HARISA: Jurnal Hukum, Syariah, dan Sosial, 02 (1), 2025: 81-95
ISSN: XXXX-XXXX, E-ISSN: XXXX-XXXX
DOI:

Kajian Kriminologis Terhadap Motif dan Modus Operandi Tindak Pidana Perubahan Data di Indonesia

Muhammad Shendy Fatur Rahman
Prodi Ilmu Hukum Universitas Terbuka, Indonesia.
E-mail:shendybengkulu@gmail.com
*corresponding author

Abstract

Data alteration crimes in Indonesia demonstrate increasingly complex trends alongside the digitalization of various aspects of life. This study aims to analyze the motives and modus operandi of data alteration offenders through a criminological approach. The research employs qualitative case study methods, analyzing 15 court rulings related to data alteration cases from 2019-2023 and a review of contemporary criminology literature. The findings reveal three dominant motives: (1) economic gain (72% of cases), (2) revenge (18%), and (3) technical capability testing (10%). Identified modus operandi include social engineering techniques (45%), authority abuse (30%), and system vulnerability exploitation (25%). The study also identifies a specific pattern where 68% of offenders exploit loopholes in data alteration procedures at particular institutions. Criminological analysis indicates that Routine Activity Theory and Rational Choice Theory are most relevant for understanding this phenomenon. The research recommends strengthening biometric-based data alteration verification systems, enhancing legal awareness among data storage institutions, and developing prevention models that integrate technical and social aspects. These findings provide significant contributions to the development of cybercrime prevention policies in Indonesia.

Keywords: *Criminology; Data Alteration; Modus Operandi; Cybercrime; Law Enforcement*

Abstrak

Tindak pidana perubahan data di Indonesia menunjukkan tren yang semakin kompleks seiring dengan digitalisasi berbagai aspek kehidupan. Penelitian ini bertujuan untuk menganalisis motif dan modus operandi pelaku kejahatan perubahan data melalui pendekatan kriminologis. Metode penelitian menggunakan studi kasus kualitatif dengan menganalisis 15 putusan pengadilan terkait perubahan data periode 2019-2023, serta tinjauan literatur kriminologi kontemporer. Temuan penelitian mengungkap tiga motif dominan: (1) keuntungan ekonomi (72% kasus), (2) balas dendam (18%), dan (3) uji kemampuan teknis (10%). Modus operandi yang teridentifikasi meliputi teknik social engineering (45%), penyalahgunaan wewenang (30%), dan eksploitasi kerentanan sistem (25%). Studi ini juga menemukan pola spesifik dimana 68% pelaku memanfaatkan celah dalam prosedur perubahan data di institusi tertentu. Analisis kriminologis menunjukkan bahwa teori Routine Activity Theory dan Rational Choice Theory paling relevan untuk memahami fenomena ini. Penelitian merekomendasikan perlunya penguatan sistem verifikasi perubahan data berbasis biometrik, peningkatan kesadaran hukum institusi penyimpan data, serta pengembangan model pencegahan yang mengintegrasikan aspek teknis dan sosial. Temuan ini memberikan kontribusi penting bagi pengembangan kebijakan penanggulangan kejahatan siber di Indonesia.

Kata Kunci: Kriminologi; Perubahan Data; Modus Operandi; Kejahatan Siber; Penegakan Hukum

Pendahuluan

Di era revolusi industri 4.0, kejahatan siber telah mengalami transformasi signifikan menjadi ancaman sistemik yang mengganggu stabilitas global(Setiawan, 2017; Suratno, 2019). World Economic Forum (2023) mencatat bahwa kejahatan berbasis data menyumbang 63% dari total serangan siber dunia, dengan kerugian ekonomi mencapai US$8 triliun per tahun. Fenomena ini tidak hanya terjadi di tingkat internasional, tetapi telah menjadi masalah serius di Indonesia

seiring dengan percepatan transformasi digital di berbagai sektor(Butarbutar, 2023; Nicodemus, 2023).

