Al-Zayn: Jurnal Ilmu Sosial & Hukum e-ISSN 3026-2917
https://ejournal.yayasanpendidikandzurriyatulquran.id/index.php/AlZyn p-ISSN 3026-2925
Volume 4 Number 2, 2026
DOI: https://doi.org/10.61104/alz.v4i2.5005

Pencurian Identitas Digital sebagai Bentuk Kejahatan Pendahuluan dalam Cybercrime

Angelica Suciara[1], Darrel Michelin[2], Giovano Allan Loway[3], Grace Amaze Huberta[4], kimberly Fewsan[5], M. Almer Fathoni[6], Meiraate Leos Lediana Tombeg[7], Michelle Regine Maukar[8], Muhammad Bintang Guntoro[9]
Universitas Pelita Harapan, Indonesia[1-9]
Email Korespondensi: 01051230167@student.uph.edu, 01051230097@student.uph.edu, 01051230104@student.uph.edu, 01051230042@student.uph.edu, 01051230022@student.uph.edu, 01051230201@student.uph.edu, 01051230119@student.uph.edu, 01051230010@student.uph.edu, 01051230194@student.uph.edu

Article received: 01 Januari 2026, Review process: 12 Januari 2026
Article Accepted: 22 Februari 2026, Article published: 16 Maret 2026

ABSTRACT
The development of information technology has driven the transformation of identity data from physical forms into digital formats integrated within electronic systems. Digital identity, which encompasses population data, account credentials, and financial information, now possesses significant economic value and is therefore highly vulnerable to misuse. The phenomenon of identity theft in Indonesia has shown a substantial increase in line with the rapid digitalization of financial services, e-commerce platforms, and online communication services. In contemporary practice, identity theft no longer stands as an isolated criminal offense; rather, it functions as an entry crime within a broader chain of cybercrimes, such as online fraud and money laundering. Normatively, the protection of personal data and electronic systems in Indonesia is regulated under the Law on Electronic Information and Transactions and the Personal Data Protection Law. However, there is no explicit legal provision that classifies identity theft as a distinct criminal offense. This absence creates a gap in legal certainty, particularly in the construction of criminal liability. This research employs a normative legal method using statutory and conceptual approaches. The findings indicate that identity theft possesses the characteristics of an entry crime within the structure of modern cybercrime. Accordingly, a more systematic legal framework is required to ensure legal certainty, enhance the effectiveness of law enforcement, and provide adequate protection for victims.
Keywords: *Identity theft, entry crime, criminal liability.*

ABSTRAK
Perkembangan teknologi informasi telah mendorong transformasi data identitas dari bentuk fisik menjadi digital yang terintegrasi dalam sistem elektronik. Identitas digital yang meliputi data kependudukan, kredensial akun, serta informasi finansial yang kini memiliki nilai ekonomi tinggi membuatnya menjadi rentan disalahgunakan. Fenomena pencurian identitas (Identity theft) di Indonesia menunjukkan peningkatan signifikan seiring dengan masifnya digitalisasi layanan keuangan, e-commerce, dan platform komunikasi daring. Dalam fenomena sekarang, pencurian identitas tidak lagi berdiri sebagai tindak pidana tunggal melainkan berfungsi sebagai entry crime dalam rangkaian kejahatan siber, seperti

penipuan daring dan tindak pidana pencucian uang. Secara normatif, perlindungan terhadap data pribadi dan sistem elektronik diatur dalam Undang-Undang Informasi dan Transaksi Elektronik serta Undang-Undang Perlindungan Data Pribadi. Namun belum terdapat pengaturan yang secara eksplisit yang mengkualifikasikan pencurian identitas sebagai delik tersendiri yang menyebabkan adanya kekosongan kepastian hukum dalam konstruksi pertanggungjawaban pidana. Penelitian ini menggunakan metode hukum normatif dengan pendekatan perundang-undangan dan konseptual. Hasil kajian menunjukkan bahwa pencurian identitas memiliki karakter sebagai entry crime dalam struktur kejahatan siber modern, sehingga memerlukan konstruksi hukum yang lebih sistematis guna menjamin kepastian hukum, efektivitas penegakan hukum, dan perlindungan korban.
Kata kunci: *Pencurian identitas, entry crime dan pertanggungjawaban pidana*

PENDAHULUAN

Perkembangan teknologi informasi telah membawa transformasi fundamental dalam struktur kehidupan sosial dan ekonomi masyarakat. Berbagai aspek aktivitas manusia kini berbasis digital dan terintegrasi dalam sistem elektronik. Data kependudukan, kredensial akun, rekam jejak transaksi, hingga informasi finansial tersimpan dan diproses dalam infrastruktur digital yang saling terhubung. Transformasi ini memang meningkatkan efisiensi pelayanan publik dan mempercepat pertumbuhan ekonomi digital, namun pada saat yang sama memperluas kerentanan terhadap penyalahgunaan data pribadi yang tersimpan dalam sistem elektronik. Dalam beberapa tahun terakhir, Indonesia mengalami peningkatan signifikan kasus kebocoran dan penyalahgunaan data pribadi. Berdasarkan survei oleh Asosiasi Penyelenggara Jasa Internet Indonesia, kebocoran data pribadi pada tahun 2024 mencapai 20,8 persen, meningkat sekitar 8 persen dibandingkan tahun sebelumnya. Data ini menunjukkan bahwa hampir seperlima pengguna internet di Indonesia pernah terdampak insiden kebocoran informasi pribadi, baik dalam bentuk peretasan akun, pencurian identitas, maupun penyalahgunaan data untuk kepentingan kriminal.

Fenomena tersebut juga diperkuat oleh berbagai kasus kebocoran data berskala besar, seperti insiden pada Tokopedia dan BPJS Kesehatan, yang melibatkan jutaan data pengguna. Selain itu, laporan dari Kementerian Komunikasi dan Informatika Republik Indonesia menunjukkan bahwa mayoritas insiden siber di Indonesia berkaitan dengan lemahnya sistem pengamanan data dan rendahnya kesadaran keamanan digital pengguna. Kondisi ini memperlihatkan bahwa kebocoran data bukan lagi peristiwa insidental, melainkan telah menjadi pola sistemik dalam ekosistem digital nasional.

