehingga penggunaan data pribadi oleh bukan pemiliknya dapat memenuhi unsur perbuatan melawan hukum.

Kasus penyalahgunaan layanan *PayLater* oleh anak di bawah umur melalui identitas orang lain dapat ditemukan dalam penelitian Alida Saidah yang membahas transaksi Shopee *PayLater* oleh anak di bawah umur. Dalam kasus tersebut, anak yang belum memenuhi syarat usia secara hukum menggunakan akun Shopee milik orang tuanya yang telah terverifikasi untuk mengaktifkan layanan Shopee *PayLater* dan melakukan transaksi pembelian secara kredit. Tindakan tersebut menimbulkan tagihan cicilan yang secara hukum dibebankan kepada pemilik identitas, meskipun transaksi dilakukan oleh anak yang tidak memiliki kecakapan hukum. Perbuatan ini tidak hanya menimbulkan persoalan keabsahan perjanjian, tetapi juga berpotensi mengandung unsur tindak pidana dalam ruang digital berupa penyalahgunaan identitas dan data pribadi. (Sa'idah, 2024)

Pengaturan mengenai perlindungan data pribadi dalam sistem elektronik telah mendapatkan perhatian melalui Undang-Undang Perlindungan Data Pribadi yang memberikan perlindungan terhadap penggunaan data pribadi tanpa hak. Di sisi lain, Undang-Undang Informasi dan Transaksi Elektronik juga memberikan dasar hukum terhadap berbagai bentuk manipulasi dan penyalahgunaan informasi elektronik yang dilakukan secara melawan hukum. Meskipun berbagai ketentuan tersebut telah tersedia, penggunaan identitas orang lain dalam transaksi Paylater oleh anak di bawah umur masih menyisakan persoalan hukum yang belum sepenuhnya terjawab dalam praktik penegakan hukum.

Persoalan pertama berkaitan dengan kualifikasi tindak pidana yang paling tepat untuk diterapkan terhadap penggunaan identitas orang lain transaksi Paylater oleh anak di bawah umur. Perbuatan tersebut dapat dikualifikasikan sebagai tindak pidana penipuan apabila penggunaan identitas dilakukan untuk memperoleh fasilitas kredit digital melalui rangkaian perbuatan yang menyesatkan penyelenggaraan layanan. Namun demikian, penggunaan identitas orang lain tanpa hak juga dapat dikualifikasikan sebagai bentuk pemalsuan identitas atau penyalahgunaan data pribadi. keberagaman kemungkinan kualifikasi delik tersebut menunjukkan adanya problematika normative dalam menentukan konstruksi hukum pidana yang paling tepat terhadap perbuatan yang dilakukan oleh anak.

Dalam perkembangannya, Undang-Undang Informasi dan Transaksi Elektronik telah memberikan kewajiban kepada penyelenggara sistem elektronik untuk menyediakan mekanisme perlindungan anak melalui sistem verifikasi dan pengamanan akses terhadap layanan digital. Meskipun demikian, praktik penggunaan identitas orang lain oleh anak dalam transaksi paylater menunjukkan bahwa mekanisme perlindungan tersebut belum sepenuhnya mampu mencegah terjadinya penyalahgunaan layanan pembiayaan digital. Berdasarkan uraian tersebut, penelitian ini bertujuan untuk menganalisis kualifikasi tindak pidana penggunaan identitas orang lain dalam transaksi paylater oleh anak di bawah umur serta menganalisis konstruksi pertanggungjawaban pidana terhadap anak yang melakukan perbuatan tersebut.

2. KAJIAN TEORITIS

Pengertian Tindak Pidana

Tindak pidana merupakan salah satu istilah yang sering dipergunakan untuk menterjemahkan istilah *strafbaarfeit* dalam bahasa Belanda. Tindak pidana merupakan salah satu sendi penting dari hukum pidana selain kesalahan, dan pidana. Tindak pidana merupakan perbuatan yang dirumuskan dalam perundang-undangan pidana sebagai perbuatan yang

dilarang. Perbuatan ini bila dilakukan dengan kesalahan maka orang yang melakukan perbuatan dapat dikenakan sanksi pidana.(Mertha & Gusti, 2016)

Istilah tindak pidana dipakai sebagai terjemah dari istilah *strafbaar feit* atau *delict*. *Strafbaar feit* terdiri dari tiga kata, yakni straf, baar, dan feit, secara literlijk, kata “straf” artinya pidana, “baar” artinya dapat atau boleh dan “feit” adalah perbuatan. Dalam kaitannya dengan istilah strafbaar feit secara utuh, ternyata straf diterjemahkan juga dengan kata hukum. Dan sudah lazim hukum itu adalah terjemahan dari kata recht, seolah-olah arti straf sama dengan recht. Untuk kata “baar”, ada dua istilah yang digunakan yakni boleh dan dapat. Sedangkan kata “feit” digunakan empat istilah yakni, tindak, peristiwa, pelanggaran, dan perbuatan(Chazawi, Adami, 2011). Simons menerangkan strafbaarfeit adalah kelakuan yang diancam dengan pidana, yang bersifat melawan hukum yang berhubungan dengan kesalahan dan yang dilakukan oleh orang yang mampu bertanggung jawab(Rosyadi, 2022). Moeljatno merumuskan strafbaarfeit atau perbuatan pidana adalah suatu perbuatan yang dilarang oleh aturan suatu hukum, larangan mana yang disertai ancaman (sanksi) yang berupa pidana tertentu, bagi barang siapa melanggar larangan tersebut(Siantury, 1998).

Van Hamel menyatakan strafbaarfeit adalah kelakuan orang yang dirumuskan didalam wet, yang bersifat melawan hukum, yang patut dipidana dan dilakukan dengan kesalahan. R.Tresna menyatakan strafbaarfeit atau peristiwa pidana adalah suatu perbuatan atau rangkaian perbuatan manusia yang bertentangan dengan undang-undang atau peraturan lainnya terhadap perbuatan mana diadakan tindakan penghukuman. Wirjono Prodjodikiro menyebutkan tindak pidana adalah suatu perbuatan yang pelakunya dapat dikenakan hukuman pidana(Setiady, 2010). Sekalipun istilah tindak pidana diterjemahkan macam-macam sebagaimana dipaparkan diatas, dalam penjelasannya istilah-istilah tersebut, mengandung pengertian “kelakuan” atau “tingkah laku”.

Tindak Pidana di Ruang Digital

Perkembangan teknologi informasi dan komunikasi telah membawa perubahan besar dalam kehidupan masyarakat modern. Internet dan media digital tidak hanya memberikan manfaat dalam bidang komunikasi, ekonomi, pendidikan, dan pemerintahan, tetapi juga melahirkan berbagai bentuk kejahatan baru yang dikenal sebagai tindak pidana di ruang digital atau *cybercrime*. Tindak pidana di ruang digital merupakan segala bentuk perbuatan melawan hukum yang dilakukan dengan menggunakan sistem elektronik, jaringan internet, maupun perangkat digital sebagai sarana atau objek kejahatan. Fenomena ini menjadi tantangan serius

bagi sistem hukum pidana karena karakteristiknya yang lintas batas, anonim, dan berkembang sangat cepat mengikuti perkembangan teknologi.

Dalam konteks Indonesia, tindak pidana di ruang digital diatur melalui berbagai regulasi, terutama Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik yang telah diubah melalui Undang-Undang Nomor 19 Tahun 2016 dan beberapa penyesuaian regulasi lainnya. Tindak pidana di ruang digital pada dasarnya merupakan bagian dari perkembangan *cybercrime* yang memiliki karakteristik berbeda dengan tindak pidana konvensional.

Salah satu bentuk tindak pidana di ruang digital yang paling sering terjadi adalah penipuan online. Penipuan digital dilakukan melalui berbagai media seperti marketplace, media sosial, aplikasi pesan instan, maupun situs palsu. Penipuan semacam ini sering memanfaatkan kelengahan korban dalam melakukan transaksi elektronik. Penelitian berjudul “Eksistensi Tindak Pidana Penipuan (Bedrog) Dalam Pasal 378 KUHP Di Era Digital” menjelaskan bahwa perkembangan teknologi telah melahirkan modus penipuan baru yang membutuhkan adaptasi hukum pidana agar unsur-unsur dalam Pasal 378 KUHP tetap relevan diterapkan dalam era digital (Miski, Putra, Purwanto, & Luthfiyyah, 2025).

Tindak pidana di ruang digital juga berkaitan erat dengan pencurian data elektronik. Di era digital, data pribadi memiliki nilai ekonomi yang tinggi sehingga sering menjadi sasaran kejahatan siber. Bentuk pencurian data dapat berupa skimming, hacking, phishing, maupun pencurian identitas digital. Penelitian “Tindak Pidana Pencurian Data Elektronik Ditinjau Berdasarkan Undang-Undang ITE” menjelaskan bahwa pencurian data elektronik merupakan bentuk *cybercrime* yang semakin meningkat seiring berkembangnya transaksi digital dan sistem pembayaran elektronik (Tampubolon & Wiryadi, 2025).

Selain itu, reformasi hukum pidana di Indonesia juga mulai menyesuaikan diri dengan perkembangan era digital. Kehadiran KUHP baru melalui Undang-Undang Nomor 1 Tahun 2023 menunjukkan adanya upaya negara untuk memperbarui sistem hukum pidana agar lebih relevan dengan perkembangan teknologi informasi. Penelitian “Reformasi Hukum Pidana di Era Digital: Analisis terhadap KUHP Baru” menjelaskan bahwa KUHP baru mulai mengakomodasi beberapa bentuk tindak pidana digital, meskipun masih terdapat potensi tumpang tindih dengan pengaturan dalam UU ITE dan UU Perlindungan Data Pribadi (Fajriansyah, Siregar, & Panggabean, n.d.).