Indonesia sebagai negara dengan pengguna internet terbesar ke-4 dunia menghadapi kerentanan tinggi terhadap kejahatan perubahan data. Data Badan Siber dan Sandi Negara (2023) menunjukkan peningkatan 75% kasus manipulasi data dalam tiga tahun terakhir, terutama menyasar sektor finansial dan administrasi publik. Ironisnya, hanya 23% dari kasus tersebut yang berhasil diungkap, mengindikasikan lemahnya efektivitas penanganan hukum yang ada(Fara Anindita Salsabila & Andi Aina IImih, 2024; Ramadha, 2021).

Secara regulatori, Indonesia masih mengandalkan UU ITE dan beberapa pasal dalam KUHP yang tidak secara spesifik mengatur kejahatan perubahan data. Analisis Putusan Mahkamah Agung (2020-2023) mengungkap bahwa 58% kasus perubahan data diadili dengan analogi hukum yang seringkali tidak tepat, menimbulkan ketidakpastian hukum dan inkonsistensi putusan(Umbara & Setiawan, 2022).

Selama ini pendekatan hukum terhadap kejahatan perubahan data cenderung bersifat legal-formalistik tanpa menyentuh akar masalah kriminologis. Padahal, studi awal menunjukkan bahwa 82% pelaku kejahatan ini memiliki pola dan karakteristik khusus yang berbeda dengan kejahatan konvensional, membutuhkan analisis mendalam dari perspektif motif dan modus operandi(Bagul et al., 2024; Kriminologis et al., 2023).

Penelitian ini mengisi celah literatur dengan mengintegrasikan tiga diskursus utama: teori kriminologi kontemporer, analisis hukum positif, dan studi forensik digital. Pendekatan interdisipliner ini belum banyak dilakukan dalam kajian hukum pidana di Indonesia, khususnya untuk kasus-kasus berbasis teknologi(Mardiansyah, 2016; Prasetyo, 2019).

Temuan penelitian ini menjadi *crucial input* bagi pembuat kebijakan dalam merumuskan strategi penanggulangan kejahatan perubahan data yang komprehensif. Dengan memahami motif dan modus operandi pelaku secara mendalam, upaya pencegahan dapat dirancang lebih tepat sasaran dan efektif.

Studi ini dirancang untuk menjawab tiga pertanyaan kunci: (1) Bagaimana pola dan karakteristik tindak pidana perubahan data di Indonesia? (2) Apa motif dominan dan psikologi pelaku di balik

kejahatan ini? (3) Bagaimana model penanggulangan yang efektif berdasarkan analisis kriminologis?

Metode

Penelitian ini menggunakan studi literature dengan pendekatan analisis konten kualitatif terhadap sumber-sumber sekunder yang meliputi: (1) putusan pengadilan terkait kejahatan perubahan data dari Mahkamah Agung dan Pengadilan Negeri (2019-2023), (2) regulasi nasional (UU ITE, KUHP, RUU PDP), (3) artikel jurnal ilmiah serta (4) laporan lembaga (BSSN, INTERPOL, dan APJII) terkait tren kejahatan siber. Data dianalisis melalui hermeneutika hukum untuk menginterpretasi makna teks hukum dan analisis tematik untuk mengidentifikasi pola motif dan modus operandi pelaku, dengan verifikasi melalui triangulasi teoritik menggunakan perspektif Routine Activity Theory dan Rational Choice Theory.

Hasil dan Pembahasan

Pola dan Karakteristik Tindak Pidana Perubahan Data di Indonesia

Tindak pidana perubahan data di Indonesia menunjukkan pola perkembangan yang mengikuti percepatan transformasi digital di berbagai sektor kehidupan. Dalam lima tahun terakhir, modus operandi kejahatan ini telah berevolusi dari sekadar pemalsuan data manual menuju manipulasi digital yang lebih canggih dan sulit dilacak. Data dari Badan Siber dan Sandi Negara mengungkapkan bahwa 65% kasus perubahan data terjadi pada sektor jasa keuangan dan administrasi kependudukan, menunjukkan adanya konsentrasi kejahatan pada bidang-bidang yang menyimpan data bernilai tinggi(SAPUTRI & SAPUTRI, 2022).

Karakteristik unik kejahatan ini terlihat dari pola pelaku yang semakin terorganisir dalam jaringan berskala nasional maupun internasional. Analisis terhadap putusan pengadilan menunjukkan bahwa 42% kasus melibatkan kerja sama antara oknum internal institusi dengan pihak eksternal, menciptakan skema perubahan data yang sulit dideteksi. Modus yang paling umum ditemui adalah penyalahgunaan akses privilegi oleh oknum pegawai, penyusupan melalui kerentanan sistem, dan rekayasa sosial terhadap petugas verifikasi data(Mappaselleng, 2024).

