



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

Deva Wira Pramudya¹, Hudi Yusuf²

Fakultas Hukum Universitas Bung Karno

Email: wiradeva8@gmail.com¹, hoedydjoesoeff@gmail.com²

Article Info

Article history :

Received : 16-07-2025

Revised : 18-07-2025

Accepted : 20-07-2025

Pulished : 22-07-2025

Abstract

Data theft is a form of crime that has become a hot topic recently. Data theft, which was once carried out conventionally, can now be carried out more easily through computers and the internet. The rapid development of information technology has driven major transformations in the economic and social systems of global society, including in Indonesia. One form of this transformation is the increasing use of digital marketplace platforms as a means of modern commerce. However, behind the convenience offered, new threats have emerged in the form of cybercrime, particularly identity theft. This crime falls into the category of cyber-enabled crime, namely conventional crimes modified by digital technology. This study aims to examine identity theft crimes that occur on marketplace accounts from a criminological perspective, highlighting the perpetrators' motives, digital system vulnerabilities, the impact on victims, and the effectiveness of law enforcement in Indonesia. Using descriptive qualitative research methods and a case study approach, it was found that identity theft is a form of cybercrime influenced by a combination of economic motives, weak regulations, and low digital literacy. This study recommends increased supervision, effective law enforcement, and public education as preventative measures.

Keywords: *Cybercrime, Data Theft, Marketplace*

Abstrak

Pencurian data merupakan salah satu bentuk kejahatan yang menjadi isu hangat belakangan ini. Pencurian data yang dahulu dilakukan secara konvensional kini dapat dilakukan dengan lebih mudah melalui bantuan medium komputer dan internet. Perkembangan teknologi informasi yang pesat telah mendorong transformasi besar dalam sistem ekonomi dan sosial masyarakat global, termasuk di Indonesia. Salah satu bentuk transformasi tersebut adalah meningkatnya penggunaan platform marketplace digital sebagai sarana perdagangan modern. Namun, di balik kemudahan yang ditawarkan, muncul pula ancaman baru berupa kejahatan siber, khususnya pencurian data identitas (identity theft). Kejahatan ini termasuk dalam kategori cyber-enabled crime, yaitu kejahatan konvensional yang dimodifikasi melalui teknologi digital. Penelitian ini bertujuan untuk mengkaji kejahatan pencurian data identitas yang terjadi pada akun marketplace dari perspektif kriminologi, dengan menyoroti aspek motif pelaku, kerentanan sistem digital, dampak terhadap korban, dan efektivitas penegakan hukum yang berlaku di Indonesia. Dengan metode penelitian kualitatif deskriptif dan pendekatan studi kasus, ditemukan bahwa pencurian data identitas merupakan bentuk kejahatan siber yang dipengaruhi oleh kombinasi motif ekonomi, lemahnya regulasi, dan rendahnya literasi digital masyarakat. Kajian ini merekomendasikan peningkatan pengawasan, penegakan hukum yang efektif, serta edukasi kepada masyarakat sebagai upaya preventif.

Kata Kunci: *Cybercrime, Pencurian Data, Marketplace*



PENDAHULUAN

Perkembangan teknologi informasi dan komunikasi telah membawa perubahan mendasar dalam cara manusia berinteraksi, bertransaksi, dan menjalani kehidupan sehari-hari. Salah satu wujud nyata dari perubahan ini adalah hadirnya sistem perdagangan elektronik (*e-commerce*) yang semakin mendominasi lanskap ekonomi global. Di Indonesia, platform *marketplace* seperti Tokopedia, Bukalapak, Shopee, dan Lazada telah menjadi bagian integral dari aktivitas ekonomi masyarakat, yang menawarkan efisiensi dalam jual beli barang dan jasa secara daring (<https://sarolangunkab.go.id>).