Dengan demikian, tindak pidana di ruang digital merupakan bentuk kejahatan modern yang terus berkembang mengikuti perkembangan teknologi informasi. Karakteristiknya yang lintas batas, anonim, dan berbasis teknologi menjadikan *cybercrime* sebagai tantangan besar

bagi sistem hukum pidana Indonesia. Keberadaan UU ITE, KUHP baru, dan regulasi perlindungan data pribadi menjadi instrumen penting dalam mengatasi berbagai bentuk kejahatan digital. Namun demikian, perkembangan teknologi yang sangat cepat menuntut adanya pembaruan regulasi dan peningkatan kapasitas aparat penegak hukum agar penegakan hukum di ruang digital dapat berjalan secara efektif dan memberikan perlindungan hukum bagi masyarakat.

Penyalahgunaan Data Pribadi

Perlindungan data pribadi berkaitan dengan konsep privasi. Konsep privasi sendiri merupakan gagasan untuk menjaga integritas dan martabat pribadi. Hak atas privasi juga berarti bahwa individu dapat memilih siapa yang mempunyai informasi tentang dirinya dan bagaimana informasi tersebut digunakan. Selain itu, individu juga mempunyai hak untuk menentukan kondisi di mana transfer data pribadi mereka terjadi. Selain itu, ini juga membantu melindungi privasi Anda. Hak atas privasi telah berkembang dan kini dapat digunakan untuk merumuskan hak untuk melindungi data pribadi.

Ketentuan di Indonesia mengenai perlindungan data pribadi konsumen khususnya dalam transaksi dengan cara elektronik diatur dalam Undang-Undang Nomor 19 Tahun 2016 tentang perubahan atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi secara Elektronik, yang menjelaskan mengenai pemanfaatan informasi melalui elektronik yang ada kaitannya dengan data pribadi harus dilakukan atas persetujuan pemilik data, kecuali telah ada ketentuan lain oleh peraturan perundang-undangan. Undang-Undang Transaksi Elektronik disahkan pada tanggal 27 Oktober 2016 yang mendukung tugas dari pemerintahan dalam memberikan perlindungan kepada masyarakat dari berbagai ancaman penyalahgunaan informasi dan transaksi elektronik dengan memasukkan kewenangan tambahan pada ketentuan pasal 40, yaitu pemerintah wajib mencegah menyebarluaskan informasi elektronik yang memiliki muatan terlarang dan pemerintah memiliki kewajiban dalam memerintahkan penyelenggara sistem elektronik untuk memutus akses yang dimiliki muatan yang dilarang oleh hukum.

Badan Jasa Keuangan juga menerbitkan Peraturan OJK Nomor 77/POJK.01/2016 tentang Pelayanan Pinjam Meminjam Uang Berbasis Teknologi Informasi. Pasal 26 huruf a mengatur bahwa kerahasiaan, integritas, dan ketersediaan data pribadi, transaksional, dan keuangan yang dikendalikan harus dijaga sejak saat diterima hingga dimusnahkan. Selain itu, Peraturan OJK Nomor 13 Tahun 2018 tentang Inovasi Keuangan Digital di Sektor Keuangan memuat hal-hal mengenai perlindungan dan kerahasiaan data. Pasal 30 ayat (1) mengatur bahwa Penyelenggara berkewajiban menjaga kerahasiaan, keutuhan, dan ketersediaan data

pribadi, transaksi, dan keuangan yang dikuasainya sejak diterima hingga dimusnahkan (Aryani & Susanti, 2022).

Banyaknya peraturan mengenai perlindungan data pribadi menunjukkan betapa pentingnya melindungi data pribadi. Sayangnya, aturan tersebut masih tersebar di berbagai peraturan, sehingga belum memberikan perlindungan yang optimal dan efektif terhadap data pribadi sebagai bagian dari privasi. Oleh karena itu, perlu dikembangkan undang-undang yang secara khusus menjamin perlindungan data pribadi.

Kejahatan Pemalsuan Identitas

Identitas digital pada dasarnya merupakan representasi elektronik dari identitas seseorang yang meliputi nama, nomor identitas, data biometrik, alamat, akun media sosial, email, hingga informasi finansial. Dalam konteks digital, identitas memiliki nilai ekonomi dan strategis sehingga menjadi sasaran berbagai bentuk *cybercrime*. Penelitian berjudul “Mini Research Teknologi Keuangan Syariah Identitas Digital Vs Kejahatan Siber” menjelaskan bahwa identitas digital merupakan versi digital dari dokumen identitas fisik yang memungkinkan seseorang mengakses layanan daring. Namun, identitas tersebut rentan terhadap berbagai bentuk penyalahgunaan seperti phishing, hacking, dan pencurian data (Oktafiani, Trisnawati, Maymunah, & Paridah, 2024).

Menurut penelitian “Kejahatan Siber dan Kebijakan Identitas Kependudukan Digital: Sebuah Studi Tentang Potensi Pencurian Data Online”, Indonesia menghadapi tantangan serius terkait keamanan siber akibat maraknya kebocoran data baik di sektor pemerintah maupun swasta (Otniel Purba & Mauluddin, 2023). Kebocoran data tersebut meningkatkan risiko penyalahgunaan identitas digital masyarakat karena informasi pribadi yang tersebar dapat dimanfaatkan untuk berbagai tindakan ilegal. Dalam beberapa kasus, data identitas digunakan untuk registrasi kartu SIM ilegal, pinjaman online, maupun tindak penipuan berbasis digital.

Dalam perspektif hukum pidana, kejahatan identitas digital termasuk bagian dari *cybercrime* yang memiliki karakteristik khusus. Berbeda dengan tindak pidana konvensional, pelaku kejahatan identitas digital dapat beroperasi secara anonim dan lintas negara. Selain itu, alat bukti yang digunakan juga berbentuk elektronik seperti log aktivitas digital, metadata, rekaman transaksi elektronik, dan data komputer. Oleh karena itu, penegakan hukum terhadap kejahatan identitas membutuhkan pendekatan khusus melalui digital forensik dan regulasi hukum yang adaptif terhadap perkembangan teknologi.

Dengan demikian, kejahatan identitas digital merupakan bentuk *cybercrime* yang berkembang pesat seiring kemajuan teknologi informasi. Penyalahgunaan data pribadi, pencurian identitas, hingga manipulasi identitas virtual menunjukkan bahwa identitas digital

telah menjadi objek penting dalam kejahatan modern. Oleh sebab itu, pembaruan regulasi, penguatan keamanan siber, serta peningkatan kesadaran masyarakat menjadi langkah penting dalam memberikan perlindungan hukum terhadap identitas digital di era teknologi informasi.

3. METODE PENELITIAN

Jenis Penelitian ini adalah penelitian yuridis normatif atau *legal research* yang difokuskan pada asas-asas hukum, merupakan jenis penelitian hukum kepustakaan yang dilakukan melalui analisis bahan-bahan kepustakaan atau data sekunder saja.(Pertiwi, Nuraldini, Buana, & Arthacerses, n.d.). Penelitian ini menggunakan metode pendekatan undang-undang (*statue approach*), dan juga menggunakan pendekatan konseptual (*conseptual approach*). Pengertian pendekatan undang-undang (*statue approach*) menurut Peter Mahmud Marzuki adalah pendekatan dengan menelaah semua regulasi dan undang-undang yang terkait dengan isu hukum yang tengah di hadapi. Sedangkan penelitian *conseptual approach* pendekatan ini beranjak dari pandangan-pandangan dan doktrin-doktrin yang berkembang dalam ilmu hukum. Pendekatan penelitian dipilih dalam rangka mencari jawaban atas isu-isu hukum dalam suatu penelitian hukum. Oleh karena itu, kesesuaian antara pendekatan dengan isu hukum merupakan pertimbangan utama dalam melakukan pilihannya(Marzuki, 2019)

4. HASIL DAN PEMBAHASAN

Kualifikasi Tindak Pidana Penggunaan Identitas Orang Lain dalam Transaksi PayLater oleh Anak di Bawah Umur

Secara empiris, berbagai penelitian menunjukkan bahwa penggunaan *PayLater* di kalangan generasi muda didorong oleh faktor kemudahan, fleksibilitas pembayaran, serta pengaruh gaya hidup konsumtif. Muzakkir et al dalam penelitiannya mengungkapkan bahwa generasi Z cenderung menggunakan layanan *PayLater* karena kemudahan akses dan kurangnya pertimbangan risiko jangka panjang(Syam & Fatwa, n.d.). Sementara itu, Nurfitri menegaskan bahwa *PayLater* dapat mendorong perilaku konsumtif dan impulsif, yang dalam kondisi tertentu berpotensi mengarah pada penyalahgunaan, termasuk penggunaan identitas orang lain(Nurfitri, Setyaningsih, & Gunadarma, n.d.). Hal ini menunjukkan bahwa persoalan penyalahgunaan *PayLater* oleh anak tidak hanya berkaitan dengan aspek hukum, tetapi juga dipengaruhi oleh faktor sosial, ekonomi, dan psikologis.

Dalam menentukan apakah penyalahgunaan *PayLater* oleh anak merupakan tindak pidana, harus dianalisis terlebih dahulu apakah perbuatan tersebut memenuhi unsur-unsur tindak pidana, baik unsur subjektif maupun unsur objektif. Unsur subjektif berkaitan dengan

kesengajaan atau kealpaan pelaku, sedangkan unsur objektif berkaitan dengan perbuatan, akibat, serta sifat melawan hukum dari tindakan tersebut. Dalam praktiknya, penyalahgunaan *PayLater* oleh anak bukanlah perbuatan tunggal, melainkan rangkaian perbuatan yang dimulai dari pengambilan data pribadi, manipulasi sistem elektronik, hingga perolehan keuntungan secara melawan hukum. Oleh karena itu, analisis unsur delik harus dilakukan secara bertahap sesuai dengan alur perbuatan tersebut.