Peningkatan kebocoran data tersebut tidak terlepas dari masifnya digitalisasi layanan perbankan, fintech, e-commerce, serta platform komunikasi daring yang menjadikan data identitas sebagai komoditas bernilai ekonomi tinggi di pasar gelap digital. Data pribadi yang diperoleh secara ilegal sering diperjualbelikan dalam forum daring untuk digunakan dalam berbagai tindak pidana lanjutan, seperti penipuan daring, pembobolan rekening, pinjaman online ilegal, hingga pemalsuan

identitas. Dengan demikian, pencurian identitas berfungsi sebagai *entry crime* yang membuka akses bagi pelaku terhadap rangkaian kejahatan siber berikutnya. Pola ini menunjukkan adanya pergeseran karakter kejahatan dari yang bersifat individual dan oportunistik menuju kejahatan terorganisasi berbasis teknologi. Pelaku tidak lagi hanya memanfaatkan kelemahan korban secara personal, melainkan mengeksploitasi celah sistemik dalam pengelolaan data. Sementara itu, dari perspektif yuridis, meningkatnya kasus pencurian identitas menandakan bahwa perlindungan data pribadi tidak lagi sekadar persoalan administratif, tetapi telah berkembang menjadi isu hukum pidana yang kompleks, yang berkaitan dengan pertanggungjawaban korporasi, keamanan sistem elektronik, serta efektivitas penegakan hukum siber.

Tingginya angka kebocoran data dan maraknya penyalahgunaan identitas digital memperlihatkan bahwa pencurian identitas merupakan titik awal strategis dalam mata rantai kejahatan siber di Indonesia. Kondisi ini menuntut penguatan regulasi, peningkatan standar keamanan sistem elektronik, serta pengembangan kapasitas aparat penegak hukum agar mampu memutus rantai kejahatan sejak tahap awal terjadinya pelanggaran data.

Salah satu bentuk kejahatan yang berkembang pesat dalam ruang siber adalah pencurian identitas (*identity theft*). Secara konseptual, pencurian identitas berfokus pada pengambilalihan, penguasaan, atau penggunaan tanpa hak atas data identitas seseorang untuk tujuan tertentu. Dalam praktiknya, pelaku memanfaatkan data tersebut untuk mengakses layanan keuangan, membuat akun palsu, mengajukan pinjaman daring, hingga melakukan transaksi ilegal atas nama korban. Akibatnya, korban tidak hanya menanggung kerugian materiil berupa kehilangan aset dan beban utang, tetapi juga kerugian immateriil berupa rusaknya reputasi, tekanan psikologis, serta menurunnya kepercayaan terhadap sistem digital.

Dari perspektif normatif, perlindungan terhadap data pribadi dan sistem elektronik di Indonesia pada dasarnya telah diatur melalui Undang-Undang Informasi dan Transaksi Elektronik serta Undang-Undang Perlindungan Data Pribadi yang dibentuk oleh Dewan Perwakilan Rakyat Republik Indonesia bersama pemerintah. Regulasi tersebut mengatur larangan akses ilegal, manipulasi data, distribusi informasi tanpa hak, serta kewajiban perlindungan data oleh penyelenggara sistem elektronik yang berada di bawah pembinaan Kementerian Hukum dan Hak Asasi Manusia Republik Indonesia dan kementerian terkait.

Kedua undang-undang tersebut belum memuat rumusan delik yang secara eksplisit mengkualifikasikan pencurian identitas sebagai tindak pidana mandiri. Ketentuan yang ada masih bersifat fragmentaris, yaitu tersebar dalam pasal-pasal mengenai akses ilegal, perusakan sistem elektronik, atau penyalahgunaan data. Akibatnya, penegakan hukum terhadap pelaku pencurian identitas seringkali bergantung pada konstruksi pasal lain yang tidak secara spesifik merepresentasikan karakter kejahatan tersebut. Ketiadaan delik khusus ini menimbulkan problematika dalam konstruksi pertanggungjawaban pidana. Dalam banyak kasus, pencurian identitas hanya diposisikan sebagai perbuatan pendahuluan (*preparatory act*) yang melebur dalam tindak pidana lanjutan, seperti penipuan, pencucian uang, atau

pembobolan rekening. Kondisi ini berpotensi melemahkan efek jera, karena fokus penegakan hukum lebih diarahkan pada kejahatan akhir, sementara perbuatan awal berupa penguasaan identitas ilegal kurang memperoleh perhatian proporsional.

Pencurian identitas berfungsi sebagai *entry crime* yang memungkinkan pelaku membangun akses terhadap berbagai sistem dan sumber daya digital. Tanpa adanya penguasaan identitas korban, sebagian besar kejahatan siber lanjutan tidak dapat dilakukan secara efektif. Oleh karena itu, lemahnya pengaturan khusus terhadap pencurian identitas menunjukkan adanya celah struktural dalam sistem hukum pidana siber di Indonesia. Belum diaturnya pencurian identitas sebagai delik tersendiri mencerminkan kebutuhan akan pembaruan kebijakan hukum pidana yang lebih adaptif terhadap karakter kejahatan digital. Penguatan regulasi melalui perumusan delik khusus pencurian identitas menjadi penting untuk memastikan kepastian hukum, efektivitas penegakan, serta perlindungan optimal bagi korban dalam ekosistem digital nasional.

Dalam praktiknya *identity theft* kerap berperan sebagai *entry crime* dalam rangkaian kejahatan siber. Data identitas yang diperoleh secara ilegal digunakan sebagai sarana untuk melakukan penipuan daring, pengajuan kredit fiktif, pembukaan rekening penampung dana, hingga tindak pidana pencucian uang. Dengan demikian, pencurian identitas tidak berdiri sebagai kejahatan tunggal, melainkan menjadi kejahatan awal bagi serangkaian kejahatan lanjutan yang menimbulkan kerugian ekonomi dan sosial yang lebih luas. Berdasarkan uraian tersebut, timbul pertanyaan mendasar mengenai bagaimana karakteristik pencurian identitas dalam kejahatan siber, apakah pencurian identitas dapat dikualifikasikan sebagai *entry crime* dalam struktur kejahatan siber modern, serta bagaimana konstruksi pertanggungjawaban pidana terhadap pelaku dalam rangkaian kejahatan tersebut. Pertanyaan-pertanyaan inilah yang menjadi fokus kajian dalam penelitian ini guna mendorong pembentukan konstruksi hukum yang lebih sistematis demi menjamin kepastian hukum, efektivitas penegakan hukum, dan perlindungan yang optimal bagi korban.