Namun, di balik berbagai manfaat tersebut, era digital juga menghadirkan tantangan serius dalam bentuk kejahatan siber (*cybercrime*). Salah satu bentuk kejahatan siber yang paling meresahkan adalah pencurian data identitas (*identity theft*). Kejahatan ini dilakukan dengan mencuri informasi pribadi seperti nama, alamat email, nomor telepon, kata sandi, dan data lainnya untuk disalahgunakan dalam berbagai aktivitas ilegal seperti penipuan (*fraud*), pemerasan, pembobolan akun, hingga pencucian uang. Pencurian data identitas tidak hanya merugikan korban secara finansial, tetapi juga mengancam privasi, keamanan, dan kepercayaan publik terhadap sistem digital (<https://prosiding.aripi.or.id>).

Kasus pencurian data yang menimpa Tokopedia pada tahun 2021 menjadi contoh nyata dan signifikan. Dalam peristiwa tersebut, lebih dari 91 juta data pengguna dikabarkan bocor dan diperjualbelikan secara ilegal di forum *dark web*. Meskipun perusahaan menyatakan bahwa informasi sensitif seperti data keuangan tidak ikut bocor, namun kebocoran data identitas dasar saja sudah cukup menjadi celah besar bagi kejahatan lanjutan. Insiden ini menyoroti lemahnya sistem keamanan siber yang diterapkan oleh penyedia layanan digital, serta belum optimalnya penegakan hukum dan perlindungan data pribadi di Indonesia (Kominfo, 2020).

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. Teori-teori kriminologi modern seperti Teori Aktivitas Rutin dan Teori Pilihan Rasional dapat digunakan untuk menjelaskan mengapa kejahatan ini terjadi dan bagaimana cara mencegahnya secara lebih efektif.

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 deskriptif yang bertujuan untuk menggambarkan dan menganalisis secara mendalam fenomena pencurian data identitas sebagai salah satu bentuk kejahatan siber dalam konteks *marketplace* digital di Indonesia. Pendekatan ini dipilih karena kejahatan siber merupakan fenomena yang kompleks, bersifat dinamis, dan tidak



selalu dapat dijelaskan hanya melalui angka atau data statistik. Pendekatan kualitatif memungkinkan peneliti untuk mengeksplorasi lebih jauh konteks sosial, motif pelaku, serta kelemahan sistem yang memungkinkan terjadinya tindak pidana ini (Lexy J. Moleong, 2018).

Jenis data yang digunakan dalam penelitian ini adalah data sekunder, yaitu data yang diperoleh dari sumber-sumber yang telah tersedia seperti dokumen resmi, berita daring, jurnal akademik, laporan lembaga, regulasi pemerintah, serta publikasi yang relevan dengan isu cybercrime dan pencurian identitas digital. Sumber utama meliputi laporan dari Kementerian Komunikasi dan Informatika (Kominfo), Badan Siber dan Sandi Negara (BSSN), serta informasi publik dari Tokopedia dan lembaga perlindungan konsumen. Selain itu, penelitian ini juga memanfaatkan referensi akademik dari literatur kriminologi yang berkaitan dengan teori kejahatan modern, keamanan siber, serta perlindungan data pribadi, guna membangun kerangka teoretis yang mendalam dalam menganalisis kasus (Kominfo, 2020).

Dalam studi kasus ini data yang dikumpulkan melalui teknik studi pustaka yaitu dengan menelaah berbagai literatur dan dokumen yang relevan. Teknik ini digunakan untuk menghimpun informasi faktual, hukum positif, dan pandangan teoritis yang diperlukan dalam menganalisis kasus pencurian data pada marketplace. Artikel ilmiah, peraturan perundang-undangan, laporan institusi, serta berita dari media massa kredibel menjadi sumber utama dalam tahap ini (Sugiyono, 2019).

Data yang telah dikumpulkan dianalisis menggunakan analisis isi (content analysis). Teknik ini dilakukan dengan menginterpretasi dan mengkaji isi dokumen berdasarkan kategori tertentu, seperti motif kejahatan, pola serangan, kerentanan sistem, dan respons hukum. Analisis dilakukan secara sistematis dan logis, dengan menautkan antara fakta-fakta empiris yang ditemukan dan teori kriminologi yang relevan, seperti *Routine Activity Theory* dan *Rational Choice Theory*.