Tahap pertama adalah perolehan dan penggunaan data pribadi orang lain, yang diatur dalam Pasal 67 Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi, yang menyatakan:

(1) Setiap Orang yang dengan sengaja dan melawan hukum memperoleh atau mengumpulkan Data Pribadi yang bukan miliknya dengan maksud untuk menguntungkan diri sendiri atau orang lain yang dapat mengakibatkan kerugian Subjek Data Pribadi dipidana dengan pidana penjara paling lama 5 (lima) tahun dan/atau pidana denda paling banyak Rp5.000.000.000,00 (lima miliar rupiah). (2) Setiap Orang yang dengan sengaja dan melawan hukum mengungkapkan Data Pribadi yang bukan miliknya dipidana dengan pidana penjara paling lama 4 (empat) tahun dan/atau pidana denda paling banyak Rp4.000.000.000,00 (empat miliar rupiah). (3) Setiap Orang yang dengan sengaja dan melawan hukum menggunakan Data Pribadi yang bukan miliknya dipidana dengan pidana penjara paling lama 5 (lima) tahun dan/atau pidana denda paling banyak Rp5.000.000.000,00 (lima miliar rupiah).

Berdasarkan rumusan pasal tersebut, terdapat sejumlah unsur yang harus dianalisis secara lebih mendalam, baik dari sisi subjektif maupun objektif. Unsur pertama yang perlu diperhatikan adalah frasa “Setiap Orang”. Frasa ini menunjukkan bahwa subjek hukum dalam ketentuan ini bersifat umum (*algemeen*), sehingga tidak membedakan usia, status, maupun kapasitas hukum seseorang. Dengan demikian, anak sebagai pelaku tetap termasuk dalam kategori “Setiap Orang” dan dapat dimintai pertanggungjawaban pidana, meskipun mekanisme dan bentuk pertanggungjawabannya tunduk pada sistem peradilan pidana anak.

Unsur berikutnya adalah “dengan sengaja”, yang merupakan bentuk kesalahan (*schuld*) dalam hukum pidana dan termasuk dalam unsur subjektif. Kesengajaan (*dolus*) dalam konteks ini tidak hanya berarti pelaku mengetahui perbuatannya, tetapi juga menghendaki akibat dari perbuatan tersebut. Dalam kasus penyalahgunaan *PayLater*, anak yang menggunakan identitas orang lain umumnya memahami bahwa data tersebut bukan miliknya dan tetap menggunakannya untuk mendapatkan akses layanan, sehingga unsur kesengajaan dapat dikatakan terpenuhi. Bahkan, dalam beberapa kasus, tindakan tersebut dilakukan secara

aktif dan terencana, misalnya dengan mencari data identitas melalui media sosial atau lingkungan sekitar.

Selanjutnya adalah unsur “melawan hukum”, yang merupakan unsur objektif sekaligus normatif. Sifat melawan hukum dalam pasal ini tidak selalu harus dinyatakan secara eksplisit, tetapi secara implisit melekat pada perbuatan yang bertentangan dengan norma hukum yang berlaku. Penggunaan data pribadi orang lain tanpa izin jelas bertentangan dengan hak privasi dan perlindungan data pribadi yang dijamin oleh undang-undang, sehingga memenuhi unsur melawan hukum baik secara formal maupun material.

Unsur penting lainnya dalam ayat (1) adalah “memperoleh atau mengumpulkan Data Pribadi yang bukan miliknya”. Frasa ini mencakup dua bentuk perbuatan, yaitu memperoleh (*acquiring*) dan mengumpulkan (*collecting*). Memperoleh dapat diartikan sebagai tindakan mendapatkan data pribadi dari sumber tertentu, baik secara langsung maupun tidak langsung, sedangkan mengumpulkan mengandung makna adanya aktivitas sistematis untuk menghimpun data dalam jumlah tertentu. Dalam praktik penyalahgunaan *PayLater*, anak dapat memperoleh data melalui berbagai cara, seperti meminjam KTP tanpa izin, mengambil foto identitas, atau bahkan mengakses data digital milik orang lain. Dengan demikian, unsur ini bersifat luas dan mencakup berbagai modus operandi.

Selanjutnya, unsur “dengan maksud untuk menguntungkan diri sendiri atau orang lain” merupakan unsur subjektif yang menunjukkan adanya tujuan tertentu dari perbuatan tersebut. Keuntungan dalam konteks ini tidak harus selalu berupa uang secara langsung, tetapi dapat berupa fasilitas kredit, barang, atau jasa yang diperoleh melalui layanan *PayLater*. Dalam kasus ini, pelaku anak menggunakan identitas orang lain untuk mendapatkan limit kredit, sehingga jelas terdapat tujuan untuk memperoleh keuntungan tidak sah.

Unsur berikutnya adalah “yang dapat mengakibatkan kerugian Subjek Data Pribadi”. Unsur ini bersifat objektif dan berkaitan dengan akibat yang ditimbulkan dari perbuatan tersebut. Kerugian tidak hanya terbatas pada kerugian materiil, seperti beban utang yang harus ditanggung oleh pemilik data, tetapi juga mencakup kerugian immateriil, seperti pelanggaran privasi, reputasi, dan rasa aman. Bahkan, dalam beberapa kasus, korban dapat mengalami kesulitan administratif atau hukum akibat penyalahgunaan identitasnya.

Dalam ayat (2), unsur yang perlu diperhatikan adalah “mengungkapkan Data Pribadi”, yang berarti menyebarluaskan atau memberikan akses data kepada pihak lain tanpa hak. Meskipun dalam kasus *PayLater* unsur ini tidak selalu dominan, namun dapat terjadi apabila pelaku membagikan data tersebut kepada pihak lain, misalnya dalam praktik jual beli data atau penggunaan bersama.

Sementara itu, dalam ayat (3), unsur “menggunakan Data Pribadi yang bukan miliknya” merupakan inti dari perbuatan dalam kasus ini. Penggunaan di sini mencakup pemanfaatan data dalam suatu sistem atau transaksi, termasuk dalam proses registrasi dan verifikasi layanan *PayLater*. Unsur ini sangat relevan karena menjadi titik utama terjadinya kerugian, yaitu ketika data digunakan untuk memperoleh fasilitas keuangan.

Dengan demikian, apabila seluruh unsur tersebut dianalisis secara sistematis, maka perbuatan anak yang menggunakan identitas orang lain dalam transaksi *PayLater* tidak hanya memenuhi satu unsur delik, tetapi mencakup keseluruhan rangkaian unsur dalam Pasal 67 Undang-Undang Perlindungan Data Pribadi. Hal ini menunjukkan bahwa sejak tahap awal, perbuatan tersebut telah memiliki kualitas sebagai tindak pidana yang utuh, baik dari aspek perbuatan, kesalahan, maupun akibat yang ditimbulkan. Oleh karena itu, secara yuridis, tidak terdapat keraguan bahwa penyalahgunaan data pribadi dalam konteks ini merupakan bentuk pelanggaran hukum yang serius, meskipun dalam penerapan sanksinya tetap harus mempertimbangkan status pelaku sebagai anak.

Tahap berikutnya adalah manipulasi data dalam sistem elektronik, yang diatur dalam Pasal 35 Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik: *“Setiap Orang dengan sengaja dan tanpa hak atau melawan hukum melakukan manipulasi, penciptaan, perubahan, penghilangan, pengrusakan Informasi Elektronik dan/atau Dokumen Elektronik dengan tujuan agar Informasi Elektronik dan/atau Dokumen Elektronik tersebut dianggap seolah-olah data yang otentik.”*

Dengan ancaman pidana dalam Pasal 51 ayat (1): *“Setiap Orang yang memenuhi unsur sebagaimana dimaksud dalam Pasal 35 dipidana dengan pidana penjara paling lama 12 (dua belas) tahun dan/atau denda paling banyak Rp12.000.000.000,00 (dua belas miliar rupiah).”* Dalam hal ini, unsur objektif berupa manipulasi informasi elektronik memang telah terpenuhi ketika pelaku mengunggah atau memasukkan data palsu ke dalam sistem *PayLater*. Namun, jika dianalisis lebih mendalam, Pasal 35 sebenarnya memuat beberapa unsur lain yang memiliki cakupan luas dan relevansi kuat dalam konteks penyalahgunaan identitas oleh pelaku anak.

Pertama, unsur “Setiap Orang” menunjukkan bahwa subjek hukum dalam delik ini bersifat umum dan tidak terbatas pada kategori tertentu. Dengan demikian, anak sebagai pelaku tetap termasuk dalam cakupan subjek hukum pidana. Meskipun demikian, dalam hal pertanggungjawaban pidananya, anak tetap tunduk pada ketentuan khusus dalam sistem peradilan pidana anak. Hal ini menegaskan bahwa dari sisi perumusan delik, tidak ada pengecualian terhadap usia, tetapi dari sisi penerapan sanksi terdapat perlakuan khusus.

Kedua, unsur “dengan sengaja” merupakan unsur subjektif yang sangat penting. Kesengajaan (*dolus*) dalam konteks ini tidak hanya berarti mengetahui, tetapi juga menghendaki terjadinya perbuatan tersebut. Dalam praktik penyalahgunaan *PayLater*, anak biasanya secara sadar memasukkan data orang lain, memahami bahwa data tersebut bukan miliknya, dan tetap menggunakannya untuk memperoleh akses kredit. Hal ini menunjukkan adanya bentuk kesengajaan langsung (*dolus directus*), karena tujuan utama pelaku memang untuk membuat sistem percaya bahwa data tersebut sah.