METODE

Penelitian ini menggunakan metode penelitian hukum normatif yaitu penelitian yang bertumpu pada analisis norma hukum positif yang berlaku serta konsep-konsep hukum yang berkembang dalam doktrin. Pendekatan ini dipilih karena fokus penelitian terletak pada konstruksi yuridis pencurian identitas sebagai *entry crime* dalam rangkaian kejahatan siber serta implikasinya terhadap pertanggungjawaban pidana. Pendekatan yang digunakan adalah pendekatan perundang-undangan dan pendekatan konseptual. Pendekatan perundang-undangan dilakukan dengan menelaah ketentuan dalam Undang-Undang Informasi dan Transaksi Elektronik, Undang-Undang Perlindungan Data Pribadi, serta peraturan lain yang relevan dengan kejahatan siber dan pertanggungjawaban pidana. Sementara itu, pendekatan konseptual digunakan untuk menganalisis konsep pencurian identitas, *entry crime*, dan teori pertanggungjawaban pidana dalam doktrin hukum pidana.

Bahan hukum yang digunakan terdiri atas bahan hukum primer berupa peraturan perundang-undangan, serta bahan hukum sekunder seperti buku dan jurnal ilmiah yang relevan. Seluruh bahan hukum dikumpulkan melalui studi kepustakaan dan dianalisis secara kualitatif untuk mengidentifikasi kekosongan norma serta merumuskan konstruksi hukum yang tepat terkait pertanggungjawaban pidana dalam kasus pencurian identitas sebagai bagian dari kejahatan siber modern.

HASIL DAN PEMBAHASAN

Karakteristik Pencurian Identitas dalam Praktik Kejahatan Siber

Pencurian data identitas merupakan salah satu bentuk kejahatan siber (*cyber crime*) yang semakin marak seiring dengan pesatnya perkembangan teknologi informasi dan meningkatnya ketergantungan masyarakat terhadap layanan digital. Dalam ekosistem digital yang terhubung, setiap aktivitas pengguna mulai dari komunikasi, transaksi ekonomi, hingga administrasi publik meninggalkan jejak data yang berpotensi disalahgunakan apabila tidak dilindungi secara memadai. Berdasarkan pemantauan keamanan siber oleh Badan Siber dan Sandi Negara, sebagian besar insiden kebocoran data di Indonesia terjadi akibat lemahnya sistem keamanan, praktik pengelolaan data yang tidak standar, serta rendahnya literasi keamanan digital pengguna. Kondisi ini diperparah oleh maraknya aplikasi dan situs web yang tidak terverifikasi, sehingga membuka peluang bagi pelaku untuk melakukan phishing, malware injection, dan peretasan sistem.

Dalam praktiknya, pencurian identitas tidak hanya terbatas pada pengambilan data dasar seperti nama, alamat, atau nomor identitas, tetapi telah berkembang pada penguasaan aset digital bernilai ekonomi tinggi. Data yang menjadi target utama meliputi nomor rekening, informasi kartu debit dan kredit, kredensial perbankan digital, akun dompet elektronik, serta akses ke platform keuangan. Data tersebut kemudian dimanfaatkan untuk melakukan transaksi ilegal, penipuan daring, pinjaman online fiktif, hingga pencucian uang. Karakteristik utama pencurian identitas dalam kejahatan siber modern adalah sifatnya yang sistematis dan terorganisasi. Pelaku tidak lagi bertindak secara individual, melainkan membangun jaringan yang mencakup peretas, penjual data ilegal, serta pelaku kejahatan lanjutan. Data hasil pencurian sering diperjualbelikan melalui forum gelap daring (*dark web*), sehingga memperluas dampak kejahatan terhadap korban.

Selain itu, pencurian identitas juga memiliki karakter laten dan berjangka panjang. Dalam banyak kasus, korban tidak langsung menyadari bahwa identitasnya telah disalahgunakan, karena data dapat disimpan dan dimanfaatkan kembali dalam waktu yang lama. Akibatnya, kerugian yang dialami korban tidak hanya bersifat finansial, tetapi juga mencakup kerusakan reputasi, gangguan psikologis, serta kesulitan administratif di kemudian hari. Dari perspektif pengawasan dan pembinaan sistem elektronik, Kementerian Komunikasi dan Informatika Republik Indonesia menekankan pentingnya penerapan standar keamanan data oleh penyelenggara sistem elektronik. Namun, dalam praktiknya,

masih banyak penyelenggara yang belum menerapkan sistem perlindungan secara optimal, sehingga menjadikan data pengguna sebagai objek yang rentan terhadap eksploitasi.

Pencurian identitas dalam kejahatan siber memiliki karakteristik utama berupa eksploitasi kelemahan sistem, penguasaan aset digital bernilai ekonomi, pola kejahatan terorganisasi, serta dampak jangka panjang bagi korban. Karakteristik ini menunjukkan bahwa pencurian identitas bukan sekadar pelanggaran privasi, melainkan merupakan instrumen strategis dalam membangun rangkaian kejahatan siber yang lebih kompleks dan merugikan.

Salah satu modus operandi yang paling umum digunakan dalam pencurian identitas adalah *phishing*. *Phishing* merupakan aktivitas pengiriman pesan palsu melalui email, WhatsApp, SMS, atau media komunikasi digital lainnya dengan tujuan memancing korban untuk mengakses tautan tertentu. Tautan tersebut biasanya dirancang menyerupai situs resmi lembaga, perusahaan, atau layanan digital terpercaya. Ketika korban mengaksesnya dan memasukkan data pribadi, informasi tersebut secara otomatis terekam dan dikuasai oleh pelaku. Di Indonesia, modus *phishing* berkembang dengan memanfaatkan isu-isu yang dekat dengan kehidupan masyarakat, seperti pemberitahuan pengiriman paket, undangan pernikahan digital, informasi bantuan sosial, hingga notifikasi akun bermasalah. Berdasarkan pemantauan Badan Siber dan Sandi Negara, pola phishing semacam ini termasuk dalam kategori serangan berbasis manipulasi psikologis yang tingkat keberhasilannya relatif tinggi karena memanfaatkan rasa penasaran dan kepercayaan korban.