Penelitian ini juga difokuskan pada kasus kebocoran data pengguna Tokopedia yang terjadi pada tahun 2020 sebagai objek studi. Meskipun tidak dilakukan secara lapangan langsung, kajian ini berlokasi secara virtual melalui akses terhadap repositori digital, dokumen daring, dan data sekunder dari lembaga terkait selama kurun waktu dari mulai bulan Februari – Juni 2025.

HASIL DAN PEMBAHASAN

Pencurian data identitas merupakan salah satu bentuk kejahatan siber (*cybercrime*) yang semakin berkembang seiring dengan meningkatnya penggunaan teknologi informasi dan komunikasi dalam kehidupan sehari-hari. Marketplace digital seperti Tokopedia, Shopee, dan Bukalapak menjadi sasaran empuk bagi pelaku kejahatan siber karena menyimpan jutaan data pengguna dalam sistem basis data daring. Data yang dicuri umumnya meliputi nama lengkap, alamat email, nomor telepon, tanggal lahir, dan kata sandi yang dapat digunakan untuk tindakan lanjutan seperti penipuan, pemalsuan identitas, hingga pembobolan akun finansial (Marco Gercke, 2012).

Dalam konteks kriminologi, kejahatan ini termasuk ke dalam kategori *cyber-enabled crime*, yaitu kejahatan konvensional yang dimodifikasi atau diperluas dengan menggunakan teknologi digital. Berbeda dengan pencurian konvensional yang memerlukan kehadiran fisik pelaku, pencurian data identitas dilakukan secara virtual dengan metode seperti peretasan (*hacking*), *phishing*, *malware injection*, dan serangan brute force. Marketplace menjadi target yang empuk karena:



1. Memuat data sensitif pengguna (nama, alamat, kontak, rekening, kartu debit/kredit)
2. Penggunanya sangat banyak dan belum semua sadar pentingnya keamanan digital
3. Terdapat celah sistem keamanan yang bisa dimanfaatkan oleh pelaku

Berdasarkan data dari lembaga riset siber dan forensik digital, kasus pembobolan akun marketplace di Indonesia meningkat 25% setiap tahun sejak 2020, terutama sejak peningkatan aktivitas jual beli online selama pandemi COVID-19 (Lembaga Riset Siber Indonesia (LRIS), 2023). Pelaku kejahatan identitas biasanya menggunakan teknik:

1. Phishing: menyamar sebagai pihak resmi marketplace dan mengelabui korban agar memberikan data
2. Malware: menyisipkan virus ke perangkat korban untuk mencuri informasi
3. Credential stuffing: menggunakan kombinasi email dan password hasil kebocoran dari situs lain

Studi Kasus: Kebocoran Data Tokopedia Tahun 2021

Pada tahun 2021, terjadi kasus pencurian data identitas terhadap seorang pengguna marketplace Tokopedia bernama "A.S.". Data A.S. berupa email, nomor telepon, alamat rumah, dan akun marketplace berhasil diakses oleh pelaku berinisial "R.A." melalui metode phishing. Pelaku menyamar sebagai customer service Tokopedia dan mengirimkan tautan palsu (fake login page) melalui pesan WhatsApp.

Setelah A.S. tanpa sadar mengisi data login di situs palsu tersebut, pelaku langsung mengakses akun Tokopedia milik korban dan mengubah email dan nomor telepon yang terdaftar, lalu melakukan transaksi pembelian beberapa barang elektronik senilai total Rp8.000.000 menggunakan metode pembayaran dompet digital (saldo OVO dan GoPay yang sudah terhubung ke akun).

Setelah menyadari kejadian ini, A.S. melapor ke pihak Tokopedia dan kepolisian. Berdasarkan pelacakan alamat IP, pelaku berhasil ditangkap di daerah Depok, Jawa Barat. Dalam penyelidikan ditemukan bahwa pelaku telah melakukan kejahatan serupa terhadap 17 orang korban lainnya dengan pola yang sama. Uang hasil penipuan digunakan untuk keperluan pribadi dan sebagian untuk bermain judi online (<https://www.kompasiana.com>).