Ketiga, unsur “tanpa hak atau melawan hukum” menegaskan bahwa perbuatan tersebut tidak memiliki dasar legal yang sah. Dalam konteks ini, pelaku tidak memiliki otoritas untuk menggunakan data pribadi orang lain. Bahkan jika data tersebut diperoleh dengan cara yang tampaknya “tidak ilegal” (misalnya dari teman atau keluarga), penggunaan tanpa izin tetap dapat dikategorikan sebagai perbuatan melawan hukum. Unsur ini mempertegas bahwa sifat melawan hukum tidak hanya dilihat dari cara memperoleh data, tetapi juga dari cara penggunaannya.

Keempat, unsur perbuatan dalam pasal ini sangat luas, yaitu mencakup “manipulasi, penciptaan, perubahan, penghilangan, dan pengrusakan Informasi Elektronik dan/atau Dokumen Elektronik.” Dalam kasus *PayLater*, bentuk yang paling umum adalah manipulasi dan penciptaan data. Manipulasi dapat berupa pengubahan informasi agar sesuai dengan identitas palsu yang digunakan, sedangkan penciptaan dapat berupa pembuatan akun baru dengan data yang tidak benar. Namun, tidak tertutup kemungkinan juga terjadi unsur perubahan, misalnya ketika pelaku mengedit data asli agar tampak berbeda. Luasnya cakupan perbuatan ini menunjukkan bahwa hukum berusaha mengantisipasi berbagai bentuk kejahatan digital yang terus berkembang.

Kelima, unsur “Informasi Elektronik dan/atau Dokumen Elektronik” juga memiliki makna yang sangat luas. Informasi elektronik mencakup data, teks, gambar, atau suara yang diproses secara digital, sedangkan dokumen elektronik mencakup setiap informasi yang dibuat, diteruskan, atau disimpan dalam bentuk elektronik. Dalam sistem *PayLater*, seluruh proses verifikasi identitas berbasis pada dokumen elektronik, seperti foto KTP, selfie, dan data digital lainnya. Oleh karena itu, tindakan pelaku yang memanfaatkan data tersebut secara tidak sah secara langsung memenuhi unsur ini.

Keenam, unsur yang paling krusial adalah “dengan tujuan agar dianggap seolah-olah data yang otentik.” Unsur ini merupakan inti dari delik manipulasi elektronik, karena menunjukkan adanya maksud untuk menciptakan ilusi keaslian. Dalam sistem digital, kepercayaan terhadap data merupakan fondasi utama. Ketika pelaku berhasil membuat data

palsu terlihat asli, maka sistem akan memberikan akses atau hak tertentu yang seharusnya tidak dimiliki oleh pelaku. Dengan demikian, unsur ini tidak hanya berkaitan dengan perbuatan teknis, tetapi juga dengan aspek psikologis berupa niat untuk menipu sistem atau pihak lain.

Selain itu, penting untuk dipahami bahwa delik dalam Pasal 35 ini merupakan delik formil, yang berarti perbuatan dianggap selesai pada saat tindakan manipulasi dilakukan, tanpa harus menunggu timbulnya kerugian. Hal ini berbeda dengan delik material yang mensyaratkan adanya akibat tertentu. Dengan demikian, meskipun dalam praktik *PayLater* kerugian biasanya memang terjadi, secara hukum kerugian bukanlah syarat mutlak untuk menyatakan bahwa tindak pidana telah terjadi.

Dari perspektif teoritis, unsur-unsur dalam Pasal 35 ini mencerminkan perpaduan antara unsur subjektif (kesengajaan dan tujuan) dan unsur objektif (perbuatan manipulasi terhadap data elektronik). Hal ini sejalan dengan teori tindak pidana yang membedakan antara aspek batin pelaku dan perbuatan lahiriah. Kedua aspek tersebut harus terpenuhi secara bersamaan agar suatu perbuatan dapat dikualifikasikan sebagai tindak pidana.

Dengan demikian, apabila dikaitkan dengan penyalahgunaan *PayLater* oleh anak, dapat disimpulkan bahwa seluruh unsur dalam Pasal 35 telah terpenuhi secara komprehensif. Pelaku bertindak sebagai “setiap orang”, melakukan perbuatan manipulasi atau penciptaan data elektronik, tanpa hak, dengan sengaja, dan dengan tujuan agar data tersebut dianggap otentik. Oleh karena itu, secara yuridis, perbuatan tersebut dapat dikualifikasikan sebagai tindak pidana manipulasi informasi elektronik, yang selanjutnya menjadi salah satu dasar penting dalam menentukan pertanggungjawaban pidana, meskipun dalam penerapannya tetap harus mempertimbangkan aspek perlindungan anak dan prinsip keadilan restoratif.

Selanjutnya, tindakan tersebut berkembang menjadi pemalsuan yang menimbulkan akibat hukum, sebagaimana diatur dalam Pasal 391 Undang-Undang Nomor 1 Tahun 2023:

(1) Setiap Orang yang membuat secara tidak benar atau memalsu Surat yang dapat menimbulkan suatu hak, perikatan atau pembebasan utang, atau yang diperuntukkan sebagai bukti dari suatu hal, dengan maksud untuk menggunakan atau meminta orang lain menggunakan seolah-olah isinya benar dan tidak palsu, jika penggunaan Surat tersebut dapat menimbulkan kerugian, dipidana karena pemalsuan Surat, dengan pidana penjara paling lama 6 (enam) tahun atau pidana denda paling banyak kategori M.

Dalam konteks ini, dokumen elektronik yang digunakan dalam sistem *PayLater* dapat dikualifikasikan sebagai “Surat”. Unsur objektif berupa perbuatan memalsu dan timbulnya hak (limit kredit) telah terpenuhi, sedangkan unsur subjektif berupa maksud untuk menggunakan

seolah-olah benar juga jelas terlihat. Hal ini menunjukkan bahwa delik ini bersifat material karena menimbulkan akibat hukum berupa perikatan.

Apabila dianalisis lebih mendalam, rumusan Pasal 391 tersebut sebenarnya memuat sejumlah unsur penting lain yang memperkuat konstruksi tindak pidana pemalsuan dalam kasus penyalahgunaan *PayLater*. Unsur pertama yang perlu diperhatikan adalah frasa “Setiap Orang”, yang menunjukkan bahwa subjek hukum dalam delik ini bersifat umum (*algemeen subject*). Artinya, tidak ada pembatasan mengenai siapa yang dapat menjadi pelaku, sehingga anak sebagai pelaku tetap termasuk dalam cakupan norma ini. Namun demikian, meskipun anak memenuhi unsur sebagai subjek hukum, aspek pertanggungjawaban pidananya tetap tunduk pada ketentuan khusus dalam sistem peradilan pidana anak.

Unsur berikutnya adalah “membuat secara tidak benar atau memalsu Surat”. Frasa ini mengandung dua bentuk perbuatan, yaitu membuat surat yang sejak awal tidak benar (*valselijk opmaken*) dan memalsu surat yang sudah ada (*vervalsen*). Dalam praktik penyalahgunaan *PayLater*, kedua bentuk ini dapat terjadi sekaligus. Pelaku dapat membuat akun baru dengan data identitas palsu (membuat secara tidak benar), atau mengubah data yang telah ada, misalnya dengan mengganti foto atau informasi tertentu (memalsu). Dengan demikian, unsur ini memiliki cakupan yang luas dan mampu menjangkau berbagai modus operandi dalam kejahatan berbasis digital.

Perkembangan teknologi informasi telah mengubah konsep “surat” dalam hukum pidana dari yang semula bersifat fisik menjadi juga mencakup bentuk elektronik. Dalam konteks transaksi *PayLater*, identitas digital seperti foto KTP elektronik, swafoto (*selfie verification*), tanda tangan elektronik, maupun data akun pengguna pada dasarnya memiliki fungsi pembuktian yang sama dengan surat dalam pengertian konvensional. Oleh karena itu, identitas digital dapat dipersamakan dengan surat apabila memenuhi fungsi sebagai alat bukti, alat legitimasi, atau dasar timbulnya hak dan kewajiban hukum. Hal ini sejalan dengan ketentuan Pasal 5 ayat (1) Undang-Undang Informasi dan Transaksi Elektronik yang menyatakan bahwa Informasi Elektronik dan/atau Dokumen Elektronik merupakan alat bukti hukum yang sah. Dengan demikian, penyalahgunaan identitas digital dalam sistem *PayLater* bukan sekadar penyalahgunaan data biasa, melainkan juga dapat dikualifikasikan sebagai pemalsuan surat dalam bentuk elektronik karena data tersebut dipergunakan untuk menciptakan hubungan hukum berupa pemberian fasilitas kredit dan pengakuan utang. Pandangan ini menunjukkan adanya perluasan makna surat dalam hukum pidana modern agar mampu menyesuaikan perkembangan transaksi digital(2019).

Selanjutnya, terdapat unsur “yang dapat menimbulkan suatu hak, perikatan atau pembebasan utang”. Unsur ini menunjukkan bahwa tidak semua pemalsuan surat dapat dipidana, melainkan hanya yang memiliki potensi akibat hukum tertentu. Dalam konteks *PayLater*, dokumen identitas yang dipalsukan menjadi dasar bagi timbulnya hubungan hukum antara pengguna dan penyedia layanan, yaitu berupa hak untuk memperoleh fasilitas kredit dan kewajiban untuk membayar di kemudian hari. Oleh karena itu, pemalsuan tersebut tidak hanya bersifat administratif, tetapi juga berdampak pada lahirnya hubungan perikatan yang sah secara hukum (meskipun didasarkan pada data palsu).