Selain *phishing*, modus lain yang sering digunakan adalah rekayasa sosial (*social engineering*). Dalam modus ini, pelaku secara aktif berinteraksi dengan korban untuk membangun kepercayaan atau menciptakan tekanan emosional, baik melalui rasa senang, takut, maupun cemas. Pelaku kemudian meminta informasi rahasia, seperti kode OTP (*One Time Password)*, PIN, atau kata sandi akun. Dengan menguasai informasi tersebut, pelaku dapat mengambil alih akun korban dan melanjutkan ke tahap kejahatan berikutnya, seperti pembobolan rekening atau penyalahgunaan identitas digital. Modus berikutnya adalah SIM *Swap*, yaitu pengambilalihan kartu SIM milik korban dengan cara memanipulasi operator seluler atau memalsukan identitas. Setelah kartu SIM berhasil dikuasai, pelaku dapat menerima seluruh pesan dan panggilan yang seharusnya diterima korban, termasuk kode verifikasi berbasis SMS. Hal ini memungkinkan pelaku menembus sistem autentikasi dua faktor (*two-factor authentication*/2FA) dan mengakses berbagai layanan digital korban secara ilegal. Menurut Kementerian Komunikasi dan Informatika Republik Indonesia, modus SIM Swap merupakan salah satu ancaman serius terhadap keamanan transaksi digital karena dapat meniadakan fungsi proteksi berlapis.

Setelah data pribadi berhasil diperoleh melalui berbagai modus tersebut, pelaku tidak serta-merta menggunakannya secara langsung. Data hasil kejahatan biasanya disimpan, diklasifikasikan, dan diperjualbelikan melalui pasar gelap digital (*dark web*). Data ini kemudian dimanfaatkan kembali oleh pihak lain untuk

berbagai tindak pidana lanjutan, seperti penipuan daring, pemalsuan identitas, pinjaman ilegal, hingga pencucian uang. Pola ini menunjukkan bahwa pencurian identitas telah menjadi bagian dari ekosistem kejahatan siber yang terorganisasi dan berorientasi ekonomi. Modus operandi pencurian identitas dalam praktik kejahatan siber di Indonesia ditandai oleh penggunaan teknik manipulasi psikologis, eksploitasi kelemahan sistem autentikasi, serta pemanfaatan jaringan perdagangan data ilegal. Karakteristik ini mempertegas bahwa pencurian identitas bukan sekadar kejahatan individual, melainkan merupakan tahap strategis dalam rangkaian kejahatan siber yang kompleks dan berkelanjutan.

Pencurian Identitas sebagai Entry Crime

Pencurian identitas sebagai *entry crime* dalam kejahatan siber umumnya berlangsung melalui beberapa tahapan yang saling berkaitan. Tahap awal yang paling menentukan adalah pengambilan data (*data harvesting*), yaitu proses pengumpulan informasi pribadi korban dari berbagai sumber, baik yang bersifat publik maupun privat. Pada tahap ini, pelaku berupaya membangun basis data awal yang akan digunakan sebagai fondasi untuk melakukan kejahatan lanjutan. Sumber data yang dieksploitasi oleh pelaku dapat berasal dari kebocoran basis data lembaga, perusahaan, maupun instansi pemerintah, termasuk data kependudukan yang dikelola oleh Direktorat Jenderal Kependudukan dan Pencatatan Sipil Kementerian Dalam Negeri. Selain itu, pelaku juga memanfaatkan informasi yang secara sukarela dipublikasikan oleh pengguna di media sosial dan *platform* digital.

Dalam praktiknya, salah satu teknik utama yang digunakan pada tahap ini adalah *scraping* media sosial. *Scraping* merupakan teknik pengambilan data secara otomatis dari platform digital melalui program komputer, bot, atau antarmuka pemrograman aplikasi (*Application Programming Interface/API*), serta pemrosesan struktur HTML (*web parsing*). Melalui teknik ini, pelaku dapat mengumpulkan data dalam jumlah besar dari platform yang berada di bawah naungan Meta *Platforms*, Inc., seperti profil pengguna, foto, nomor kontak, hingga relasi sosial, tanpa sepengetahuan pemilik data. Pada tahap fondasi ini, data yang menjadi target utama meliputi Nomor Induk Kependudukan (NIK), nama lengkap, foto KTP, nomor telepon, alamat surel, serta informasi pendukung lainnya. Kumpulan data tersebut memiliki nilai strategis tinggi karena dapat digunakan untuk melakukan verifikasi identitas pada berbagai layanan digital, khususnya layanan keuangan, perbankan, dan administrasi publik.

Tahap *data harvesting* berfungsi sebagai proses pemetaan korban (*victim profiling*). Dengan menguasai data dasar tersebut, pelaku dapat menyusun profil digital korban secara komprehensif, sehingga mempermudah proses manipulasi, pembobolan akun, maupun penyamaran identitas pada tahap berikutnya. Semakin lengkap data yang diperoleh, semakin tinggi pula peluang keberhasilan kejahatan lanjutan. Selain itu, karakteristik utama tahap ini adalah sifatnya yang masif dan berulang. Pelaku tidak hanya menargetkan satu individu, melainkan mengumpulkan ribuan hingga jutaan data sekaligus untuk membangun "bank data

ilegal". Data tersebut kemudian diseleksi sesuai kebutuhan, baik untuk digunakan sendiri maupun diperjualbelikan di pasar gelap digital.

Tahap *data harvesting* merupakan fondasi utama dalam konstruksi pencurian identitas sebagai *entry crime*. Penguasaan data dasar seperti NIK, identitas visual, dan nomor komunikasi menjadikan pelaku memiliki akses awal yang sangat kuat untuk menembus sistem digital korban. Tanpa keberhasilan pada tahap ini, rangkaian kejahatan siber lanjutan sulit dilakukan secara efektif, sehingga penguatan perlindungan data pada level awal menjadi kunci dalam memutus mata rantai kejahatan identitas.