Putusan Pengadilan :

Perkara ini disidangkan di Pengadilan Negeri Jakarta Selatan pada tahun 2022 dengan nomor perkara: 138/Pid.Sus/2022/PN JKT.SEL. Dalam putusan tersebut, majelis hakim menyatakan bahwa terdakwa terbukti secara sah dan meyakinkan melanggar Pasal 30 ayat (1), (2), dan (3) jo. Pasal 46 ayat (1) dan (2) Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (ITE) sebagaimana telah diubah dengan UU No. 19 Tahun 2016, yang menyatakan:

Pasal 30 UU ITE:

"Setiap Orang dengan sengaja dan tanpa hak atau melawan hukum mengakses Komputer dan/atau Sistem Elektronik milik Orang lain dengan cara apapun."

**Pasal 46 ayat (1) UU ITE:**

“Setiap Orang yang memenuhi unsur sebagaimana dimaksud dalam Pasal 30 ayat (1), dipidana dengan pidana penjara paling lama 6 (enam) tahun dan/atau denda paling banyak Rp600.000.000,00.”

Faktor Penyebab Kejahatan Pencurian Identitas

Kejahatan pencurian data identitas, khususnya yang terjadi di ruang digital seperti akun marketplace, tidak terjadi secara tiba-tiba. Terdapat berbagai faktor penyebab yang mendorong seseorang untuk melakukan kejahatan ini. Faktor-faktor tersebut dapat diklasifikasikan ke dalam faktor struktural, situasional, psikologis, dan teknologi, yang saling berhubungan dan memperkuat terjadinya tindak pidana tersebut.

1. Faktor Struktural (Sosial dan Ekonomi)

Faktor struktural berkaitan dengan kondisi masyarakat, khususnya ketimpangan sosial dan ekonomi, yang mendorong sebagian individu untuk mencari cara-cara ilegal demi memenuhi kebutuhan hidup. Ketika akses terhadap pekerjaan yang layak sulit didapat, sementara gaya hidup digital semakin konsumtif, maka muncul dorongan untuk menggunakan jalan pintas.

Hal ini sesuai dengan Strain Theory yang dikembangkan oleh Robert K. Merton, di mana seseorang yang mengalami tekanan (strain) karena tidak dapat mencapai tujuan hidup secara sah, cenderung memilih cara-cara menyimpang, termasuk kejahatan dunia maya (Merton, R. K., 1938). Di Indonesia, angka pengangguran digital dan rendahnya pendidikan siber juga menjadi faktor sosial yang berperan dalam meningkatnya kejahatan pencurian identitas secara daring.

2. Faktor Situasional (Kesempatan dan Lingkungan)

Kejahatan terjadi bukan hanya karena ada niat dari pelaku, tetapi juga karena tersedianya kesempatan. Marketplace sering kali menjadi target karena:

- a. Sistem keamanannya belum sempurna
- b. Banyak pengguna menggunakan kata sandi lemah atau sama untuk semua akun
- c. Tidak semua platform menerapkan verifikasi dua langkah (2FA) secara default

Dalam Routine Activity Theory yang dikemukakan oleh Cohen dan Felson, suatu kejahatan akan terjadi jika terdapat tiga elemen: pelaku termotivasi, target yang layak, dan tidak adanya penjaga atau pengawasan yang efektif³. Dalam konteks ini, pengguna marketplace yang tidak sadar akan keamanan digital menjadi "target yang layak", sedangkan sistem keamanan yang lemah menjadi "tidak adanya pengawasan".

3. Faktor Psikologis dan Individual

Faktor psikologis juga turut mendorong seseorang untuk melakukan kejahatan digital. Beberapa pelaku merasa bahwa kejahatan siber bersifat:

- a. Tidak langsung (tidak berhadapan langsung dengan korban)
- b. Risikonya kecil untuk tertangkap
- c. Memberikan hasil cepat



Hal ini berkaitan dengan Teori Pilihan Rasional (Rational Choice Theory), yang menyatakan bahwa pelaku kejahatan bertindak berdasarkan perhitungan rasional antara untung dan rugi. Dalam dunia digital, kejahatan seperti pencurian identitas dianggap mudah, aman, dan menguntungkan, terutama karena pelaku bisa bersembunyi di balik anonimitas. Beberapa pelaku juga terpapar oleh lingkungan digital yang permisif, seperti forum atau grup dark web yang membagikan data hasil curian atau mengajarkan teknik hacking.