Unsur berikutnya adalah “atau yang diperuntukkan sebagai bukti dari suatu hal”. Unsur ini memperluas cakupan objek delik, karena tidak hanya mencakup surat yang menimbulkan hak, tetapi juga surat yang berfungsi sebagai alat bukti. Dalam sistem *PayLater*, data identitas yang diunggah berfungsi sebagai bukti verifikasi pengguna. Dengan demikian, meskipun tidak secara langsung menciptakan hak, dokumen tersebut tetap memiliki nilai pembuktian yang signifikan, sehingga pemalsuannya tetap termasuk dalam ruang lingkup pasal ini.

Lebih lanjut, unsur “dengan maksud untuk menggunakan atau meminta orang lain menggunakan seolah-olah isinya benar dan tidak palsu” merupakan unsur subjektif yang menegaskan adanya kesengajaan (*dolus*). Unsur ini tidak hanya mensyaratkan adanya kehendak untuk memalsu, tetapi juga adanya tujuan lanjutan, yaitu agar surat tersebut digunakan dan dipercaya sebagai sesuatu yang sah. Dalam kasus *PayLater*, pelaku secara sadar menginginkan agar sistem atau pihak penyedia layanan mempercayai data yang dimasukkan, sehingga dapat memperoleh persetujuan kredit. Hal ini menunjukkan adanya *opzet als oogmerk* (kesengajaan sebagai maksud), yang merupakan bentuk kesengajaan tingkat tertinggi dalam hukum pidana.

Unsur terakhir yang tidak kalah penting adalah “jika penggunaan Surat tersebut dapat menimbulkan kerugian”. Unsur ini menegaskan bahwa delik pemalsuan dalam Pasal 391 merupakan delik yang mensyaratkan adanya potensi kerugian, meskipun tidak harus secara nyata. Dalam konteks *PayLater*, kerugian dapat dialami oleh berbagai pihak, termasuk penyedia layanan yang tidak menerima pembayaran, serta pemilik identitas asli yang disalahgunakan. Bahkan, kerugian juga dapat bersifat immateriil, seperti rusaknya reputasi atau terganggunya privasi seseorang.

Dengan memperhatikan seluruh unsur tersebut, terlihat bahwa Pasal 391 KUHP memiliki struktur delik yang kompleks dan komprehensif, yang mampu menjangkau berbagai bentuk pemalsuan, termasuk dalam ranah digital. Dalam perspektif teori unsur tindak pidana,

unsur-unsur tersebut mencerminkan perpaduan antara unsur objektif (perbuatan memalsu, objek berupa surat, serta akibat berupa potensi kerugian) dan unsur subjektif (kesengajaan dan maksud tertentu). Oleh karena itu, apabila seluruh unsur tersebut terpenuhi, maka perbuatan pelaku dapat secara sah dikualifikasikan sebagai tindak pidana pemalsuan surat.

Dalam konteks pelaku anak, pemenuhan unsur-unsur tersebut tetap harus dianalisis secara hati-hati, khususnya terkait dengan unsur kesengajaan dan kemampuan bertanggung jawab. Hal ini penting untuk memastikan bahwa pertanggungjawaban pidana yang dibebankan kepada anak tidak hanya didasarkan pada terpenuhinya unsur delik semata, tetapi juga mempertimbangkan aspek psikologis dan perkembangan anak itu sendiri. Dengan demikian, analisis terhadap Pasal 391 KUHP tidak hanya berhenti pada pemenuhan unsur-unsur normatif, tetapi juga harus diintegrasikan dengan prinsip-prinsip perlindungan anak dalam sistem hukum pidana Indonesia.

Tahap selanjutnya adalah perolehan keuntungan melalui penipuan sebagaimana diatur dalam Pasal 492 KUHP:

Setiap Orang yang dengan maksud menguntungkan diri sendiri atau orang lain secara melawan hukum dengan memakai nama palsu atau kedudukan palsu, menggunakan tipu muslihat atau rangkaian kata bohong, menggerakkan orang supaya menyerahkan suatu Barang, memberi utang, membuat pengakuan utang, atau menghapus piutang, dipidana karena penipuan, dengan pidana penjara paling lama 4 (empat) tahun atau pidana denda paling banyak kategori V.

Dalam ketentuan tersebut, unsur pertama yang perlu dianalisis adalah frasa “Setiap Orang”. Unsur ini menunjukkan bahwa subjek hukum dalam tindak pidana penipuan bersifat umum (*algemeen subject*), sehingga tidak membedakan antara orang dewasa maupun anak. Artinya, anak sebagai pelaku tetap dapat dikualifikasikan sebagai subjek tindak pidana, meskipun dalam hal pertanggungjawaban pidana akan tunduk pada ketentuan khusus dalam sistem peradilan pidana anak. Dengan demikian, dari perspektif unsur delik, tidak ada pengecualian terhadap status usia pelaku.

Unsur berikutnya adalah “*dengan maksud menguntungkan diri sendiri atau orang lain secara melawan hukum*”. Unsur ini merupakan unsur subjektif yang menitikberatkan pada adanya kesengajaan (*dolus*) sekaligus tujuan tertentu (*oogmerk*). Dalam konteks penyalahgunaan *PayLater*, pelaku anak secara sadar menggunakan identitas orang lain dengan tujuan memperoleh fasilitas kredit atau barang tanpa memenuhi kewajiban pembayaran. Keuntungan tersebut jelas bersifat melawan hukum karena diperoleh melalui cara yang bertentangan dengan ketentuan hukum dan tanpa hak yang sah. Unsur ini menjadi sangat

penting karena tanpa adanya maksud tersebut, perbuatan tidak dapat dikualifikasikan sebagai penipuan.

Selanjutnya, unsur “memakai nama palsu atau kedudukan palsu” memiliki relevansi langsung dengan modus operandi dalam penyalahgunaan *PayLater*. Penggunaan identitas orang lain, baik berupa KTP, nomor telepon, maupun data digital lainnya, merupakan bentuk nyata dari penggunaan nama palsu. Tidak hanya itu, dalam beberapa kasus, pelaku juga menempatkan dirinya seolah-olah memiliki status atau kedudukan tertentu yang sebenarnya tidak dimilikinya, misalnya sebagai pemilik identitas tersebut. Dengan demikian, unsur ini menunjukkan adanya bentuk penyamaran identitas yang disengaja untuk menyesatkan pihak lain.

Dalam perspektif hukum pidana, penggunaan identitas digital milik orang lain dalam transaksi *PayLater* pada dasarnya dapat dikualifikasikan sebagai penggunaan “nama palsu” sebagaimana dimaksud dalam Pasal 492 KUHP. Nama palsu tidak selalu dimaknai sebagai penggunaan nama fiktif yang sepenuhnya tidak ada, melainkan juga mencakup penggunaan identitas orang lain untuk menciptakan kesan seolah-olah pelaku adalah subjek hukum yang sah. Dalam konteks transaksi digital, identitas tidak hanya terdiri atas nama, tetapi juga nomor induk kependudukan, foto diri, nomor telepon, alamat surel, hingga data biometrik yang digunakan untuk verifikasi elektronik. Ketika anak menggunakan data tersebut untuk memperoleh fasilitas kredit *PayLater*, maka secara yuridis pelaku telah menempatkan dirinya sebagai orang lain di hadapan sistem elektronik maupun penyedia layanan. Oleh karena itu, unsur “nama palsu” terpenuhi karena terdapat penyamaran identitas yang bertujuan menimbulkan kepercayaan palsu demi memperoleh keuntungan secara melawan hukum. Pandangan ini sejalan dengan perkembangan doktrin hukum pidana modern yang memandang identitas digital sebagai perluasan dari identitas personal konvensional dalam transaksi elektronik (Chazawi, Adami, 2011).

Unsur berikutnya yang tidak kalah penting adalah “menggunakan tipu muslihat atau rangkaian kata bohong”. Unsur ini memperluas bentuk perbuatan penipuan, tidak hanya terbatas pada penggunaan identitas palsu, tetapi juga mencakup segala bentuk rekayasa atau manipulasi informasi yang bertujuan menimbulkan kepercayaan palsu. Dalam sistem *PayLater* yang berbasis digital, tipu muslihat dapat berupa manipulasi data elektronik, pengisian informasi yang tidak benar, hingga penggunaan teknik tertentu agar sistem verifikasi menganggap data tersebut valid. Dengan demikian, unsur ini menunjukkan bahwa penipuan tidak selalu dilakukan melalui komunikasi langsung, tetapi juga dapat terjadi melalui interaksi dengan sistem elektronik.

Lebih lanjut, unsur “menggerakkan orang supaya menyerahkan suatu Barang, memberi utang, membuat pengakuan utang, atau menghapus piutang” merupakan unsur objektif yang berkaitan dengan akibat dari perbuatan penipuan. Dalam konteks *PayLater*, unsur ini terpenuhi ketika sistem atau penyedia layanan memberikan fasilitas kredit kepada pelaku berdasarkan data yang telah dimanipulasi. Meskipun dalam praktiknya tidak selalu ada interaksi langsung dengan manusia, sistem elektronik yang memberikan persetujuan kredit tetap dapat dipandang sebagai representasi dari kehendak penyedia layanan. Dengan demikian, tindakan pelaku telah menggerakkan pihak lain (dalam hal ini penyedia layanan) untuk memberikan utang.