Pada tahap yang kedua yaitu penyalahgunaan identitas atau *weaponization*, setiap data yang sudah didapatkan akan dipergunakan sebagai alat kejahatan. Cara kerjanya adalah melalui manipulasi sistem dengan menggunakan foto KTP korban untuk melewati proses verifikasi di aplikasi aset korban. Kemudian, pelaku kejahatan akan mengakses isi rekening bank atau *e-wallet* atas nama korban, tanpa diketahui pemilik maupun korban. Setelah itu, pelaku menggunakan NIk curian untuk meregistrasi ribuan kartu perdana yang akan digunakan untuk menyebarkan SMS penipuan ataupun spam.

Tahap yang ketiga yaitu kejahatan utama. Pada tahap ini, pelaku melancarkan serangan utamanya melalui penipuan transaksi jual beli menggunakan akun kurasi. Dengan cara lain juga dapat melalui pinjaman online (pinjol) yang menggunakan data korban untuk mencairkan uang dalam rekening korban. Tahap yang ketiga ini dapat menggunakan modus peretasan akun sosial media untuk meminta para koneksi korban sejumlah dana atau pinjaman.

Tahap yang terakhir dapat berakibat pada potensi pencucian uang atau *money laundering*, yang berarti memutus jejak aliran dana agar tidak terlacak oleh aparat hukum. Melalui tahap ini, uang hasil dari kejahatan pada tahap-tahap sebelumnya akan dipindahkan berkali-kali sehingga akan menjadi bersih menuju kantong pelaku kejahatan.

Konstruksi Pertanggungjawaban Pidana

Konstruksi pertanggungjawaban pidana terhadap pelaku pencurian identitas dalam sistem hukum Indonesia saat ini masih bersifat tidak langsung (*indirect criminalization*), karena belum terdapat rumusan delik yang secara eksplisit mengkualifikasikan *identity theft* sebagai tindak pidana tersendiri. Penegakan hukum terhadap perbuatan tersebut pada umumnya masih bergantung pada pasal-pasal lain, seperti ketentuan mengenai akses ilegal, manipulasi data, penipuan, atau penyalahgunaan informasi elektronik. Dalam praktik peradilan, aparat penegak hukum yang berada di bawah koordinasi Kepolisian Negara Republik Indonesia dan lembaga peradilan yang berada dalam lingkup Mahkamah Agung Republik Indonesia sering kali harus melakukan konstruksi hukum secara ekstensif untuk mengaitkan perbuatan pencurian identitas dengan delik yang telah ada. Pendekatan ini menyebabkan terjadinya penafsiran yang beragam antar penegak hukum, baik pada tahap penyidikan, penuntutan, maupun pemeriksaan di pengadilan.

Sebagaimana telah diuraikan sebelumnya, ketiadaan delik khusus pencurian identitas menimbulkan problematika serius dalam kepastian hukum. Pelaku tidak selalu dapat dimintai pertanggungjawaban atas perbuatan penguasaan identitas itu sendiri, melainkan baru dapat diproses setelah terjadi tindak pidana lanjutan, seperti penipuan atau pembobolan rekening. Akibatnya, pencurian identitas sebagai perbuatan awal seringkali dipandang hanya sebagai bagian dari kejahatan utama, bukan sebagai perbuatan yang berdiri sendiri dan patut dipidana. Kondisi tersebut juga berdampak pada lemahnya perlindungan hukum bagi korban. Dalam banyak kasus, korban mengalami kesulitan untuk memperoleh pemulihan hak ketika pelaku belum melakukan kejahatan lanjutan secara nyata, meskipun identitasnya telah dikuasai secara ilegal. Hal ini menunjukkan bahwa sistem hukum pidana belum sepenuhnya mengakomodasi karakter preventif dalam penanggulangan kejahatan siber.

Ketika pencurian identitas berfungsi sebagai *entry crime* dalam rangkaian kejahatan siber, ketiadaan delik khusus menyebabkan terputusnya rantai pertanggungjawaban pidana pada tahap awal. Penegakan hukum menjadi bersifat represif dan reaktif, karena baru bergerak setelah timbul kerugian nyata, bukan pada saat terjadi pengambilalihan identitas. Konstruksi pertanggungjawaban pidana yang masih bersifat tidak langsung mencerminkan adanya kekosongan normatif dalam hukum pidana siber Indonesia. Situasi ini menegaskan urgensi pembaharuan kebijakan hukum pidana melalui perumusan delik khusus pencurian identitas, guna menjamin kepastian hukum, memperkuat perlindungan korban, serta meningkatkan efektivitas pencegahan kejahatan siber sejak tahap awal.

1. Pertanggungjawaban Berdasarkan Undang-Undang Informasi dan Transaksi Elektronik

Meskipun Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik sebagaimana telah diubah terakhir dengan Undang-Undang Nomor 1 Tahun 2024 (UU ITE) tidak secara eksplisit mengatur *identity theft* sebagai delik tersendiri, sejumlah ketentuannya dapat digunakan sebagai dasar pertanggungjawaban pidana. Dalam hal pencurian identitas dilakukan melalui akses tanpa hak terhadap sistem elektronik, maka perbuatan tersebut dapat dikualifikasikan berdasarkan Pasal 30 ayat (1), (2), dan (3) UU ITE, dengan ancaman pidana sebagaimana diatur dalam Pasal 46 UU ITE. Unsur "mengakses tanpa hak" dan "memperoleh informasi elektronik" relevan apabila pelaku meretas atau membobol sistem elektronik untuk mendapatkan data identitas korban.

Apabila perbuatan dilakukan melalui intersepsi atau penyadapan terhadap transmisi data elektronik, maka dapat diterapkan Pasal 31 UU ITE *juncto* Pasal 47 UU ITE. Sementara itu, dalam hal terjadi pemindahan, manipulasi, atau distribusi data identitas secara melawan hukum, Pasal 32 UU ITE *juncto* Pasal 48 UU ITE dapat menjadi dasar pemidanaan. Lebih lanjut, apabila identitas yang diperoleh digunakan untuk melakukan penipuan atau transaksi ilegal, pertanggungjawaban dapat diperluas melalui Pasal 378 KUHP. Dalam konstruksi ini, pencurian identitas berfungsi sebagai perbuatan pendahuluan (*entry crime*), sedangkan tindak pidana penipuan menjadi delik utama yang menimbulkan kerugian. Namun demikian,

perlindungan dalam UU ITE berorientasi pada sistem elektronik sebagai objek hukum, bukan pada identitas sebagai kepentingan hukum yang berdiri sendiri. Akibatnya, konstruksi pertanggungjawaban terhadap pencurian identitas masih bersifat tidak langsung dan fragmentaris, sehingga belum sepenuhnya mencerminkan karakter khas *identity theft* dalam kejahatan siber *modern*.

