Indonesian Journal of Law and Justice Volume: 3, Number 2, 2025, *Page*: 1-11

Analisis Kriminologi dalam Tindak Pidana Pencurian Data Pribadi di Era Digital

Camiliya Fakhriyah Garnita*, Kuswandi

Faculty of Law, Suryakancana University

DOI:
https://doi.org/10.47134/ijlj.v3i2.5288
*Correspondence: Camiliya Fakhriyah Garnita
Email: garnitaameyy@gmail.com

Received: 03-10-2025
Accepted: 19-11-2025
Published: 28-12-2025

Abstract: *The The development of information technology in the digital age has increased the ease of access to data-based services, but it has also posed a serious threat in the form of personal data theft as a form of cybercrime. Personal data theft not only causes financial losses, but also has psychological and social impacts such as stress, anxiety, decreased trust in digital institutions, and damage to the victim's reputation. This study aims to analyze personal data theft from a criminological perspective by examining the driving factors, impacts, and weak data protection in Indonesia. The research method used is a qualitative approach through a literature study of regulations, criminological theories, and cases of data theft in digital and banking services. The results show that data theft is triggered by the perpetrators' economic motives, human error, malware attacks, social engineering, weak digital security systems, and low public literacy. In addition, the implementation of the Personal Data Protection Law (PDP Law) is considered suboptimal, thus failing to provide effective protection. This study concludes that personal data theft is a complex crime that requires regulatory strengthening, improved cybersecurity, and collaboration between the government, digital institutions, and the public to create a secure digital ecosystem.*

Keywords: *Personal Data Theft, Cybercrime, Criminology, PDP Law, Digital Security*

Pendahuluan

Di era digital saat ini, kemajuan teknologi informasi telah membawa dampak besar bagi kehidupan masyarakat, termasuk dalam aspek keamanan data pribadi. Pencurian data pribadi menjadi salah satu tindak pidana yang marak terjadi, seiring dengan meningkatnya pemanfaatan internet dan perangkat digital. Kejahatan ini tidak hanya merugikan korban secara materi dan psikologis, tetapi juga mengancam keamanan dan privasi individu serta institusi. Kondisi ini menuntut adanya pemahaman kriminologis yang mendalam untuk menganalisis motif, modus operandi, serta faktor yang mempengaruhi terjadinya tindak pidana tersebut. Pendekatan kriminologi modern memungkinkan untuk mengkaji secara komprehensif bagaimana perilaku pelaku, lingkungan sosial, serta perkembangan teknologi dapat memicu dan mempermudah terjadinya pencurian data pribadi di dunia maya. Melalui analisis ini, diharapkan dapat ditemukan solusi pencegahan dan penanggulangan yang efektif untuk mengurangi risiko kejahatan siber tersebut.

Kemajuan teknologi informasi dianggap sebagai faktor yang dapat mempengaruhi kehidupan individu. Hal ini menyebabkan masyarakat Indonesia cenderung semakin

bergantung pada teknologi informasi, yang juga meningkatkan potensi terjadinya tindak kejahatan. Teknologi informasi memiliki kemampuan untuk memperbaiki pola pikir masyarakat, namun di sisi lain, juga dapat disalah gunakan sebagai sarana untuk melakukan tindakan kriminal, yang dikenal dengan istilah "kejahatan dunia maya" atau "cybercrime". Cybercrime ialah merujuk kepada kejahatan atau tindakan ilegal yang dilakukan melalui jaringan elektronik global. Kejahatan di dunia maya semakin mengancam karena dampaknya yang luas.

Kejahatan siber berhubungan dengan ruang digital yang dapat merusak privasi individu. Secara umum, kejahatan di dunia maya semakin meningkat, dengan karakteristik pelaku yang semakin beragam. Berkat kemajuan teknologi informasi, pelaku kejahatan dengan mudah melakukan tindakan kriminal. Pencurian data di dunia maya dikenal sebagai phishing, yaitu tindakan ilegal dimana bertujuan untuk memperoleh informasi yang bersifat pribadi atau data yang bersifat sensitif seseorang. Dalam aksi ini, pelaku berusaha mendapatkan data seperti nomor kartu kredit, PIN, ID pengguna, nomor telepon, nomor rekening, serta informasi pribadi lainnya. Setelah mendapatkan data tersebut, pelaku memanfaatkannya untuk merugikan korban melalui penipuan dan tindakan kriminal lainnya. Ancaman terhadap eksploitasi data pribadi di Indonesia semakin meningkat setelah pemerintah memperkenalkan kebijakan Kartu Tanda Penduduk Elektronik (e-KTP), yang bertujuan untuk mengumpulkan data kependudukan. dengan maraknya kasus kriminal ini menghambat program pemerintah dalam pembuatan Kartu Tanda Penduduk elektronik di karenakan mulai berkurang nya rasa percaya masyarakat terhadap kemajuan teknologi digital sehingga menjadi tantangan besar bagi Aparatur Pemerintah Indonesia dalam memperkuat pertahanan cyber juga memperketat sanksi bagi pelaku pelaku cybercrime di Indonesia.