Unsur “menyerahkan suatu Barang” dalam pasal ini juga perlu dimaknai secara luas, tidak hanya terbatas pada benda berwujud, tetapi juga mencakup manfaat ekonomi, termasuk fasilitas pembiayaan dalam *PayLater*. Hal ini menunjukkan bahwa hukum pidana telah berkembang mengikuti dinamika transaksi modern yang tidak lagi selalu melibatkan penyerahan barang secara fisik.

Selain itu, unsur “membuat pengakuan utang” juga relevan dalam konteks ini, karena dalam sistem *PayLater*, setiap transaksi pada dasarnya menciptakan hubungan hukum berupa utang-piutang antara pengguna dan penyedia layanan. Dengan menggunakan identitas palsu, pelaku secara tidak langsung menciptakan pengakuan utang atas nama orang lain, yang jelas merupakan bentuk penyimpangan hukum.

Adapun unsur “menghapus piutang” meskipun tidak selalu muncul dalam setiap kasus *PayLater*, tetap memiliki relevansi dalam konteks yang lebih luas, misalnya apabila pelaku dengan sengaja menghindari kewajiban pembayaran sehingga merugikan pihak penyedia layanan.

Berdasarkan keseluruhan uraian tersebut, dapat disimpulkan bahwa seluruh unsur dalam Pasal 492 KUHP terpenuhi secara kumulatif dalam kasus penyalahgunaan *PayLater* oleh anak, baik unsur subjektif maupun unsur objektif. Oleh karena itu, tindak pidana penipuan dapat dikatakan sebagai delik inti (*core offense*) yang menjadi pusat dari rangkaian perbuatan tersebut. Bahkan secara kritis dapat dikatakan bahwa tanpa adanya unsur penipuan, rangkaian perbuatan lain seperti penyalahgunaan data pribadi dan manipulasi informasi elektronik tidak akan menghasilkan keuntungan ekonomi bagi pelaku.

Dengan demikian, penipuan dalam konteks ini tidak hanya merupakan salah satu tindak pidana, tetapi juga menjadi titik kulminasi dari seluruh rangkaian kejahatan yang dilakukan, yang sekaligus menjadi dasar utama dalam menentukan pertanggungjawaban pidana terhadap pelaku.

Selain memenuhi unsur penipuan dan pemalsuan, secara doktrinal terdapat pendapat yang mencoba memperluas konstruksi tindak pidana ini ke arah pencurian dalam arti luas berdasarkan Pasal 476 KUHP: *“Setiap Orang yang mengambil suatu Barang yang sebagian atau seluruhnya milik orang lain, dengan maksud untuk dimiliki secara melawan hukum, dipidana karena pencurian, dengan pidana penjara paling lama 5 (lima) tahun atau pidana denda paling banyak kategori V.”*

Meskipun dilakukan melalui sistem digital, unsur pengambilan barang secara melawan hukum tetap terpenuhi, sehingga memperkuat bahwa kejahatan ini merupakan kombinasi antara delik konvensional dan modern. Namun, untuk memberikan pemahaman yang lebih komprehensif, perlu diuraikan lebih lanjut setiap unsur yang terkandung dalam pasal tersebut, baik dari aspek objektif maupun subjektifnya.

Unsur pertama yang terkandung dalam pasal ini adalah frasa “Setiap Orang”, yang menunjukkan bahwa subjek hukum dalam tindak pidana pencurian bersifat umum (generalis). Artinya, siapa pun tanpa terkecuali dapat menjadi pelaku tindak pidana ini, termasuk anak. Dalam konteks hukum pidana anak, meskipun anak termasuk dalam kategori “Setiap Orang”, namun perlakuan terhadapnya tetap tunduk pada rezim khusus sebagaimana diatur dalam sistem peradilan pidana anak. Dengan demikian, unsur ini menegaskan bahwa secara normatif tidak ada pengecualian terhadap anak sebagai subjek delik, tetapi dalam hal pertanggungjawaban dan pемidanaannya berlaku ketentuan khusus.

Unsur berikutnya adalah “mengambil suatu Barang”, yang merupakan inti dari perbuatan dalam tindak pidana pencurian. Secara klasik, “mengambil” diartikan sebagai memindahkan suatu barang dari kekuasaan orang lain ke dalam kekuasaan pelaku. Namun dalam perkembangan hukum modern, pengertian ini tidak lagi terbatas pada benda berwujud (*tangible goods*), melainkan juga mencakup nilai ekonomi, manfaat, atau akses terhadap suatu fasilitas yang memiliki nilai finansial. Dalam konteks *PayLater*, pelaku tidak secara langsung mengambil barang secara fisik dari pemiliknya, melainkan memperoleh barang atau jasa melalui fasilitas kredit yang diperoleh secara tidak sah. Oleh karena itu, tindakan tersebut dapat dipandang sebagai bentuk “pengambilan” dalam arti luas, yaitu penguasaan atas nilai ekonomi milik pihak lain tanpa hak.

Selanjutnya, unsur “yang sebagian atau seluruhnya milik orang lain” menegaskan bahwa objek yang diambil bukan merupakan milik pelaku. Dalam kasus penyalahgunaan *PayLater*, barang yang diperoleh atau fasilitas kredit yang digunakan merupakan milik penyedia layanan atau merchant yang bekerja sama dengan platform tersebut. Dengan demikian, terdapat pemisahan yang jelas antara pelaku dan pemilik objek, sehingga unsur ini

terpenuhi. Bahkan dalam beberapa kasus, kerugian tidak hanya dialami oleh satu pihak, tetapi juga dapat melibatkan pemilik identitas yang disalahgunakan, sehingga memperluas dimensi korban dalam tindak pidana ini.

Unsur yang sangat penting berikutnya adalah “dengan maksud untuk dimiliki”, yang merupakan unsur subjektif yang menunjukkan adanya kehendak (*mens rea*) dari pelaku untuk menguasai barang tersebut. Maksud untuk memiliki ini tidak selalu berarti kepemilikan secara permanen, tetapi cukup menunjukkan adanya niat untuk memperlakukan barang tersebut seolah-olah miliknya sendiri. Dalam konteks ini, ketika pelaku menggunakan fasilitas *PayLater* dengan identitas orang lain dan tidak memiliki niat untuk membayar kewajiban tersebut, maka sejak awal sudah terdapat kehendak untuk menguasai barang secara tidak sah. Hal ini menunjukkan adanya kesengajaan (*dolus*) yang menjadi dasar penting dalam pertanggungjawaban pidana.

Unsur terakhir adalah “secara melawan hukum”, yang merupakan unsur normatif yang melekat pada setiap tindak pidana. Sifat melawan hukum ini tidak hanya diartikan sebagai bertentangan dengan undang-undang (*formil*), tetapi juga bertentangan dengan rasa keadilan dan norma yang hidup dalam masyarakat (*materiil*). Dalam kasus ini, penggunaan identitas orang lain untuk memperoleh barang atau fasilitas kredit jelas merupakan perbuatan yang tidak sah dan bertentangan dengan hukum. Bahkan jika dilihat secara lebih luas, perbuatan tersebut juga melanggar prinsip kepercayaan dalam transaksi digital, yang menjadi dasar utama dalam sistem *fintech*.

Dengan terpenuhinya seluruh unsur tersebut, maka secara yuridis perbuatan penyalahgunaan *PayLater* oleh pelaku di bawah umur dapat dikualifikasikan sebagai tindak pidana pencurian. Namun, penting untuk dicatat bahwa delik pencurian dalam konteks ini tidak berdiri sendiri, melainkan berkaitan erat dengan delik lain seperti penipuan, pemalsuan, dan penyalahgunaan data pribadi. Hal ini menunjukkan adanya karakter delik berlapis (*multi-layered offense*) yang memperlihatkan kompleksitas kejahatan digital saat ini.

Secara kritis, perlu juga dipertimbangkan bahwa perluasan makna “barang” dalam konteks digital dapat menimbulkan perdebatan dalam praktik penegakan hukum. Tidak semua ahli sepakat bahwa fasilitas kredit atau nilai ekonomi dapat langsung disamakan dengan “barang” dalam pengertian klasik pencurian. Oleh karena itu, dalam beberapa kasus, penegak hukum lebih cenderung menggunakan konstruksi penipuan sebagai delik utama. Meskipun demikian, memasukkan unsur pencurian dalam analisis tetap penting untuk menunjukkan bahwa perbuatan tersebut pada hakikatnya merupakan pengambilan hak milik orang lain secara melawan hukum, terlepas dari medium yang digunakan.

Dengan demikian, dapat disimpulkan bahwa Pasal 476 KUHP tetap relevan untuk digunakan dalam menganalisis penyalahgunaan *PayLater*, selama dilakukan dengan pendekatan interpretasi yang adaptif terhadap perkembangan teknologi. Pendekatan ini diperlukan agar hukum pidana tetap mampu menjawab tantangan kejahatan modern tanpa kehilangan esensi perlindungan terhadap hak milik dan kepentingan hukum masyarakat.

Dalam kasus penyalahgunaan identitas untuk transaksi *PayLater*, penentuan korban tidak dapat dipahami secara sederhana karena tindak pidana ini menimbulkan kerugian terhadap lebih dari satu pihak sekaligus. Korban utama tentu adalah pemilik identitas yang datanya digunakan tanpa izin, karena ia menanggung risiko administratif, kerugian finansial, penurunan reputasi, hingga kemungkinan terjerat tagihan utang yang tidak pernah dibuatnya. Namun demikian, penyedia layanan *PayLater* juga dapat dipandang sebagai korban karena mengalami kerugian ekonomi akibat pemberian kredit berdasarkan data palsu. Selain itu, merchant atau penjual barang yang bekerja sama dengan platform *PayLater* juga berpotensi mengalami kerugian apabila transaksi dibatalkan atau gagal dibayar. Bahkan secara lebih luas, kejahatan semacam ini juga merugikan sistem kepercayaan publik terhadap transaksi digital dan *fintech*. Oleh karena itu, tindak pidana penyalahgunaan identitas dalam *PayLater* memiliki karakter multi-victim crime, yaitu kejahatan yang menimbulkan dampak terhadap banyak pihak sekaligus. Konsep korban yang luas ini penting dipahami agar penyelesaian perkara tidak hanya berorientasi pada penghukuman pelaku, tetapi juga pada pemulihan seluruh pihak yang dirugikan (Arif, 2004).