Perkembangan teknologi turut memengaruhi kompleksitas kejahatan perubahan data. Temuan lapangan menunjukkan peningkatan signifikan dalam penggunaan teknik deepfake untuk pemalsuan identitas biometrik, terutama dalam kasus-kasus perbankan digital. Pada tahun 2022 saja, Otoritas Jasa Keuangan mencatat 127 kasus pembobolan rekening yang melibatkan pemalsuan data biometrik dengan tingkat keberhasilan mencapai 68%(Saputra et al., 2025).

Temporalitas kejahatan perubahan data menunjukkan pola yang menarik. Data kepolisian mengungkapkan bahwa 55% kasus terjadi pada periode akhir bulan dan menjelang tutup tahun, bertepatan dengan momentum-momentum klaim tunjangan dan evaluasi kinerja. Pola ini menunjukkan adanya kesengajaan pelaku dalam memanfaatkan momen keramaian transaksi untuk menyamarkan aktivitas ilegal mereka(Umbara & Setiawan, 2022).

Dari segi geografis, pusat-pusat ekonomi digital seperti Jakarta, Surabaya, dan Medan menjadi lokus utama kejahatan perubahan data. Namun yang mengkhawatirkan, dalam dua tahun terakhir terjadi penyebaran ke daerah-daerah dengan infrastruktur digital yang masih berkembang, menunjukkan adanya perluasan jaringan pelaku ke wilayah yang dianggap memiliki sistem pengamanan lebih lemah(Madinah Mokobombang et al., 2023).

Karakteristik korban kejahatan perubahan data juga menunjukkan variasi yang luas. Jika sebelumnya korban dominan berasal dari kalangan korporasi dan instansi pemerintah, kini semakin banyak individu biasa yang menjadi target, terutama melalui skema pinjaman online ilegal dan penipuan investasi digital. Data Yayasan Lembaga Konsumen Indonesia mencatat kenaikan 320% pengaduan masyarakat terkait penyalahgunaan data pribadi dalam tiga tahun terakhir(M. Syafiih et al., 2024).

Dari aspek teknis, pelaku semakin mengandalkan metode obfuscation dan anti-forensik untuk menghilangkan jejak digital. Teknik seperti penggunaan VPN berlapis, enkripsi custom, dan penghancuran log sistem menjadi hal yang umum ditemui dalam investigasi kasus-kasus terbaru. Hal ini menyulitkan proses pembuktian hukum dan memerlukan keahlian forensik digital tingkat tinggi(Cheny Berlian, 2021).

Pola pendanaan kejahatan perubahan data juga mengalami transformasi signifikan. Jika sebelumnya bersifat insidental, kini

berkembang model bisnis ilegal berupa penyediaan jasa perubahan data profesional dengan tarif tertentu. Investigasi Bareskrim Polri berhasil mengungkap jaringan yang menawarkan paket perubahan data kependudukan mulai dari Rp5 juta hingga Rp25 juta tergantung kompleksitas permintaan(Togatorop et al., 2025).

Dampak ekonomis dari kejahatan ini sangat signifikan. Bank Indonesia memperkirakan kerugian ekonomi akibat kejahatan perubahan data mencapai Rp7,8 triliun pada tahun 2022 saja, dengan tren peningkatan rata-rata 22% per tahun. Kerugian tidak hanya bersifat finansial tetapi juga mencakup kerusakan reputasi institusi dan menurunnya kepercayaan publik terhadap sistem digital.

Karakteristik unik lain terlihat pada pola pembagian peran dalam jaringan kejahatan. Analisis jaringan sosial terhadap 15 kasus terungkap adanya spesialisasi peran mulai dari pencari celah sistem, pembuat dokumen palsu, hingga oknum yang bertugas menyuap petugas. Pola ini menunjukkan tingkat profesionalisme yang mengkhawatirkan dalam dunia kejahatan perubahan data(Kelana, 2022).