Selain itu juga cybercrime juga dibagi berdasarkan dua kategori, antara lain: cybercrime yang menargetkan komputer dan cybercrime yang kejahatannya menggunakan alat yaitu dengan bertambahnya pengguna jejaring sosial di Indonesia, tak dipungkiri banyak informasi pribadi pengguna yang bocor. Menurut Polri, terdapat 1.409 perkara terkait penipuan yang terjadi setiap tahun yang diakibatkan bocornya informasi para pengguna social media yang bersifat pribadi. Data pribadi adalah hal yang biasa bagi semua orang. Data yang bersifat pribadi sangat sensitif. Data pribadi harus mendapat perlindungan karena hal tersebut merupakan hak atas privasi tiap orang. Hak atas privasi merupakan kewarganegaraan konstitusional yang diabadikan dalam UUD RI 1945. Hak dasar ialah sesuatu yang harus dilakukan negara terhadap tiap warga negaranya. Saat ini, di Indonesia sendiri marak problematika hukum yang berkaitan dengan penyalah gunaan informasi pribadi yang digunakan untuk keuntungan sendiri.

Dengan demikian, dampak dari pencurian data ini bisa meluas, melibatkan komunitas dan masyarakat Indonesia secara keseluruhan. Namun, di Indonesia, perlindungan data pribadi belum diatur secara rinci dalam perundang undangan, sehingga peraturan yang ada masih bersifat parsial atau sektoral dan sering kali tumpang tindih. Beberapa undang-undang yang mengatur sistem elektronik, seperti Undang-Undang (UU) Nomor 1 Tahun 2024 tentang Perubahan Kedua atas Undang-Undang Nomor 11 Tahun

2008 tentang Informasi dan Transaksi Elektronik, hanya mencakup beberapa aspek perlindungan data pribadi secara umum.

Pencurian data identitas sebagai bentuk cybercrime menuntut perhatian serius dari perspektif kriminologi, mengingat sifatnya yang transnasional, tidak kasat mata, dan berdampak luas. Dalam konteks kriminologi, penting untuk memahami motivasi pelaku, pola kejahatan, peran teknologi sebagai alat dan ruang kejahatan, serta bagaimana struktur sosial dan kebijakan hukum turut memengaruhi dinamika tersebut.

Berdasarkan latar belakang tersebut, penelitian ini akan membahas pencurian data identitas sebagai kejahatan siber dengan fokus pada kasus-kasus yang terjadi di marketplace digital. Tujuan dari kajian ini adalah untuk memberikan pemahaman mendalam mengenai karakteristik dan implikasi kriminologis dari kejahatan ini, serta menawarkan rekomendasi terhadap upaya pencegahan dan penanggulangan yang dapat dilakukan baik oleh pemerintah, penyedia platform digital, maupun masyarakat sebagai pengguna layanan teknologi.

Metode Penelitian

Penelitian ini menggunakan pendekatan kualitatif dengan metode studi literatur (library research) untuk mengkaji hukum pidana dan perlindungan data pribadi sebagai upaya menanggulangi kejahatan siber di era digital di Indonesia. Metode ini dipilih karena relevan dalam menggali informasi dari sumber-sumber akademik dan dokumen hukum yang mendalam dan terfokus. Proses analisis mencakup telaah terhadap teori hukum, prinsip hukum, serta konsep hukum yang relevan, yang bersumber dari referensi hukum primer maupun sekunder.