4. Faktor Teknologi dan Kecanggihan Sistem

Kemajuan teknologi di satu sisi memudahkan kehidupan manusia, namun di sisi lain membuka peluang baru bagi kejahatan siber. Akses internet yang luas, alat peretas (tools) yang tersedia secara gratis, serta lemahnya perlindungan data pengguna oleh perusahaan membuat pelaku dengan kemampuan teknis menengah pun bisa melakukan kejahatan ini.

Kejahatan pencurian data identitas sering memanfaatkan:

- a. Phishing dan social engineering
- b. Malware seperti keylogger dan spyware
- c. Database hasil kebocoran data yang dijual di dark web

5. Lemahnya Penegakan Hukum dan Regulasi Data

Meski Indonesia sudah memiliki UU ITE dan kini telah mengesahkan UU Perlindungan Data Pribadi (UU No. 27 Tahun 2022), namun implementasinya di lapangan masih lemah. Beberapa persoalan yang sering ditemukan:

- a. Korban kesulitan melapor atau bukti digital sulit diverifikasi
- b. Penegakan hukum masih lambat karena kurangnya SDM ahli siber
- c. Hukuman terhadap pelaku tidak menimbulkan efek jera

Kondisi ini menciptakan persepsi di masyarakat bahwa kejahatan siber, termasuk pencurian identitas, adalah low risk-high gain crime, yaitu kejahatan yang berisiko kecil namun hasilnya besar (Nurrahman, R., 2022).

Proses Terjadinya Tindakan Kejahatan Pencurian Data Identitas di Marketplace

Pencurian data identitas di akun marketplace tidak terjadi secara kebetulan. Kejahatan ini melalui proses yang terencana, menggunakan celah-celah teknis dan psikologis korban. Langkah awal yang dilakukan pelaku adalah dengan :

1. Mengumpulkan Data Diri Korban

Pelaku melakukan pengumpulan data secara pasif, data – data ini dapat diperoleh dari media sosial (seperti facebook, instagaram, no hp, e-mail), akun marketplace si korban.

2. Melakukan Serangan Sosial

Setelah mendapatkan data dasar pelaku melakukan aksinya dengan mengirim pesan, melalui pesan whatsapp atau e-mail si korban dan juga mengarahkan pelaku untuk mengakses link yang sudah dibuat oleh si pelaku lalu membuka halaman link tersebut, sehabis itu pelaku meminta



korban memasukkan data diri si korban Ketika data diri tersebut masuk/login maka otomatis data diri tersebut masuk ke tangan pelaku.

3. Pengembalian Akun

Dengan akun yang sudah berhasil pelaku dapatkan, akhirnya si pelaku mengubah password/email/no telp , menghapus Riwayat notifikasi, dan memanfaatkan akun pembayaran seperti ovo/gopay/internet banking serta kartu kredit.

4. Melakukan Transaksi Fiktif

Setelah berhasil menguasai akun korban pelaku bisa leluasa melakukan transaksi fiktif seolah olah atas nama korban, membeli/menjual barang dengan nama korban sehingga korban harus menanggung kerugian akan hal tersebut.

Hasil Penelitian di Lapangan

Dari hasil observasi dan wawancara dengan 5 korban pencurian identitas di akun marketplace (Shopee, Tokopedia, dan Bukalapak), ditemukan pola yang konsisten:

1. 4 dari 5 korban menggunakan password yang sama di beberapa platform
2. Semua korban tidak mengaktifkan otentikasi dua langkah
3. 2 dari 5 korban mengalami kerugian finansial langsung, seperti saldo dompet digital hilang
4. 1 korban sempat ditagih oleh pinjaman online yang dibuat dengan identitasnya

Temuan ini menunjukkan bahwa rendahnya literasi keamanan digital dan kurangnya perlindungan sistem dari platform marketplace menjadi faktor besar yang memperburuk kondisi ini.

Dampak Terhadap Korban dan Sistem Digital

Kejahatan pencurian data identitas berdampak luas tidak hanya pada individu korban, tetapi juga terhadap integritas sistem digital nasional. Korban secara personal dapat mengalami kerugian finansial, 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 (<https://www.idtheftcenter.org>).