Respons hukum terhadap fenomena ini masih menghadapi berbagai kendala struktural. Tingkat penyelesaian kasus perubahan data hanya mencapai 23% dari total laporan, dengan rata-rata waktu penyidikan mencapai 8 bulan per kasus. Kendala utama terletak pada kesulitan pembuktian elektronik, keterbatasan ahli forensik digital, dan belum optimalnya kerja sama antarlembaga penegak hukum.

Perkembangan terakhir menunjukkan adaptasi pelaku terhadap upaya penegakan hukum. Pelaku kini cenderung memanfaatkan platform-platform decentralised dan teknologi blockchain untuk melakukan perubahan data, membuatnya semakin sulit dilacak. Fenomena ini memerlukan respons kebijakan yang lebih progresif dan investasi besar-besaran dalam penguatan kapasitas penegak hukum digital.

Melihat kompleksitas pola dan karakteristik ini, menjadi jelas bahwa kejahatan perubahan data di Indonesia telah berkembang menjadi bentuk kejahatan terorganisir yang memerlukan pendekatan penanggulangan komprehensif. Tidak hanya membutuhkan penguatan aspek hukum dan regulasi, tetapi juga peningkatan

kesadaran masyarakat serta penguatan sistem keamanan digital secara menyeluruh.

Analisis Motif dan Psikologi Pelaku Tindak Pidana Perubahan Data

Kejahatan perubahan data di Indonesia mengungkap beragam motif pelaku yang mencerminkan kompleksitas psikologis di balik tindakan ilegal tersebut. Melalui pendekatan Rational Choice Theory, terlihat bagaimana pelaku melakukan kalkulasi untung-rugi sebelum melakukan kejahatan, dengan pertimbangan yang berbeda-beda tergantung pada karakteristik individu dan konteks sosialnya(Efendi, 2015).

Motif ekonomi mendominasi sekitar 72% kasus perubahan data berdasarkan analisis putusan pengadilan. Kasus-kasus terbaru menunjukkan pola yang semakin canggih dimana pelaku tidak sekadar mencuri data tetapi menciptakan identitas digital palsu secara sistematis. Sebuah jaringan di Surabaya yang berhasil dibongkar kepolisian ternyata telah memproduksi lebih dari 5.000 identitas palsu untuk pengajuan pinjaman online, dengan perkiraan keuntungan mencapai Rp28 miliar. Pelaku dalam kasus ini menunjukkan pemahaman mendalam tentang sistem verifikasi digital dan celah dalam proses know-your-customer industri fintech(Rahmanto, 2019).

Balas dendam sebagai motif muncul dalam 18% kasus, terutama dalam lingkup korporasi dan institusi pemerintah. Kasus yang menonjol terjadi di sebuah bank BUMN dimana mantan kepala cabang mengubah data nasabah untuk menciptakan kerugian bagi perusahaan. Psikologi pelaku dalam kasus ini mengikuti pola "equity theory" dimana mereka merasa diperlakukan tidak adil sehingga melakukan pembalasan melalui manipulasi data. Yang menarik, pelaku cenderung meninggalkan jejak digital yang mudah dilacak karena ingin pengakuan atas tindakannya.

Kelompok ketiga adalah pelaku yang termotivasi oleh tantangan teknis, mencakup sekitar 10% kasus. Profil *script kiddie* ini umumnya berusia muda (17-25 tahun) dengan keterampilan digital otodidak tetapi minim pemahaman konsekuensi hukum. Sebuah kasus di Bandung mengungkap bagaimana seorang mahasiswa teknik berhasil menyusup ke sistem perguruan tinggi hanya untuk mengubah nilai akademik temannya. Pelaku jenis ini seringkali terperangkap dalam logika *hacker ethic* yang mengaburkan batas antara eksperimen teknis dan kejahatan.

Analisis psikologis mendalam terhadap para pelaku biasanya menunjukkan pola kognitif yang khas. Sebanyak 68% pelaku menganggap risiko hukum sebagai harga yang pantas dibanding keuntungan yang akan diperoleh. Mereka juga menunjukkan bias kognitif berupa *illusion of invulnerability*, meyakini sistem keamanan digital dapat dikelabui tanpa konsekuensi. Yang mengkhawatirkan, 42% pelaku mengaku belajar teknik perubahan data dari forum-forum underground dan tutorial online(Firdiawan, 2022).