Hasil dan Pembahasan

Apa dampak sosial, ekonomi, dan psikologis yang muncul pada korban akibat pencurian data pribadi

Munculnya teknologi digital dalam informasi dan komunikasi membawa perkembangan dan perubahan yang berdampak besar dalam berbagai sisi kehidupan masyarakat Indonesia, terutama dalam hal pengelolaan dan pertukaran data pribadi. Digitalisasi yang masi di sektor publik maupun privat telah mendorong masyarakat untuk semakin bergantung pada layanan berbasis data, mulai dari transaksi keuangan, layanan kesehatan, hingga aktivitas pemerintahan. Namun, kemajuan ini juga diiringi dengan meningkatnya risiko kebocoran data pribadi yang dapat mengancam privasi dan keamanan individu. Fenomena ini menuntut adanya regulasi yang komprehensif guna melindungi hak-hak masyarakat atas data pribadinya di era digital.

Selain itu, implementasi Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi (UU PDP) masih belum memaksimalkan dalam menjawab tantangan perlindungan privasi di tengah maraknya digitalisasi layanan publik dan privat. Kesenjangan penelitian terletak pada perbedaan antara norma hukum yang diatur dalam UU PDP dengan realitas implementasi di lapangan. Secara normatif, UU PDP telah

mengadopsi prinsip-prinsip perlindungan data pribadi yang sejalan dengan standar internasional.

Namun, dalam praktiknya, masih ditemukan berbagai kendala seperti lemahnya penegakan hukum, kurangnya infrastruktur pendukung, serta minimnya koordinasi antar lembaga terkait. Penelitian terdahulu umumnya berfokus pada aspek yuridis atau perbandingan regulasi, sementara kajian mengenai dampak sosial kebocoran data dan keterbatasan implementasi UU PDP masih sangat terbatas.

Tetapi kasus bocornya data pribadi yang terjadi kepada korban, dapat disimpulkan bahwa contohnya sistem keamanan pihak bank tidak cukup ketat. Hal ini tentu mengakibatkan hilangnya rasa percaya nasabah yang sebelumnya memiliki kepercayaan kepada bank sebagai lembaga keuangan yang seharusnya dapat menjaga data-data pribadinya. Berdasarkan Pasal 65 UU PDP, bank sebagai pengendali data pribadi telah gagal melaksanakan kewajibannya dalam menjaga kerahasiaan dan keamanan data pribadi nasabah dan berdampak negatif bagi korban yang dapat dikategorikan ke dalam tiga aspek utama, yaitu psikologis, sosial, ekonomi.

A. Dampak psikologis

Psikologis dari pelanggaran data bisa sangat luas. Bagi sebagian korban, trauma emosional dapat menyebabkan masalah kesehatan mental jangka panjang, seperti gangguan stres pascatrauma (PTSD), depresi, dan kecemasan berat. Kekhawatiran yang terus-menerus tentang potensi pencurian identitas atau penipuan keuangan dapat berkontribusi pada stres kronis, yang memengaruhi kehidupan sehari-hari, hubungan, dan kesejahteraan Anda secara keseluruhan.

1. Stres dan Frustasi

   Korban harus menghadapi penagihan dari pihak bank yang tidak dikenal, tanpa mengetahui bagaimana data pribadinya bisa disalahgunakan. Ketidakjelasan penyelesaian kasus oleh bank juga memperburuk kondisi emosionalnya.

2. Kemarahan dan Rasa Tidak Berdaya

   Ketika korban mencoba untuk menghubungi pihak bank untuk melakukan klarifikasi, ia mendapatkan respons yang lambat dan berbelit-belit. Hal ini tentu menyebabkan frustrasi dan kemarahan karena seolah-olah pihak bank tidak serius dalam menanggapi masalah ini.

3. Kecemasan dan Ketidakpastian

   Ketidakjelasan dalam penyelesaian masalah dan ketakutan akan memberikan dampak jangka panjang (misalnya, kesulitan dalam mengakses dalam mengakses layanan keuangan) menyebabkan kecemasan yang berkepanjangan. Apalagi, pihak bank terus meminta waktu tambahan tanpa kepastian penyelesaian.

4. Trauma Terhadap Layanan Perbankan dan Keuangan

   Setelah mengalami kejadian ini, korban bisa menjadi lebih takut untuk berinteraksi dengan bank atau lembaga keuangan lainnya. Korban juga dapat

mengalami perasaan takut yang menyebabkan korban cenderung menghindari penggunaan kartu kredit atau layanan pinjaman.

5. Gangguan Tidur dan Kesehatan Mental

Gangguan tidur (Insomnia) dapat terjadi kepada korban karena terus-menerus memikirkan masalah ini, terutama jika terus mendapat tekanan dan tagihan dari debt collector atau pihak bank.