2. Kualifikasi Pidana Berdasarkan Undang-Undang Perlindungan Data Pribadi

Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi (UU PDP) memberikan dasar hukum yang lebih spesifik dalam mengatur perlindungan data pribadi sebagai hak subjek data. Dalam konteks pencurian identitas, perbuatan tersebut dapat dikualifikasikan sebagai tindakan memperoleh, mengumpulkan, mengungkapkan, atau menggunakan data pribadi secara melawan hukum. Secara normatif, Pasal 65 ayat (1), (2), dan (3) UU PDP melarang setiap orang secara 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, serta melarang pengungkapan dan penggunaan data pribadi tanpa hak. Ketentuan pidananya diatur dalam Pasal 67 dan Pasal 68 UU PDP, yang memuat ancaman pidana penjara dan/atau denda bagi pelanggaran tersebut.

Dalam hal ini, pencurian identitas dapat dikonstruksikan sebagai bentuk perolehan dan penggunaan data pribadi secara melawan hukum, khususnya apabila dilakukan dengan kesengajaan dan menimbulkan kerugian bagi korban. UU PDP dengan demikian memperluas perlindungan dari sekadar sistem elektronik menjadi perlindungan terhadap data pribadi sebagai hak individual. Namun demikian, meskipun UU PDP telah memperkenalkan sanksi pidana yang lebih tegas, pengaturannya tetap belum secara eksplisit merumuskan *identity theft* sebagai delik khusus dengan unsur-unsur yang berdiri sendiri. Pencurian identitas masih ditempatkan dalam kerangka umum pelanggaran perlindungan data pribadi, sehingga konstruksi pertanggungjawaban pidananya tetap bergantung pada interpretasi terhadap norma perolehan dan penggunaan data secara melawan hukum.

3. Potensi Hubungan dengan Tindak Pidana Pencucian Uang

Dalam praktik kejahatan siber modern, pencurian identitas kerap berfungsi sebagai tahap awal (*entry crime*) sebelum terjadinya tindak pidana lanjutan, seperti penipuan daring, pengajuan kredit fiktif, maupun pembukaan rekening penampung dana hasil kejahatan. Identitas korban digunakan untuk memenuhi persyaratan administratif dan verifikasi layanan keuangan, sehingga pelaku dapat mengalihkan, menempatkan, atau *mentransfer* dana tanpa menggunakan identitas aslinya. Dalam konstruksi ini, identitas berfungsi sebagai instrumen penyamaran (*instrument of concealment*). Secara normatif, tindak pidana pencucian uang di Indonesia diatur dalam Undang-Undang Nomor 8 Tahun 2010 tentang Pencegahan dan Pemberantasan Tindak Pidana Pencucian Uang, khususnya dalam Pasal 3 dan Pasal 4, yang pada pokoknya mengatur perbuatan menempatkan, mentransfer, atau

menyamarkan asal-usul harta kekayaan yang diketahui atau patut diduga berasal dari tindak pidana dengan tujuan menyembunyikan atau menyamarkan asal-usulnya. Dalam konteks ini, penggunaan identitas orang lain untuk membuka rekening atau melakukan transaksi dapat menjadi bagian dari mekanisme penyamaran tersebut.

Dengan demikian, pencurian identitas tidak hanya berdiri sebagai pelanggaran terhadap sistem elektronik atau data pribadi, tetapi juga memiliki hubungan kausal dengan tindak pidana lanjutan yang bersifat ekonomi. Identitas yang diperoleh secara melawan hukum menjadi sarana untuk memutus jejak antara pelaku dan hasil kejahatan, sehingga memperumit proses pelacakan aset (*asset tracing*) oleh aparat penegak hukum. Hubungan fungsional antara pencurian identitas dan pencucian uang menunjukkan bahwa *identity theft* berpotensi dikualifikasikan sebagai perbuatan pendahuluan dalam suatu rangkaian kejahatan yang lebih kompleks. Oleh karena itu, dalam konstruksi pertanggungjawaban pidana, penting untuk melihat pencurian identitas tidak secara terpisah, melainkan sebagai bagian dari struktur kejahatan yang terintegrasi dalam skema kejahatan ekonomi digital.

4. Urgensi Perumusan Delik Khusus Pencurian Identitas

Secara teoritik, pertanggungjawaban pidana mensyaratkan adanya perbuatan melawan hukum (*wederrechtelijkheid*), kesalahan dalam bentuk kesengajaan (*dolus*) atau kealpaan (*culpa*), serta tidak adanya alasan pembenar maupun pemaaf. Dalam konteks pencurian identitas, unsur kesengajaan pada umumnya terpenuhi karena pelaku secara sadar dan terencana mengambil, menguasai, atau menggunakan identitas orang lain untuk memperoleh keuntungan tertentu atau untuk memfasilitasi terjadinya tindak pidana lain. Identitas dalam hal ini tidak sekadar data administratif, melainkan telah menjadi instrumen ekonomi yang memiliki nilai strategis dalam ekosistem digital.

Namun demikian, ketiadaan delik khusus yang secara eksplisit merumuskan pencurian identitas sebagai tindak pidana yang berdiri sendiri menyebabkan konstruksi pertanggungjawaban pidana tersebar dalam berbagai peraturan perundang-undangan, seperti UU ITE, UU PDP, maupun ketentuan dalam KUHP. Fragmentasi norma ini menimbulkan persoalan sistemik, antara lain ketidakseragaman dalam penerapan pasal, perbedaan konstruksi dakwaan, serta kesulitan dalam merumuskan hubungan antara perbuatan awal (pengambilalihan identitas) dan tindak pidana lanjutan yang ditimbulkannya.