Penerapan Rational Choice Theory mengungkap bagaimana pelaku melakukan kalkulasi biaya-manfaat yang spesifik. Dalam kasus pinjaman online, pelaku menghitung bahwa potensi keuntungan Rp50-100 juta per identitas palsu jauh lebih menarik dibanding risiko hukuman penjara 5 tahun. Mereka juga mempertimbangkan faktor seperti kemungkinan tertangkap (diperkirakan hanya 12-15%) dan lamanya proses hukum (rata-rata 1,5 tahun).

Motif-motif ini tidak selalu berdiri sendiri. Kasus di Makassar menunjukkan bagaimana mantan karyawan sebuah fintech (balas dendam) kemudian membentuk jaringan penjualan data palsu (motif ekonomi) setelah menyadari potensi keuntungannya. Pola hybrid semacam ini semakin umum ditemui dan menunjukkan evolusi motif kejahatan yang dinamis.

Dari segi karakteristik psikologis, pelaku dengan motif ekonomi cenderung memiliki profil kepribadian antisosial dengan skor tinggi pada trait manipulativeness dalam tes psikologi. Sementara pelaku balas dendam menunjukkan skor tinggi pada neuroticism dan hostility. Pelaku eksperimen teknis umumnya memiliki curiosity tinggi tetapi rendah dalam conscientiousness.

Teori Strain dari Merton juga relevan untuk memahami kasus-kasus dimana pelaku berasal dari kalangan terdidik namun terlibat dalam kejahatan perubahan data. Sejumlah kasus mengungkap bagaimana lulusan perguruan tinggi dengan keterampilan TI terlibat dalam kejahatan ini karena tekanan ekonomi atau kesenjangan antara harapan dan realitas karir.

Aspek psikososial turut berperan penting. Banyak pelaku mengawali karier kejahatannya dalam kelompok kecil yang memberikan validasi sosial terhadap tindakan ilegal tersebut. Forum-

forum underground dan komunitas hacker menjadi ruang dimana norma-norma penyimpangan ini dikonstruksi dan diperkuat.

Pemahaman mendalam tentang motif dan psikologi pelaku ini memberikan dasar penting untuk menyusun strategi pencegahan yang efektif. Pendekatan hukum semata tidak cukup tanpa intervensi psikologis dan sosial untuk mengubah kalkulasi biaya-manfaat yang dilakukan calon pelaku. Terlebih lagi, temuan ini menyoroti perlunya edukasi etika digital sejak dini sebagai bagian dari upaya pencegahan struktural.

Kelemahan Sistem dan Rekomendasi Kebijakan Penanggulangan Kejahatan Perubahan Data

Sistem verifikasi identitas digital di Indonesia masih menjadi titik lemah utama yang sering dimanfaatkan pelaku kejahatan perubahan data. Penelitian menunjukkan bahwa mayoritas layanan publik masih mengandalkan metode autentikasi sederhana berbasis NIK dan nomor telepon, tanpa lapisan keamanan biometrik atau multi-faktor yang memadai. Celah kritis muncul dalam mekanisme validasi silang data antarinstansi yang tidak berjalan secara real-time, menciptakan jeda waktu 3-7 hari yang kerap dieksploitasi pelaku untuk melakukan manipulasi data. Kasus-kasus terbaru membuktikan bagaimana pelaku dengan mudah memanfaatkan ketidaksinkronan antara basis data kependudukan dengan sistem layanan kesehatan atau perbankan untuk menciptakan identitas palsu(Mahira Dewantoro & Dian Alan Setiawan S.H., M.H., 2023).

Kapasitas penegakan hukum dalam menangani kejahatan perubahan data masih sangat terbatas, baik dari segi kuantitas maupun kualitas. Jumlah ahli forensik digital yang tersertifikasi tidak sebanding dengan volume kasus yang terjadi, sementara metode investigasi konvensional seringkali gagal mengamankan bukti digital yang rentan terhapus atau termodifikasi. Banyak penyidik masih mengandalkan teknik tradisional dalam mengumpulkan bukti elektronik, tanpa pemahaman memadai tentang preservasi data digital yang sesuai standar internasional. Akibatnya, sebagian besar laporan perubahan data tidak berujung pada proses hukum karena ketiadaan alat bukti yang sah di pengadilan(Aldriano & Priyambodo, 2022).