Pelanggaran kepercayaan yang terjadi ketika sebuah perusahaan gagal melindungi informasi pribadi Anda dapat menyebabkan perasaan dikhianati dan skeptisisme yang berkepanjangan. Anda mungkin merasa sulit untuk mempercayakan data Anda kepada organisasi di masa mendatang, yang mengakibatkan rasa terisolasi dan terputus hubungan.

B. Dampak Sosial

Dampak Sosial pencurian data pribadi dapat merusak reputasi sosial korban dan menurunkan kepercayaan masyarakat terhadap korban, terutama jika data disalah gunakan untuk kejahatan lain. Korban juga dapat mengalami tekanan sosial akibat stigma dan ketidaknyamanan dalam hubungan sosialnya karena penyalahgunaan identitas atau informasi pribadi mengenai dampak sosial kebocoran data dan keterbatasan implementasi UU PDP (Perlindungan Data Pribadi) masih sangat terbatas.

Dampak sosial dari kebocoran data pribadi sering kali diabaikan, tetapi dalam kasus efeknya bisa sangat merugikan korban.

Beberapa dampak sosial yang dialami oleh korban meliputi:

1. Penurunan Kepercayaan terhadap Lembaga Keuangan

Setelah mengalami kasus ini, korban merasa bahwa bank tidak memiliki sistem keamanan yang baik dan tidak peduli terhadap perlindungan akan data nasabah. Hal ini bisa berdampak pada keengganan menggunakan layanan perbankan di masa depan.

2. Stigma Negatif di Lingkungan Sosial

Nama korban yang tercatat dalam daftar hitam perbankan dapat menimbulkan stigma negatif. Terutama jika ada pihak yang lain yang mengetahui status kreditnya. Ini dapat mempengaruhi interaksi sosial dan kepercayaan dalam lingkungan kerja atau bisnis.

3. Gangguan dalam Aktivitas Sehari-hari

Korban harus menghabiskan waktu yang cukup lama untuk menyelesaikan kasus ini, mulai dari menghubungi call center, mendatangi bank, hingga berusaha mendapatkan kejelasan dari pihak terkait. Hal ini tentu sangat mengganggu aktivitas sehari-hari dan menurunkan produktivitas.

4. Dampak Terhadap Kehidupan Profesional

Jika informasi mengenai hutang fiktif ini tersebar, bisa berdampak buruk pada reputasi profesional korban. Jika korban memiliki bisnis atau

usaha sendiri, maka kepercayaan pelanggan atau mitra bisnis bisa menurun karena melihat adanya masalah keuangan yang terkait dengan namanya.

Isolasi Sosial Jika kasus ini tersebar luas, dapat muncul stigma dari teman atau rekan kerja yang menganggap korban sebagai orang yang tidak bisa mengelola keuangan dengan baik, meskipun sebenarnya ia adalah korban dari pencurian identitas. Bahkan korban bisa merasa malu untuk menceritakan kejadian ini baik kepada teman atau keluarganya yang bisa membuat dirinya semakin terisolasi.

Ini menunjukkan perlunya analisis kritis yang mengaitkan antara harapan normatif (dass sollen) dan kenyataan empiris (dass sein) dalam perlindungan data pribadi di Indonesia. seiring meningkatnya ketergantungan masyarakat pada layanan digital dan besarnya potensi kerugian akibat kebocoran data pribadi dan bocoran data tidak hanya menyebabkan kerugian materiil, tetapi juga dapat menimbulkan trauma psikologis, penyalahgunaan identitas, serta menurunnya kepercayaan publik terhadap institusi penyelenggara layanan digital.

Oleh sebab itu, untuk memberikan rekomendasi strategis dalam memperkuat perlindungan privasi masyarakat sekaligus mendorong pembaruan kebijakan yang adaptif terhadap perkembangan teknologi dan kebutuhan masyarakat. Hal ini sejalan dengan pengesahan Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi yang menjadi landasan hukum utama dalam melindungi data pribadi warga negara Indonesia di era digital. Undang-undang ini tidak hanya menetapkan standar perlindungan data yang tinggi, tetapi juga memberikan dasar hukum bagi pemerintah untuk mengatasi dan mencegah kebocoran data pribadi.

Ketidaktertiban yang terjadi dalam hal penggunaan data pribadi dan bentuk penanggulangan data pribadi dari pencurian dalam media elektronik di tengah era-ekonomi digital kini kerap terjadi, sehingga keadaan yang seperti ini memerlukan kebijakan baik dalam pembentukan peraturan perundang-undangan yang secara khusus memberikan perlindungan hukum kepada data pribadi setiap orang serta bagaimana penanggulangan yang baik melalui sarana hukum atau non hukum sebagai "penjaga" agar perkembangan ke arah ekonomi digital berjalan dengan tertib.