Selain menimbulkan persoalan pidana, penyalahgunaan identitas dalam transaksi *PayLater* oleh anak juga menimbulkan problematika dalam aspek hukum perdata, khususnya terkait kecakapan hukum untuk membuat perjanjian. Dalam hukum perdata Indonesia, syarat sah perjanjian diatur dalam Pasal 1320 Kitab Undang-Undang Hukum Perdata, yang salah satunya mensyaratkan adanya kecakapan para pihak. Anak yang belum mencapai usia dewasa pada prinsipnya belum memiliki kecakapan penuh untuk melakukan perbuatan hukum, termasuk membuat perjanjian pembiayaan atau utang-piutang. Oleh karena itu, ketika seorang anak mengakses layanan *PayLater* dengan menggunakan identitas orang lain, sebenarnya terdapat cacat sejak awal dalam hubungan hukum yang terbentuk karena pihak yang melakukan transaksi bukanlah subjek hukum yang cakap dan sah.

Dalam konteks ini, penggunaan identitas orang lain oleh anak sering kali dilakukan untuk mengatasi keterbatasan sistem yang mensyaratkan usia minimum pengguna. Hal tersebut menunjukkan bahwa penyalahgunaan identitas bukan hanya didorong oleh niat pelaku, tetapi juga dipengaruhi oleh lemahnya mekanisme verifikasi kecakapan hukum pengguna dalam

sistem digital. Dengan demikian, persoalan penyalahgunaan *PayLater* oleh anak tidak dapat dipahami semata-mata sebagai masalah kriminal individual, melainkan juga sebagai konsekuensi dari lemahnya pengawasan dan validasi hukum dalam transaksi elektronik. Oleh karena itu, perlu adanya integrasi antara perlindungan data pribadi, sistem verifikasi identitas digital, dan pengawasan terhadap kecakapan hukum pengguna agar layanan *fintech* tidak menjadi sarana yang mempermudah anak melakukan perbuatan melawan hukum (Subekti, 2008).

Meskipun berbagai ketentuan pidana tersebut dapat diterapkan, penting untuk dicermati bahwa pelaku dalam konteks ini adalah anak di bawah umur. Oleh karena itu, pertanggungjawaban pidana tidak dapat disamakan dengan orang dewasa. Dalam Undang-Undang Nomor 11 Tahun 2012 tentang Sistem Peradilan Pidana Anak, Pasal 1 angka 3 menyatakan: “Anak yang Berkonflik dengan Hukum yang selanjutnya disebut Anak adalah anak yang telah berumur 12 (dua belas) tahun, tetapi belum berumur 18 (delapan belas) tahun yang diduga melakukan tindak pidana.” Ketentuan ini menegaskan bahwa anak tetap dapat dimintai pertanggungjawaban pidana, namun dengan mekanisme khusus. Salah satu prinsip utama dalam sistem peradilan pidana anak adalah diversifikasi, sebagaimana diatur dalam Pasal 7 yang menyatakan: “(1) Pada tingkat penyidikan, penuntutan, dan pemeriksaan perkara Anak di pengadilan negeri wajib diupayakan Diversifikasi. (2) Diversifikasi sebagaimana dimaksud pada ayat (1) dilaksanakan dalam hal tindak pidana yang dilakukan: a. diancam dengan pidana penjara di bawah 7 (tujuh) tahun; dan b. bukan merupakan pengulangan tindak pidana.” Ketentuan ini menunjukkan bahwa sistem hukum Indonesia lebih mengedepankan pendekatan restoratif dalam menangani anak yang berkonflik dengan hukum, termasuk dalam kasus penyalahgunaan *PayLater*.

Pendekatan perlindungan terhadap anak juga diperkuat dalam Undang-Undang Nomor 35 Tahun 2014 tentang Perlindungan Anak. Dalam Pasal 64 ditegaskan bahwa: “Perlindungan Khusus bagi Anak yang berhadapan dengan hukum sebagaimana dimaksud dalam Pasal 59 ayat (2) huruf b dilakukan melalui: a. perlakuan secara manusiawi dengan memperhatikan kebutuhan sesuai dengan umurnya; b. pemisahan dari orang dewasa; c. pemberian bantuan hukum dan bantuan lain secara efektif; d. pembebasan dari penyiksaan; e. penghindaran dari penjatuh pidana mati; f. penghindaran dari penangkapan, penahanan atau penjara kecuali sebagai upaya terakhir; g. pemberian keadilan di muka pengadilan Anak yang objektif; h. penghindaran dari publikasi atas identitasnya; dan seterusnya.” Ketentuan ini menegaskan bahwa meskipun anak melakukan tindak pidana, negara tetap berkewajiban memberikan perlindungan maksimal terhadap hak-haknya.

Di sisi lain, tanggung jawab tidak hanya berada pada pelaku, tetapi juga pada penyelenggara layanan *PayLater*. Dalam POJK Nomor 10/POJK.05/2022, khususnya Pasal 35 ayat (4), dinyatakan bahwa: “Kegiatan memfasilitasi mitigasi risiko bagi Pengguna paling sedikit: melakukan analisis risiko, melakukan verifikasi identitas Pengguna dan keaslian dokumen, melakukan penagihan, memfasilitasi pengalihan risiko, dan lain-lain.” Ketentuan ini menunjukkan bahwa penyelenggara memiliki kewajiban untuk memastikan keabsahan identitas pengguna. Apabila verifikasi dilakukan secara lemah, maka potensi penyalahgunaan akan semakin besar. Dengan demikian, dalam analisis hukum, perlu juga dipertimbangkan aspek kelalaian (*negligence*) dari penyelenggara.

Dalam praktiknya, berbagai kasus penyalahgunaan identitas pada layanan *PayLater* menunjukkan bahwa kelemahan sistem verifikasi elektronik (*electronic Know Your Customer/e-KYC*) masih menjadi persoalan serius dalam industri fintech. Banyak platform hanya mengandalkan unggahan foto KTP dan verifikasi swafoto (*selfie verification*) tanpa pemeriksaan mendalam terhadap kecocokan identitas maupun usia pengguna. Bahkan dalam beberapa kasus, sistem verifikasi masih dapat dilewati dengan menggunakan foto identitas milik orang lain atau manipulasi gambar digital. Kondisi ini memperlihatkan bahwa penyelenggara layanan belum sepenuhnya menerapkan prinsip kehati-hatian (*prudential principle*) dan mitigasi risiko sebagaimana diwajibkan dalam regulasi Otoritas Jasa Keuangan.

Selain itu, lemahnya *age verification* dalam sistem *PayLater* turut membuka peluang bagi anak di bawah umur untuk mengakses fasilitas kredit secara tidak sah. Padahal, transaksi pembiayaan digital memiliki risiko hukum dan finansial yang tinggi apabila dilakukan oleh pihak yang belum cakap hukum. Oleh karena itu, penyelenggara tidak dapat sepenuhnya melepaskan tanggung jawab dengan alasan bahwa seluruh kesalahan berada pada pengguna. Dalam perspektif kriminologi, lemahnya sistem pengawasan dan keamanan digital dapat dikategorikan sebagai faktor kriminogen, yaitu kondisi yang mempermudah terjadinya tindak pidana. Dengan kata lain, sistem elektronik yang mudah dimanipulasi secara tidak langsung turut berkontribusi terhadap terjadinya penyalahgunaan identitas dalam transaksi *PayLater*.

Dari sudut pandang perlindungan konsumen dan tata kelola teknologi keuangan, penyelenggara seharusnya menerapkan sistem verifikasi berlapis, seperti validasi biometrik yang lebih ketat, sinkronisasi dengan data kependudukan, pendeteksian usia pengguna, serta pengawasan terhadap aktivitas transaksi mencurigakan. Kegagalan menerapkan sistem pengamanan yang memadai dapat menimbulkan tanggung jawab hukum bagi penyelenggara, baik dalam bentuk tanggung jawab administratif maupun tanggung jawab perdata apabila kelalaian tersebut mengakibatkan kerugian bagi pengguna maupun pihak ketiga. Dengan

demikian, analisis hukum terhadap penyalahgunaan *PayLater* tidak boleh hanya berfokus pada pelaku anak, tetapi juga harus mempertimbangkan sejauh mana sistem digital yang disediakan penyelenggara telah memenuhi standar perlindungan hukum dan keamanan elektronik yang memadai(2014).

Dari perspektif teori hukum pidana, perbuatan anak yang menggunakan identitas orang lain dalam *PayLater* dapat dianalisis melalui konsep *mens rea* (niat jahat) dan *actus reus* (perbuatan). Menurut Muladi dan Barda Nawawi Arief dalam *Teori-Teori dan Kebijakan Pidana*, pertanggungjawaban pidana mensyaratkan adanya kesalahan yang dapat berupa kesengajaan atau kealpaan(Arief, 2010). Dalam konteks ini, anak yang secara sadar menggunakan identitas orang lain untuk memperoleh keuntungan dapat dikatakan memiliki unsur kesengajaan. Namun, tingkat kesalahan tersebut harus dinilai dengan mempertimbangkan faktor usia, tingkat kedewasaan, serta lingkungan sosial anak.