Implementasi teknologi blockchain untuk audit trail perubahan data dapat menjadi solusi transformasional dalam

memperkuat integritas sistem. Teknologi ini mampu menciptakan catatan perubahan data yang terdesentralisasi, transparan, dan tidak dapat dimanipulasi. Setiap modifikasi data akan terekam secara permanen dalam jaringan terdistribusi, dilengkapi dengan stempel waktu dan identitas pihak yang melakukan perubahan. Pengalaman penerapan sistem serupa di Singapura membuktikan efektivitas pendekatan ini dalam menekan upaya pemalsuan data hingga di bawah 10% pada sistem administrasi publik.

Pembangunan sistem deteksi dini terintegrasi antara BSSN dan Kominfo merupakan kebutuhan mendesak untuk mengantisipasi kejahatan perubahan data. Sistem ini harus mencakup kemampuan pemantauan real-time terhadap anomali data, analisis perilaku pengguna, dan peringatan dini atas aktivitas mencurigakan. Integrasi dengan pusat data berbagai instansi pemerintah akan memungkinkan pelacakan perubahan data secara lintas sektor, sekaligus mempersulit pelaku yang selama ini memanfaatkan fragmentasi sistem.

Pendidikan literasi digital perlu difokuskan pada tiga level strategis secara bersamaan. Pada level operator, diperlukan program sertifikasi kompetensi khusus yang mencakup teknik pengamanan data dan identifikasi upaya manipulasi. Di level manajerial, pelatihan manajemen risiko perubahan data harus menjadi syarat bagi pejabat yang bertanggung jawab atas sistem informasi. Sementara di level masyarakat, kampanye kesadaran akan pentingnya proteksi data pribadi harus dilakukan secara masif dan berkelanjutan(Duana et al., 2024).

Studi komparatif dengan praktik terbaik di Singapura mengungkap pentingnya membangun kerangka regulasi yang spesifik mengatur tata kelola perubahan data. Sistem sertifikasi perubahan data elektronik yang diterapkan Singapura terbukti efektif dalam menciptakan akuntabilitas dan transparansi. Setiap permintaan perubahan data penting harus melalui proses otorisasi berlapis dan diverifikasi oleh petugas tersertifikasi.

Rekomendasi kebijakan yang komprehensif harus mencakup aspek preventif, detektif, dan represif secara seimbang. Pada level preventif, penguatan sistem autentikasi berbasis biometrik dan penerapan prinsip zero-trust architecture menjadi keharusan. Di sisi detektif, pengembangan sistem monitoring terpadu dengan

kemampuan analitik canggih akan memungkinkan identifikasi dini upaya manipulasi data. Sementara pada aspek represif, peningkatan kapasitas penyidik dan kerja sama internasional dalam penelusuran aset digital pelaku harus menjadi prioritas.

Transformasi sistem pengamanan data memerlukan pendekatan holistik yang melibatkan seluruh pemangku kepentingan. Kolaborasi antara pemerintah, sektor swasta, akademisi, dan masyarakat sipil akan menentukan keberhasilan upaya penanggulangan kejahatan perubahan data. Pembentukan gugus tugas khusus yang mengintegrasikan unsur teknologi, hukum, dan penegakan hukum dapat menjadi langkah strategis untuk menyinkronkan berbagai inisiatif yang selama ini masih berjalan sendiri-sendiri(Mohamad Revaldy Fairuzzen et al., 2024).

Evaluasi berkala terhadap efektivitas kebijakan yang diterapkan harus menjadi bagian dari sistem pengelolaan risiko perubahan data. Mekanisme umpan balik dari lapangan perlu dibangun untuk mengidentifikasi celah baru yang mungkin muncul seiring perkembangan teknik kejahatan. Pembelajaran dari setiap kasus yang terjadi harus segera diimplementasikan dalam bentuk penyempurnaan sistem dan prosedur.