Ini penting untuk diteliti karena Indonesia saat ini tengah berada di era peralihan dari ekonomi tradisional ke era ekonomi digital. Era ekonomi tradisional merupakan era sebelum teknologi informasi berkembang dengan pesat. Dalam era ekonomi tradisional perdagangan dana atau transaksi-transaksi lainnya antar masyarakat dilakukan secara langsung. Transaksi semacam ini menuntut para pihak yang akan bertransaksi hadir secara fisik di waktu dan tempat yang bersamaan Secara ekonomi, korban menghadapi biaya langsung seperti pemulihan identitas, kehilangan pendapatan, dan kerugian finansial jangka panjang. Biaya ini bisa mencapai ribuan dolar, termasuk waktu yang hilang untuk menyelesaikan masalah dengan lembaga keuangan atau hukum.

Dari segi psikologis, korban mengalami stres, kecemasan dan frustrasi akibat ketidakpastian penyelesaian kasus. Sementara itu, dari segi sosial, korban bisa kehilangan

kepercayaan terhadap sistem keuangan dan mengalami dampak negatif dalam lingkungannya. Oleh karena itu, perlindungan data pribadi harus menjadi perhatian serius bagi lembaga keuangan untuk mencegah kasus serupa terjadi di masa depan.

Bagaimana dampak tindak pidana pencurian data pribadi terhadap korban dan masyarakat di era digital

Tindak pidana pencurian data pribadi menyebabkan dampak besar bagi korban dan masyarakat, mulai dari kerugian finansial hingga masalah psikologis dan sosial. Penyalahgunaan identitas untuk penipuan, kerusakan reputasi, dan tekanan mental seperti stres serta kecemasan. Bagi masyarakat luas, dampaknya adalah menurunnya kepercayaan terhadap layanan digital, terhambatnya perkembangan ekonomi digital, serta potensi ancaman keamanan nasional jika data dalam skala besar jatuh ke tangan yang salah.

Dalam era modern seperti saat ini tentunya sudah memasuki era digital/online yang dimana semua hal berbasis online namun masih kurang adanya perlindungan hukum dan perlu adanya peraturan perundang-undangan yang membahas mengenai ini. Pencurian secara digital dapat memiliki dampak yang merugikan bagi korban. Korban pencurian data pribadi dapat mengalami kerugian finansial, seperti kehilangan uang dari rekening bank atau kartu kredit yang digunakan oleh pelaku. Selain itu, korban juga dapat mengalami kerugian non-finansial, seperti pencemaran nama baik atau identitas palsu yang digunakan oleh pelaku untuk melakukan tindakan kriminal lainnya.

Korban juga dapat mengalami kerugian emosional, seperti kehilangan privasi dan rasa aman karena data pribadi mereka telah dicuri. Dalam hal ini, perlindungan hukum bagi ciptaan-ciptaan didalam era digital dan perlindungan data pribadi menjadi penting untuk mencegah terjadinya pencurian secara digital dan melindungi korban dari dampak yang merugikan.

Kejahatan pencurian data identitas berdampak luas tidak hanya pada individu korban, tetapi juga terhadap integritas sistem digital nasional. Penyalahgunaan identitas, pemerasan, hingga reputasi digital yang rusak. Di sisi lain, masyarakat secara kolektif akan mengalami penurunan kepercayaan terhadap penyedia layanan digital, yang dalam jangka panjang menghambat perkembangan ekosistem ekonomi digital

Faktor-faktor apa saja yang mendorong terjadinya pencurian data pribadi dalam konteks kriminologi?

Pencurian data pribadi merupakan bentuk *cybercrime* yang terus meningkat seiring dengan perkembangan teknologi digital. Dalam perspektif kriminologi, kejahatan ini tidak hanya dipicu oleh faktor teknis, tetapi juga faktor sosial, ekonomi, psikologis, serta peluang kejahatan.