Meskipun anak belum memiliki tingkat kedewasaan yang sama dengan orang dewasa, hal tersebut tidak secara otomatis menghapus keberadaan *mens rea* dalam tindak pidana yang dilakukannya. Dalam doktrin hukum pidana, *mens rea* berkaitan dengan kemampuan pelaku untuk memahami sifat perbuatannya serta akibat yang mungkin ditimbulkan. Dalam kasus penyalahgunaan *PayLater*, anak umumnya mengetahui bahwa identitas yang digunakan bukan miliknya dan memahami bahwa penggunaan identitas tersebut dilakukan agar sistem memberikan akses kredit. Kesadaran tersebut menunjukkan adanya bentuk kesengajaan, setidaknya dalam bentuk *dolus eventualis* maupun *dolus directus*. Namun demikian, tingkat kesalahan anak harus tetap dinilai secara proporsional dengan mempertimbangkan aspek psikologis, perkembangan emosional, pengaruh lingkungan sosial, serta tingkat literasi digital dan finansial yang dimiliki anak. Oleh karena itu, keberadaan *mens rea* pada anak tidak dapat disamakan secara absolut dengan orang dewasa, melainkan harus dianalisis secara individual berdasarkan kondisi konkret pelaku. Pendekatan ini sejalan dengan prinsip kepentingan terbaik bagi anak (*best interests of the child*) dalam sistem peradilan pidana anak(2009)

5. KESIMPULAN DAN SARAN

Kesimpulan

Penggunaan identitas orang lain dalam transaksi *PayLater* oleh anak di bawah umur merupakan perbuatan yang memiliki dimensi hukum pidana karena dilakukan melalui penggunaan identitas pihak lain tanpa hak untuk memperoleh fasilitas pembiayaan digital. Berdasarkan analisis terhadap unsur-unsur tindak pidana dalam Kitab Undang-Undang Hukum Pidana, Undang-Undang Informasi dan Transaksi Elektronik, dan Undang-Undang Nomor 27

Tahun 2022 tentang Perlindungan Data Pribadi, perbuatan tersebut dapat dikaitkan dengan beberapa ketentuan pidana yang mengatur penyalahgunaan data pribadi, manipulasi informasi elektronik, dan pemalsuan identitas.

Meskipun demikian, **kualifikasi tindak pidana yang paling tepat** terhadap penggunaan identitas orang lain dalam transaksi PayLater adalah **tindak pidana penipuan**, karena sejak awal pelaku menggunakan identitas pihak lain sebagai sarana untuk memperoleh fasilitas pembiayaan melalui rangkaian tipu muslihat yang mengakibatkan kerugian bagi pemilik identitas maupun penyelenggara layanan PayLater. Sementara itu, ketentuan mengenai penyalahgunaan data pribadi, manipulasi informasi elektronik, dan pemalsuan tidak berdiri sebagai delik utama, melainkan merupakan konstruksi hukum yang memperkuat karakteristik perbuatan sebagai kejahatan berbasis teknologi digital.

Dengan demikian, penentuan kualifikasi tindak pidana terhadap penggunaan identitas orang lain dalam transaksi PayLater tidak cukup dilakukan melalui pendekatan sektoral berdasarkan satu peraturan perundang-undangan, tetapi harus menggunakan pendekatan yang komprehensif dengan memperhatikan hubungan antara hukum pidana umum dan ketentuan pidana khusus di bidang teknologi informasi serta perlindungan data pribadi.

Saran

Disarankan untuk memperkuat regulasi yang secara spesifik mengatur penggunaan layanan keuangan digital oleh anak-anak di bawah umur, termasuk memperjelas batasan akses serta mekanisme pengawasan terhadap penggunaan teknologi finansial. Selain itu, diperlukan harmonisasi antara peraturan perundang-undangan yang berkaitan dengan hukum pidana, perlindungan data pribadi, dan sistem peradilan pidana anak guna menciptakan kepastian hukum yang lebih komprehensif.

DAFTAR REFERENSI

- Arif, G. (2004). *Masalah korban kejahatan: Kumpulan Karangan*. Bhuna Ilmu Populer.
- Aryani, A. P., & Susanti, L. E. (2022). Pentingnya Perlindungan Data Pribadi Konsumen dalam Transaksi Online pada Marketplace terhadap Kepuasan Konsumen. *Ahmad Dahlan Legal Perspective*, 2(1), 20–29. <https://doi.org/10.12928/adlp.v2i1.5610>
- Chazawi, Adami. (2011). *Pelajaran Hukum Pidana Bagian I*. Jakarta: Rajawali Pers.
- Fajriansyah, A., Siregar, R. A., & Panggabean, M. L. (n.d.). *Reformasi Hukum Pidana Di Era Digital: Analisis Terhadap KUHP Baru*.
- Hanafi, M. (2015). *Sistem Pertanggungjawaban Pidana*. Jakarta: Rajawali Pers.

- Irawati. (2025). *“Utang PayLater Warga RI di Bank Tembus Rp24,33 Triliun per Agustus 2025.”* Jakarta.
- Marlina. (2009). *Peradilan pidana anak di Indonesia: Pengembangan konsep diversi dan restorative justice*. Refika Aditama.
- Marzuki, P. M. (2019). *Penelitian Hukum*. Jakarta: Kencana Prenada Media Group.
- Maskun. (2014). *Kejahatan siber (cyber crime): Suatu pengantar*. Jakarta: Kencana.
- Mertha, I. K., & Gusti, A. (2016). *Buku Ajar Hukum Pidana*. Denpasar: Fakultas Hukum Universitas Udayana.
- Miski, Y. R. A., Putra, S. M., Purwanto, M. I., & Luthfiyyah, S. (2025). EKSISTENSI TINDAK PIDANA PENIPUAN (BEDROG) DALAM PASAL 378 KUHP DI ERA DIGITAL. *Journal Equitable*, 10(2). <https://doi.org/https://doi.org/10.37859/jeq.v10i2.9072>
- Muladi, & Arief, B. N. (2010). *Teori-teori dan Kebijakan Pidana*. Bandung: Alumni.
- Nurfitri, A. R., Setyaningsih, E., & Gunadarma, U. (n.d.). *Fenomena Peningkatan Penggunaan Paylater di Indonesia dan Dampaknya Terhadap Perilaku Masyarakat*.
- Oktafiani, R., Trisnawati, S. E., Maymunah, S., & Paridah, S. (2024). Mini Research Teknologi Keuangan Syariah Identitas Digital Vs kejahatan Siber (Studi Intensitas Kasus dan Pola Kejahatan Siber Melalui Platform Digital). *Journal of Sharia Economic Law*, 2(1), 23–34. <https://doi.org/10.37680/jshel.v2i1.5755>
- Otniel Purba, Y., & Mauluddin, A. (2023). Kejahatan Siber dan Kebijakan Identitas Kependudukan Digital: Sebuah Studi Tentang Potensi Pencurian Data Online. *JCIC : Jurnal CIC Lembaga Riset dan Konsultan Sosial*, 5(2), 55–66. <https://doi.org/10.51486/jbo.v5i2.113>
- Panjalu, D. A. (2022). *ANALISIS PENGARUH MINAT PENGGUNA FITUR PAYLATER PADA APLIKASI SHOPEE* (D4 Thesis). Politeknik Negeri Jakarta, Jakarta.
- Pertiwi, E., Nuraldini, D. D., Buana, G. T., & Arthacerses, A. (n.d.). *Analisis Yuridis Terhadap Penyalahgunaan Data Pribadi Pengguna Media Sosial*.
- Prasanti, I. G. A. A. W., Kurniawan, & Munandar, A. (2024). *PELAKSANAAN TRANSAKSI BUY NOW PAY LATER PADA E-COMMERCE DI KOTA MATARAM*. 12(3). <https://doi.org/0.37081/ed.v12i3.6622>
- Putri, A. P. Y., Miru, A., & Maskun. (2020). Praktik Penyalahgunaan Fitur Kredit (Paylater) oleh Pihak Ketiga melalui Aplikasi Belanja Online. *Amanna Gappa*.
- Rosyadi, I. (2022). *Hukum Pidana*. Surabaya: Revka Prima Media.
- Sa'idah, A. (2024). *TRANSAKSI KREDIT SHOPEE PAYLATER OLEH ANAK DI BAWAH UMUR PERSPEKTIF HUKUM PERJANJIAN DI INDONESIA* (Skripsi). UIN Syarif Hidayatullah Jakarta, Jakarta.
- Saleh, R. (1983). *Perbuatan Pidana dan Pertanggungjawaban Pidana; Dua pengertian Dasar dalam Hukum Pidana*. Jakarta: Aksara Baru.
- Setiady, T. (2010). *Pokok-Pokok Hukum Panitensier Indonesia*. Bandung: Alfabeta.
- Siantury, S. (1998). *Asas-Asas Hukum Pidana dan Penerapannya di Indonesia*. Jakarta: Alumni AHAEM PTHAEM.

- Subekti, R. (2008). *Hukum Perjanjian*. Jakarta: Intermasa.
- Syam, N. A., & Fatwa, S. (n.d.). *INTEGRASI LAYANAN FINTECH DALAM PLATFORM E-COMMERCE: STUDI KASUS PENGGUNAAN PAYLATER PADA GENERASI Z*. 10(1).
- Tampubolon, A. D. H., & Wiryadi, U. (2025). *Tindak Pidana Pencurian Data Elektronik Ditinjau Berdasarkan Undang-Undang ITE*. 3.
- Widodo. (2019). *Hukum pidana di bidang teknologi informasi cybercrime law*. Yogyakarta: Aswaja Pressindo.