Pada akhirnya, penguatan sistem hukum pidana untuk menjangkau kejahatan perubahan data kontemporer menjadi prasyarat penting. Revisi terhadap UU ITE dan KUHP perlu segera dilakukan untuk secara spesifik mengatur dan memberikan sanksi yang proporsional terhadap berbagai bentuk kejahatan perubahan data. Penyusunan pedoman pembuktian elektronik yang komprehensif juga diperlukan untuk memastikan proses hukum dapat berjalan efektif tanpa terbentur keterbatasan teknis.

Kesimpulan

Kejahatan perubahan data di Indonesia mengungkap tiga kelemahan sistemik utama: verifikasi identitas yang rentan, kapasitas forensik digital yang terbatas, dan fragmentasi kebijakan antarinstansi. Celah ini dimanfaatkan pelaku melalui berbagai modus operandi canggih, mulai dari eksploitasi jeda sinkronisasi data hingga teknik anti-forensik. Solusi transformasional seperti *blockchain-based audit trail* dan *AI-powered anomaly detection*—yang telah terbukti efektif di Singapura—perlu diadopsi dengan penyesuaian konteks lokal, didukung penguatan UU ITE dan standar pembuktian elektronik.

Pembangunan ketahanan digital memerlukan kolaborasi *tripartite* antara pemerintah, sektor swasta, dan masyarakat. Prioritas kebijakan harus mencakup: (1) sertifikasi kompetensi bagi operator dan penegak hukum, (2) integrasi sistem pemantauan BSSN-Kominfo, serta (3) kampanye literasi digital berbasis risiko. Pendekatan ini tidak hanya menutup celah eksisting tetapi juga menciptakan ekosistem pengamanan data yang adaptif terhadap evolusi teknik kejahatan di masa depan.

Daftar Pustaka

Aldriano, M. A., & Priyambodo, M. A. (2022). Cyber Crime Dalam Sudut Pandang Hukum Pidana. In *Jurnal Kewarganegaraan* (Vol. 6, Issue 1, pp. 2169–2175). download.garuda.kemdikbud.go.id. http://download.garuda.kemdikbud.go.id/article.php?article=3034720&val=20674&title=Cyber Crime Dalam Sudut Pandang Hukum Pidana

Bagul, Y., Amalo, H., & Fanggi, R. A. (2024). Kajian Kriminologis terhadap Kekerasan yang Dilakukan oleh Pasangan Kumpul Kebo: Studi Kasus di Wilayah Hukum Polres Manggarai Barat. *Perkara: Jurnal Ilmu Hukum Dan Politik*, *2*(2), 1–20. https://journal.stekom.ac.id/index.php/PERKARA/article/view/1841

Butarbutar, R. (2023). Kejahatan Siber Terhadap Individu: Jenis, Analisis, Dan Perkembangannya. *Jurnal Hukum & Pembangunan*, *2*(2). https://doi.org/10.21143/telj.vol2.no2.1043

Cheny Berlian. (2021). Kejahatan Siber Yang Menjadi Kekosongan Hukum. *Journal Equitable*, *5*(2), 19–20. https://doi.org/10.37859/jeq.v5i2.2532

Duana, G. R., Masyar, A., & Wulandari, C. (2024). TINJAUAN TEORI KRIMINOLOGI DALAM KEJAHATAN SIBER (KASUS KEBOCORAN DATA NASABAH) Overview of Criminological Theory in Cyber Crime (Customer Data Leakage Cases). *Jurnal Prioris*, *11*(2), 161–174. https://e-journal.trisakti.ac.id/index.php/prioris/article/view/18959

Efendi, E. (2015). Hukum Pidana Indonesia. In *Refika Aditama, Bandung*

(Vol. 3, Issue April). books.google.com. https://books.google.com/books?hl=en&lr=&id=YCOwEAAAQBAJ&oi=fnd&pg=PA1&dq=hukum+pidana&ots=dWkziciqUJ&sig=3FDKI6D4vlEaobDPoVtgfT_R7RQ

Fara Anindita Salsabila, & Andi Aina IImih. (2024). Penyalahgunaan Data Pribadi Sebagai Bentuk Kejahatan Sempurna Dalam Perspektlf Hukum Siber. *ALADALAH: Jurnal Politik, Sosial, Hukum Dan Humaniora*, *2*(4), 176–181. https://doi.org/10.59246/aladalah.v2i4.968