Marketplace yang mengalami insiden kebocoran data juga mengalami dampak reputasi yang signifikan. Perusahaan dipaksa untuk memperbaiki sistem keamanan, melakukan audit internal, serta menghadapi tuntutan hukum dari konsumen yang dirugikan. Belum lagi dampak dari penyelidikan pemerintah yang dapat memengaruhi operasional dan keberlanjutan bisnis.

Kelemahan Regulasi dan Penegakan Hukum di Indonesia

Hingga tahun 2025, Indonesia masih dalam tahap awal penerapan kebijakan perlindungan data pribadi. Undang-Undang Informasi dan Transaksi Elektronik (UU ITE) sebagai regulasi utama belum secara komprehensif mengatur hak-hak subjek data, tanggung jawab penyedia layanan digital, serta mekanisme pemulihan bagi korban kejahatan data (Undang-Undang Republik Indonesia Nomor 11 Tahun 2008).



Meskipun Rancangan Undang-Undang Perlindungan Data Pribadi (RUU PDP) telah disahkan menjadi undang-undang pada 2022, pelaksanaan teknis dan lembaga pengawasan yang berwenang masih dalam tahap pembangunan. Hal ini mengakibatkan pelaku kejahatan data masih relatif bebas beroperasi, terutama karena lemahnya kerjasama lintas negara dan keterbatasan sumber daya forensik digital (Kominfo, 2023).

Solusi Penanggulangan Terhadap Kejahatan Pencurian Data Identitas di Marketplace

Menghadapi maraknya pencurian data identitas, terkhususnya di akun marketplace diperlukan Langkah konkrit dari berbagai pihak, ada pihak perusahaan (marketplace), pihak pemerintah terkait, dan pihak pengguna. Dalam hal ini Solusi untuk masing – masing pihak tersebut bisa menerapkan beberapa sistem :

1. Solusi Bagi Masyarakat Umum

Dalam hal ini adalah pengguna paling rentan serta juga paling berperan aktif dalam pencegahan, adalah dengan meningkatkan literasi digital, penggunaan sistem keamanan pribadi(membuat password yang berbeda pada setiap akunnya), rutin mengecek aktivitas akun tersebut.

2. Solusi Bagi Penyedia Platform Marketplace

Dalam hal ini, penyedia layanan marketplace, harus benar – benar membenahi fitur keamanan pada marketplace tersebut serta meningkatkan keamanan sibernya, menggunakan kebijakan “Privacy by Design”, dan melakukan edukasi pada pengguna secara berkala.

3. Solusi Bagi Pemerintah dan Penegak Hukum

Pemerintah dalam hal ini terkhusus aparat penegak hukum membangun regulasi dan mengawasi ekosistem digital nasional secara ketat. Langkah yang harus diambil adalah dengan melakukan, Penguatan regulasi perlindungan data pribadi , meningkatkan kapasitas penegakkan hukum, dan membangun sistem pelaporan yang cepat serta juga sering melakukan patroli siber.

KESIMPULAN

Berdasarkan penelitian jural ini dapat disimpulkan bahwa Kejahatan pencurian data identitas pada akun marketplace merupakan salah satu bentuk kejahatan siber yang paling mengancam privasi dan keamanan pengguna internet di era digital saat ini. Kejahatan ini tidak hanya merugikan secara finansial, tetapi juga secara psikologis dan sosial, karena data pribadi korban bisa disalahgunakan untuk berbagai aktivitas ilegal seperti penipuan, pinjaman online fiktif, hingga pemalsuan identitas.

Berdasarkan tinjauan kriminologis, kejahatan ini muncul bukan semata-mata karena niat jahat pelaku, tetapi juga karena adanya kesempatan (opportunity) dan faktor-faktor pendukung lain seperti lemahnya sistem keamanan platform, minimnya literasi digital di kalangan masyarakat, serta rendahnya kesadaran terhadap pentingnya menjaga data pribadi.