Selain itu, tanpa rumusan delik khusus, identitas sebagai kepentingan hukum (*rechtsgoed*) belum memperoleh pengakuan yang tegas dalam hukum pidana. Perlindungan yang ada masih bersifat tidak langsung, yakni melalui perlindungan terhadap sistem elektronik atau data pribadi secara umum. Akibatnya, posisi korban dalam memperoleh pemulihan, rehabilitasi nama baik, maupun penghapusan tanggung jawab atas perbuatan yang dilakukan oleh pelaku menggunakan identitasnya menjadi kurang optimal. Oleh karena itu, diperlukan perumusan delik khusus pencurian identitas yang secara eksplisit mengatur definisi

dan ruang lingkup perbuatan, unsur objektif dan subjektif tindak pidana, bentuk pemberatan apabila digunakan sebagai sarana kejahatan lanjutan, serta mekanisme perlindungan dan pemulihan korban. Perumusan tersebut juga penting untuk memastikan adanya kepastian hukum (*legal certainty*), konsistensi penegakan hukum, serta efektivitas perlindungan terhadap individu dalam menghadapi dinamika kejahatan siber *modern* yang semakin kompleks dan terintegrasi.

Analisis Kelemahan Pengaturan

Pengaturan mengenai pencurian identitas dalam sistem hukum Indonesia saat ini menunjukkan sejumlah kelemahan struktural yang berdampak langsung terhadap efektivitas penegakan hukum dan perlindungan korban. Kelemahan tersebut terutama terletak pada fragmentasi norma, tidak adanya perumusan eksplisit mengenai identity theft sebagai delik tersendiri, serta implikasinya terhadap kepastian hukum dan konsistensi penerapan hukum pidana.

Pertama, dari aspek fragmentasi norma, pengaturan mengenai perbuatan yang berkaitan dengan pencurian identitas tersebar dalam berbagai peraturan perundang-undangan, antara lain dalam Undang-Undang Informasi dan Transaksi Elektronik, Undang-Undang Perlindungan Data Pribadi, Undang-Undang Pencegahan dan Pemberantasan Tindak Pidana Pencucian Uang, serta ketentuan mengenai penipuan dalam KUHP. Regulasi-regulasi tersebut dibentuk melalui proses legislasi oleh Dewan Perwakilan Rakyat Republik Indonesia bersama pemerintah, namun disusun secara sektoral sesuai dengan ruang lingkup masing-masing undang-undang. Masing-masing regulasi tersebut hanya mengatur aspek tertentu dari pencurian identitas, seperti akses ilegal terhadap sistem elektronik, perolehan dan penggunaan data pribadi secara melawan hukum, penyamaran hasil tindak pidana, atau perbuatan penipuan. Akan tetapi, tidak terdapat satu pun regulasi yang secara komprehensif mengatur keseluruhan rangkaian perbuatan identity theft sebagai satu konstruksi tindak pidana yang utuh, mulai dari pengambilan data, penguasaan identitas, hingga pemanfaatannya untuk kejahatan lanjutan.

Akibat fragmentasi tersebut, penegakan hukum terhadap pencurian identitas cenderung dilakukan dengan pendekatan parsial, yaitu bergantung pada pasal mana yang dianggap paling relevan oleh aparat penegak hukum. Dalam satu kasus, pelaku dapat dijerat dengan pasal akses ilegal, sementara dalam kasus lain dengan karakteristik serupa justru dikenakan pasal penipuan atau pencucian uang. Perbedaan pendekatan ini menunjukkan tidak adanya standar normatif yang seragam dalam menangani tindak pidana pencurian identitas. Kondisi tersebut berpotensi menimbulkan inkonsistensi dalam penerapan hukum serta perbedaan konstruksi dakwaan dalam perkara yang memiliki pola kejahatan yang sama. Dari perspektif kepastian hukum, situasi ini merugikan baik bagi pelaku maupun korban. Bagi pelaku, ketidakjelasan norma membuka ruang multitafsir dalam pemidanaan, sedangkan bagi korban, fragmentasi pengaturan menyulitkan upaya memperoleh perlindungan hukum dan pemulihan hak secara optimal.

Fragmentasi norma juga mencerminkan belum terbangunnya paradigma regulasi yang memandang pencurian identitas sebagai kejahatan sistemik dan berantai. Regulasi yang ada masih memposisikan perbuatan tersebut secara terpisah-pisah, sehingga belum mampu menangkap karakter identity theft sebagai entry crime dalam ekosistem kejahatan siber. Kelemahan struktural berupa fragmentasi norma menunjukkan perlunya pembaruan kebijakan legislasi yang lebih terintegrasi. Perumusan delik khusus pencurian identitas yang bersifat komprehensif menjadi penting untuk menyatukan berbagai aspek pengaturan yang saat ini terpisah, sekaligus memperkuat konsistensi penegakan hukum dan perlindungan korban dalam konteks kejahatan siber di Indonesia.

Kedua, tidak adanya penggunaan istilah "*identity theft*" atau "pencurian identitas" secara eksplisit sebagai delik khusus dalam peraturan perundang-undangan menyebabkan kekaburan dalam penentuan objek perlindungan hukum (*rechtsgoed*). Dalam UU ITE, fokus perlindungan terletak pada sistem elektronik dan informasi elektronik, sedangkan dalam UU PDP, perlindungan diarahkan pada data pribadi sebagai bagian dari hak subjek data. Meskipun kedua undang-undang tersebut dapat digunakan untuk menjerat pelaku pencurian identitas, konstruksi deliknya tetap bersifat umum dan tidak secara spesifik mengakui identitas sebagai entitas hukum yang memiliki nilai dan kepentingan tersendiri. Padahal dalam praktik kejahatan siber modern, identitas digital telah berkembang menjadi instrumen ekonomi yang dapat dieksploitasi sebagai sarana kejahatan lanjutan. Ketiadaan rumusan eksplisit ini menyebabkan identity theft diposisikan hanya sebagai bagian dari pelanggaran akses data atau penyalahgunaan informasi, bukan sebagai tindak pidana dengan karakteristik khas yang berdiri sendiri.