Motivasi Ekonomi dan Keuntungan Finansial

Dalam kriminologi, pencurian data pribadi sering dipandang sebagai tindakan rasional yang dilakukan untuk memperoleh keuntungan materi. Pelaku menyadari bahwa data pribadi seperti nomor identitas, data perbankan, atau akun digital memiliki nilai

ekonomi tinggi di pasar gelap (*dark web*). Dengan demikian, mereka mengambil keputusan berdasarkan pertimbangan cost-benefit sebagaimana dijelaskan dalam *Rational Choice Theory*. Keuntungan yang besar dan risiko penangkapan yang kecil membuat kejahatan ini menarik bagi banyak pelaku.

Kesempatan Kejahatan karena Kelemahan Sistem Keamanan

Kelemahan sistem keamanan informasi menjadi faktor kuat yang memungkinkan pencurian data terjadi. Dalam kriminologi, hal ini dijelaskan oleh *Routine Activity Theory*, yang menyatakan bahwa kejahatan terjadi ketika seorang pelaku termotivasi bertemu dengan target yang rentan tanpa adanya penjaga yang mampu (*capable guardian*). Sistem yang tidak terproteksi, penggunaan kata sandi lemah, minimnya enkripsi, atau celah keamanan pada aplikasi memberikan kesempatan bagi pelaku.

Faktor Psikologis dan Kepribadian Pelaku

Beberapa pelaku terdorong oleh faktor psikologis seperti rasa ingin tahu, dorongan untuk menguasai tantangan teknis, atau keinginan membuktikan kemampuan hacking. Ada pula pelaku yang memiliki ciri kepribadian antisosial atau rendah empati sehingga tidak mempertimbangkan dampak pada korban. Perspektif *cyber-psychology* menjelaskan bahwa lingkungan digital membuat pelaku merasa anonim sehingga mengurangi hambatan moral.

Pengaruh Sosial dan Lingkungan Jaringan Siber

Dalam *Differential Association Theory*, perilaku kriminal dipelajari melalui interaksi dengan kelompok sosial atau komunitas. Hal ini juga berlaku dalam kejahatan siber: pelaku belajar dan mendapatkan dukungan dari komunitas hacker, forum gelap, atau kelompok yang mempromosikan tindakan ilegal. Lingkungan pergaulan digital dapat mempengaruhi individu untuk melihat pencurian data sebagai tindakan yang normal atau bahkan prestisius.

Perkembangan Teknologi yang Semakin Kompleks

Kemajuan teknologi seperti kecerdasan buatan, malware canggih, dan otomatisasi memudahkan pelaku mencuri data dalam skala besar. Teknologi juga menciptakan sistem yang semakin terhubung, sehingga memperluas ruang serangan. Fenomena ini membuat pencurian data menjadi kejahatan yang semakin mudah dilakukan dan semakin sulit dideteksi.

Faktor Yang Melatarbelakangi Adanya Kejahatan Pencurian Data Dan Informasi Pribadi Terjadi Karena Beberapa Sebab, Diantaranya Yaitu Sebagai Berikut:

A. Human Error, Fitrah Manusia Yang Hobi Mempraktekkan Kebiasaan Ekonomis Diantaranya Dengan Mencari Free Software Atau Aplikasi Bajakan (Yang Biasanya Memberikan Iming-Iming Free Trial Atau Bonus-Bonus Lainnya) Memaksa Penggunanya Untuk Secara Suka Rela Memasukkan Data Pribadi Berupa Nomor Telepon di Situs Atau Aplikasi Yang Tidak Terjamin Keamanannya.

B. Serangan Malware, Manusia Lalai Dan Tidak Teliti Dalam Menerima Maupun Mengirim Email, Yang Berpotensi Menjadi Pintu Masuk Malware. Malware Pada Dasarnya Adalah Program Yang Dirancang Untuk Merusak Dengan Menyusup Ke Sistem Komputer, Salah Satu Jenis Malware Yang Berbahaya Yaitu Spyware. Menurut Salah Satu Vendor Antivirus Yang Sudah Mendunia Karsperky, Spyware Merupakan Software Yang Didesain Untuk Masuk Ke Dalam Perangkat Komputer Yang Mempunyai Kemampuan Mengumpulkan Data-Data Pribadi User Dan Mengirimnya Kepada Pihak Ketiga Tanpa Persetujuan User.
C. Social Engineering, Yaitu Penggunaan Manipulasi Psikologis Untuk Mengumpulkan Data Sensitive Seperti Nama Lengkap, Username, Password, Dan Sebagainya Melalui Media Elektronik Dengan Menyamar Sebagai Pihak Yang Dapat Dipercaya. Biasanya Phishing Memanfaatkan Email Untuk Mengelabui Korbannya. Email Yang Dikirimkan Pelaku Dapat Berisi Sesuatu Yang Mengatasnamakan Pihak Tertentu Dan Memancing Korban Untuk Meng-Klik Tautan Yang Tercantum Didalamnya.