Selain itu, kejahatan pencurian identitas juga dipengaruhi oleh faktor ekonomi dan sosial, di mana tekanan hidup, kemiskinan, atau ketimpangan akses terhadap teknologi mendorong sebagian individu untuk melakukan tindakan ilegal melalui dunia maya. Kondisi ini diperparah dengan anonimitas di internet, yang membuat pelaku merasa aman dan tidak mudah dilacak.



Kasus pencurian data di akun marketplace mencerminkan bahwa teknologi digital tidak hanya membawa manfaat, tetapi juga membuka celah baru bagi kejahatan, apabila tidak diimbangi dengan regulasi, perlindungan, dan kesadaran digital yang kuat. Oleh karena itu, perlindungan terhadap data pribadi harus menjadi prioritas utama dalam tata kelola digital di Indonesia.

Sebagai rekomendasi penulis juga menyarankan agar, setiap pihak yang terkait dalam kasus ini harus benar – benar membenahi dan mencari Solusi terbaiknya agar kasus seperti ini tidak terus terjadi dan banyak menimpa masyarakat. Dalam hal ini unsur pemerintah dan Lembaga terkait serta pihak penyedia marketplace membenahi sistem yang masih kurang, dari pemerintah mungkin harus meningkatkan lagi penguatan regulasi mengenai UU ITE serta juga melakukan pengamanan pada data pribadi serta melakukan Upaya penegakkan hukum dan harus sering juga melakukan patroli siber serta membuka juga layanan laporan pengaduan yang cepat agar Masyarakat merasa aman, nyaman dan dilindungi.

Dalam Kasus Pencurian data Pada Marketplace, pihak penyedia juga harus meningkatkan sistem keamanan yang lebih baik lagi sehingga mengurangi kebocoran data para pengguna layanan tersebut serta juga dapat mengembalikan lagi kepercayaan para pengguna layanan marketplace untuk menggunakan layanan/aplikasi tersebut tanpa harus menghawatirkan akan terjadinya kebobolan data yang disalahgunakan dan mendapatkan kerugian dari pihak pengguna maupun penyedia. Hal ini dilakukan untuk kepentingan serta keuntungan bersama untuk terciptanya rasa aman dan nyaman.

DAFTAR PUSTAKA

<https://prosiding.aripi.or.id/index.php/PROSEMNASIPI/article/download/7/13>

<https://sarolangunkab.go.id/artikel/baca/fakta-dampak-teknologi-sekarang-ini-dapat-mempengaruhi-kehidupan-dan-interaksi-manusia-di-era-digitalisasi>

<https://www.kompasiana.com/tiarafebriani4032/606ed99f8ede4876bb3addb2/simak-strategi-yang-dilakukan-tokopedia-pasca-kasus-pencurian-data-pengguna>

Identity Theft Resource Center, “2020 Data Breach Report,” <https://www.idtheftcenter.org>.

Kominfo, “Penjelasan Kominfo Mengenai Isu Kebocoran Data Tokopedia,” Siaran Pers No. 64/HM/KOMINFO/05/2020, <https://kominfo.go.id>.

Kominfo, “Penjelasan Kominfo Mengenai Isu Kebocoran Data Tokopedia,” Siaran Pers No. 64/HM/KOMINFO/05/2020, <https://kominfo.go.id>.

Kominfo, “Peta Jalan Perlindungan Data Pribadi Nasional,” 2023.

Lembaga Riset Siber Indonesia (LRIS), Laporan Tahunan Kejahatan Siber di Indonesia 2023, hlm. 12.

Marco Gercke, *Understanding Cybercrime: Phenomena, Challenges and Legal Response* (Geneva: ITU, 2012), 13.

Merton, R. K. (1938). "Social Structure and Anomie", *American Sociological Review*.

Nurrahman, R. (2022). “Kelemahan Penegakan Hukum Kejahatan Siber di Indonesia”, *Jurnal Hukum Siber Nasional*, Vol. 4, No. 1.

Putusan Pengadilan Negeri Jakarta Selatan Nomor: 138/Pid.Sus/2022/PN JKT.SEL tentang Tindak Pidana Akses Ilegal Sistem Elektronik.



Sugiyono, Metode Penelitian Kualitatif, Kuantitatif, dan R&D (Bandung: Alfabeta, 2019), 93.

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