Ketiga, kelemahan normatif tersebut berdampak langsung terhadap kepastian hukum dan perlindungan korban. Dari perspektif kepastian hukum (*legal certainty*), fragmentasi dan ketiadaan delik khusus menimbulkan potensi multitafsir dalam menentukan unsur-unsur perbuatan, bentuk kesalahan, serta hubungan kausal antara pencurian identitas dan tindak pidana lanjutan. Hal ini dapat mempengaruhi konsistensi putusan pengadilan serta efektivitas pembuktian di persidangan. Sementara itu, dari sisi perlindungan korban, posisi korban pencurian identitas seringkali tidak memperoleh pemulihan yang optimal. Korban tidak hanya mengalami kerugian materiil akibat transaksi ilegal, tetapi juga kerugian immateriil berupa rusaknya reputasi, terganggunya akses layanan keuangan, serta beban administratif untuk membuktikan bahwa perbuatan tersebut bukan dilakukan olehnya. Tanpa pengakuan tegas bahwa pencurian identitas merupakan delik yang berdiri sendiri, mekanisme rehabilitasi nama baik dan pemulihan tanggung jawab hukum korban menjadi kurang terstruktur.

Dengan demikian, analisis terhadap kelemahan pengaturan menunjukkan adanya kebutuhan mendesak untuk melakukan reformulasi norma yang lebih sistematis. Perumusan delik khusus pencurian identitas yang secara eksplisit mendefinisikan ruang lingkup perbuatan, unsur objektif dan subjektif, serta kaitannya dengan kejahatan lanjutan akan memperkuat kepastian hukum, meningkatkan konsistensi penegakan hukum, dan memberikan perlindungan yang

lebih komprehensif bagi korban dalam menghadapi dinamika kejahatan siber yang semakin kompleks.

SIMPULAN

Pencurian identitas dalam ekosistem siber modern memiliki karakteristik fundamental sebagai kejahatan pembuka (*entry crime*) yang berfungsi sebagai pintu masuk bagi berbagai rangkaian tindak pidana lanjutan yang lebih kompleks. Identitas digital yang meliputi data kependudukan, kredensial akun, hingga informasi finansial telah bertransformasi menjadi instrumen kejahatan ekonomi digital yang memiliki nilai komoditas strategis. Data tersebut dimanfaatkan oleh pelaku untuk melakukan penipuan daring, pembobolan rekening, hingga pencucian uang secara sistematis dan terorganisasi. Dalam praktiknya, data identitas yang diperoleh secara ilegal tidak hanya digunakan sebagai sarana utama melakukan kejahatan, tetapi juga berfungsi sebagai instrumen penyamaran (*instrument of concealment*) untuk memutus jejak aliran dana dan menyamarkan identitas pelaku. Namun demikian, pengaturan mengenai pencurian identitas dalam sistem hukum Indonesia saat ini dinilai belum komprehensif, karena tidak adanya rumusan delik yang secara eksplisit mengkualifikasikan *identity theft* sebagai tindak pidana mandiri yang berdiri sendiri.

Ketiadaan pengaturan khusus tersebut menyebabkan konstruksi pertanggungjawaban pidana terhadap pelaku masih bersifat fragmentaris dan tidak langsung. Penegakan hukum yang dilakukan oleh aparat di bawah koordinasi Kepolisian Negara Republik Indonesia masih sangat bergantung pada penafsiran terhadap berbagai norma yang tersebar dalam undang-undang sektoral. Sementara itu, dari sisi legislasi, belum terbangunnya regulasi terpadu yang dirumuskan oleh Dewan Perwakilan Rakyat Republik Indonesia bersama pemerintah menunjukkan adanya kekosongan normatif dalam merespons karakter kejahatan digital yang bersifat dinamis dan berantai. Akibat kondisi tersebut, penanganan perkara pencurian identitas sering kali bergantung pada kreativitas konstruksi hukum aparat penegak hukum, sehingga berpotensi menimbulkan perbedaan penerapan pasal dalam kasus yang serupa. Situasi ini menciptakan celah dalam kepastian hukum, melemahkan efek jera, serta mengurangi efektivitas perlindungan hukum bagi korban kejahatan siber. Penelitian ini menegaskan bahwa pencurian identitas tidak dapat lagi dipandang sebagai perbuatan pelengkap dalam tindak pidana lain, melainkan sebagai kejahatan strategis yang menjadi fondasi utama kejahatan siber modern. Oleh karena itu, diperlukan reformulasi kebijakan hukum pidana melalui perumusan delik khusus pencurian identitas yang bersifat komprehensif, terintegrasi, dan adaptif terhadap perkembangan teknologi, guna memperkuat kepastian hukum, meningkatkan efektivitas penegakan hukum, serta memberikan perlindungan yang optimal bagi masyarakat dalam ekosistem digital nasional.

DAFTAR RUJUKAN

Pramudya, D. W., & Yusuf, H. (2025). Pencurian Data Identitas Sebagai Kejahatan Cyber Related Crime: Tinjauan Kriminologis Atas Kasus Pencurian Data

Pada Akun Marketplace. *JIIC: JURNAL INTELEK INSAN CENDIKIA*, *Vol : 2*(7).

DJPB Indonesia. (2025, June 24). *Keamanan informasi phishing : Pengertian, Jenis, Dan Cara Menghindari phising*. DJPb. https://djpb.kemenkeu.go.id/kppn/manna/id/data-publikasi/artikel/3239-keamanan-informasi-phishing-pengertian,-jenis,-dan-cara-menghindari-phising.html

Republik Indonesia. (2008). Undang-Undang Republik Indonesia Nomor 11 Tahun 2008 tentang *Informasi dan Transaksi Elektronik*.

Republik Indonesia. (2024). Undang-Undang Republik Indonesia Nomor 1 Tahun 2024 tentang *Perubahan Kedua atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektroni*k.

Republik Indonesia. (2022). Undang-Undang Republik Indonesia Nomor 27 Tahun 2022 tentang *Perlindungan Data Pribadi*.

Republik Indonesia. (2010). Undang-Undang Republik Indonesia Nomor 8 Tahun 2010 tentang *Pencegahan dan Pemberantasan Tindak Pidana Pencucian Uang*.

Privy.id. (n.d.). *Apa itu Identity Theft, Cara Kerja & Tips Mencegahnya*, https://privy.id/blog/identity-theft/

Sulaeman, D., & Kemala, A. P. (2025). *Analisis Hukum terhadap Tindak Pidana Pencurian Identitas di Indonesia.* Aladalah: Jurnal Politik, Sosial, Hukum dan Humaniora, 3(2), 133–148.