Pencurian Data Pribadi Terbagi Menjadi 5 (Lima) Kategori Yaitu Sebagai Berikut:

1. Businnes/Commercial Identity Theft, Tipe Ini Menggunakan Nama Bisnis Dari Orang Lain Untuk Mengambil Kredit. Pelaku Jenis Ini Menggunakan Metode Pretexting Dalam Menjalankan Aksinya Yakni Menggunakan Identitas Atau Dengan Alasan Palsu Untuk Memperoleh Informasi Dari Korban. Criminal Identity Theft, Tipe Ini Beraksi Sebagai Orang Lain Ketika Akan Melakukan Tindakan Kejahatan.
2. Financial Identity Theft, Tipe Ini Menggunakan Identitas Orang Lain Untuk Memperoleh Kredit, Barang Serta Layanan Yang Dimiliki Oleh Orang Tersebut. Pelaku Jenis Ini Menggunakan Metode Skimming.
3. Identity Clonning, Tipe Ini Menggunakan Identitas Serta Informasi Yang Dimiliki Orang Lain Dalam Kehidupannya Sehari-Hari. Pelaku Jenis Ini Biasanya Menggunakan Metode System Exploit Jenis Password Cracking, Yakni Melakukan Tindakan Penebakan Password Degan Berbagai Metode, Yang Paling Banyak Dilakukandengan Metode Bruteforce Atau Menebak Dengan Menggunakan Daftar Kata.
4. Medical Identity Theft, Tipe Ini Menggunakan Identintas Orang Lain Untuk Memperoleh Layanan Kesehatan Dan Obat-Obatan. Pelaku Jenis Ini Menggunakan Metode Hamper Sama Dengan Jenis Nomor 4 Yakni Mencuri Identitas Pribadi Seseorang Untuk Kepentingan Mendapatka Layanan Kesehatan Dan Obat-Obatan Denga Memanfaatkan Data Pribadi Korban.

Kesimpulan

Berdasarkan analisis kriminologis dalam file, dapat disimpulkan bahwa pencurian data pribadi di era digital merupakan bentuk kejahatan siber yang berkembang seiring pesatnya teknologi informasi. Kejahatan ini muncul karena kombinasi antara lemahnya sistem keamanan digital, rendahnya literasi masyarakat, serta motif ekonomi pelaku.

Faktor seperti human error, serangan malware, dan social engineering menjadi penyebab paling umum yang membuka peluang bagi pelaku. Dampaknya sangat luas, meliputi kerugian finansial, gangguan psikologis seperti stres dan kecemasan, kerusakan reputasi sosial, hingga menurunnya kepercayaan publik terhadap lembaga keuangan dan layanan digital. Selain itu, implementasi UU Perlindungan Data Pribadi (UU PDP) dinilai masih belum optimal sehingga belum mampu memberikan perlindungan maksimal bagi masyarakat.

Saran

Dan Untuk menghadapi maraknya pencurian data pribadi, diperlukan langkah strategis dari berbagai pihak. Pemerintah perlu memperkuat implementasi UU PDP melalui penegakan hukum yang tegas, peningkatan pengawasan, serta membangun infrastruktur keamanan digital yang lebih baik. Lembaga keuangan dan penyedia layanan digital harus meningkatkan sistem keamanan, menerapkan kontrol internal yang ketat, dan memastikan data pengguna terlindungi dengan standar tinggi. Masyarakat juga perlu meningkatkan kewaspadaan dengan tidak mudah membagikan data pribadi, menghindari aplikasi yang tidak aman, serta memahami modus-modus kejahatan digital. Selain itu, kolaborasi antara pemerintah, industri, akademisi, dan masyarakat menjadi kunci penting untuk menciptakan ekosistem digital yang aman dan dipercaya.

Daftar Pustaka

Aditya, Komang Masya Surya, and I Gusti Ngurah Nyoman Krisnadi Yudiantara. "Analisis Kriminologi Dalam Tindak Pidana Pencurian Data Pribadi Di Era Digital." *Jurnal Media Akademik* 3, no. 2 (2025): 6.

Ahmad, M Razka Aditya, and Indah Sri Utari. "Perlindungan Hukum Pengguna E-Commerce : Perspektif Viktimologi Dalam Menghadapi Kejahatan Siber," 2008, 967–89.

Aritonang, Lenny Maria, Zyetwill Zyetwill, and Rara Handayani. "Analisis Hukum Terhadap Kebocoran Data Pribadi Dan Penyalahgunaan Identitas Dalam Perbankan Berdasarkan Undang-Undang Nomor 27 Tahun 2022 Tentang Perlindungan Data Pribadi." *Ranah Research : Journal of Multidisciplinary Research and Development* 7, no. 5 (2025): 3146–58. https://doi.org/10.38035/rrj.v7i5.1665.

Atara, Irvin, and Sharron Syallomeita. "ANALISIS KRIMINOLOGI TERHADAP PENCURIAN DATA PRIBADI DI ERA DIGITAL : STUDI KASUS KEBOCORAN DATA PENGGUNA APLIKASI MYPERTAMINA TAHUN 2023 Data MyPertamina Pada Mei 2023 , Yang Mengungkapkan Kerentanannya Infrastruktur" 3, no. 2 (2025): 129–40.

Febrianti, Reisha Resmalah, and Otto Yudianto. "Upaya Perlindungan Hukum Bagi Korban Tindak Pidana Pencurian Secara Digital." *Sosialita* 2, no. 1 (2023): 75–84.

Hidayat, Rahmad Sujud. "Tanggung Jawab Hukum Marketplace Terhadap Kebocoran Data Pribadi Pengguna Dalam Perspektif UU ITE Dan UU Perlindungan Data Pribadi" 4, no. 3 (2025): 7738–43.

Maulida, Difla Nur, Arfan Kaimuddin, and M Fahrudin Andriyansyah. "Tindak Pidana Pencurian Data Pribadi Di Internet." *Dinamika* 30 Nomor 1, no. 193 (2024): 9370–85.

Rahmadani, Ardita Esti, Yoga Pangestu, and Nur Halizhah. "Media Hukum Indonesia (MHI) Published by Yayasan Daarul Huda Krueng Mane Perlindungan Data Pribadi Di Era Digital: Tantangan Dan Solusi Dalam Sistem Perbankan" 2, no. 4 (2024): 180. https://doi.org/10.5281/zenodo.14060556.

Ramadani, Muhammad Yudistira. "Dampak Jangka Panjang Pelanggaran Data Terhadap Kesehatan Mental." *DATA BREACH CLASSACTIONS*, 2025, 1.

Ray, Swati, Joyati Das, Ranjana Pande, and A Nithya. "Tinjauan Yuridis Cybercrime Dalam Tindak Pidana Pencemaran Nama Baik Menurut Undang-Undang Republik Indonesia Nomor 1 Tahun 2024 Tentang Perubahan Kedua Atas Undang-Undang Nomor 11 Tahun 2oo8 Tentang Informasi Dan Transaksi Elektronik," 2024, 4.

Saptaning Ruju Paminto, Ahdi Hidayat, Bilkis Nabila, M. Raihan Husaeni, and Siti Jenar Maharani. "Perlindungan Hukum Bagi Korban Pencurian Data Dan Informasi Pribadi Di Era Kejahatan Siber." *Jurnal Dunia Ilmu Hukum (JURDIKUM)* 2, no. 2 (2024): 54–61. https://doi.org/10.59435/jurdikum.v2i2.453.

Siahaan, Tota Roganda, and Hudi Yusuf. "Tinjauan Kriminologi Terhadap Tindak Pidana Ekonomi Khusus: Faktor Penyebab Dan Dampak Sosial Di Masyarakat." *JIIC: Jurnal Intelek Insan Cendikia* 1, no. 9 (2024): Hlm. 5242-5257. https://jicnusantara.com/index.php/jiic/article/view/1440/1586.

Widyantari, Padma, and Adi Sulistiyono. "Jurnal Privat Law." *Pelaksanaan Harmonisasi Rancangan Undang-Undang Perlindungan Data Pribadi (Ruu Pdp)* 8, no. 1 (2020): 117–23.

Wira Pramudya, Deva, and Hudi Yusuf. "Pencurian Data Identitas Sebagai Kejahatan Cyber Related Crime: Tinjauan Kriminologis Atas Kasus Pencurian Data Pada Akun Marketplace Identity Data Theft as a Cyber Crime Related Crime: A Criminological Review of Marketplace Account Data Theft Cases." *Jurnal Intelek Insan Cendikia*, 2025, 13469–78. https://jicnusantara.com/index.php/jiic.