Firdiawan, M. A. (2022). *… pidana pencurian data kartu kredit (Carding) dihubungkan dengan Pasal 30 Ayat (2) Jo Pasal 46 Ayat (2) Undang-undang nomor 19 tahun 2016 tentang perubahan ….* digilib.uinsgd.ac.id. https://digilib.uinsgd.ac.id/56954/

Kelana, P. R. (2022). *… Hukum Terhadap Pelaku Tindak Pidana Pencurian Data Kartu Kredit (CARDING) Berdasarkan Undang Undang Nomor 19 Tahun 2016 Tentang Perubahan Atas ….* repository.unilak.ac.id. https://repository.unilak.ac.id/id/eprint/4764

Kriminologis, K., Tindak, T., Pencabulan, P., Yang, A., Kekerasan, D., Pattianakota, S., Adam, S., & Lewerissa, Y. A. (2023). Kajian Kriminologis Terhadap Tindak Pidana Pencabulan AnakYang Disertai Kekerasan. *338 | PATTIMURA Law Study Review*, *1*, 338–352. https://scholar.google.co.id/citations?user=THY6jRMAAAAJ&hl=en,

M. Syafiih, Nadiyah, Khairi, M., Moh. Furqan, & Beny Yusman. (2024). Pendampingan Literasi Digital untuk Mengurangi Risiko Kejahatan Siber Membentuk Masyarakat yang Lebih Aman. *JILPI : Jurnal Ilmiah Pengabdian Dan Inovasi*, *2*(4), 1027–1036. https://doi.org/10.57248/jilpi.v2i4.456

Madinah Mokobombang, Zulfikri Darwis, & Sabil Mokodenseho. (2023). Pemberantasan Tindak Pidana Cyber di Provinsi Jawa Barat: Peran Hukum dan Tantangan dalam Penegakan Hukum Terhadap Kejahatan Digital. *Jurnal Hukum Dan HAM Wara Sains*, *2*(6), 517–525. https://doi.org/10.58812/jhhws.v2i6.447

Mahira Dewantoro, N., & Dian Alan Setiawan S.H., M.H. (2023). Penegakan Hukum Kejahatan Siber Berbasis Phising dalam Bentuk Application Package Kit (APK) Berdasarkan Undang-Undang Informasi dan Transaksi Elektronik. In *Bandung Conference Series: Law Studies* (Vol. 3, Issue 2, pp. 892–900).

https://doi.org/10.29313/bcsls.v3i2.7247

Mappaselleng, N. F. (2024). Kajian Kriminologis Terhadap Kejahatan Terorisme Melalui Media Internet. *Fundamental: Jurnal Ilmiah Hukum*. https://ejurnal.umbima.ac.id/index.php/jurnalhukum/article/view/242

Mardiansyah, C. (2016). *Kajian Yuridis Kriminologis Terhadap Kejahatan Pencurian Dan Perusakan Bagasi Penumpang Pesawat Di Bandara Soekarno-Hatta Dihubungkan Dengan KUHP Jo UU No.1 Tahun 2009 Tentang Penerbangan* (pp. 1–230). Fakultas Hukum Unpas.

Mohamad Revaldy Fairuzzen, Abil Arya Putra, Akmal Reihan, & Lilik Prihatini S.H, M.H. (2024). Perkembangan Hukum dan Kejahatan Siber "Cybercrime" di Indonesia. *Indonesian Journal of Islamic Jurisprudence, Economic and Legal Theory*, *2*(1), 139–153. https://doi.org/10.62976/ijijel.v2i1.372

Nicodemus, A. A. (2023). *Tantangan dalam Penegakan Hukum Pidana terhadap Kejahatan Siber di Era Digital*. digilib.iblam.ac.id. http://digilib.iblam.ac.id/id/eprint/953/

Prasetyo, J. D. (2019). Kajian Yuridis Kriminologis Mengenai Tindak Pidana Pemerasan Oleh Pengamen Jalanan Dihubungkan Dengan Pasal 368 Kuhp Jo Perda No. 11 Tahun 2005 Tentang K3 Kota Bandung. In *Fakultas Hukum Unpas*. FAKULTAS HUKUM UNPAS.

Rahmanto, T. Y. (2019). Penegakan Hukum terhadap Tindak Pidana Penipuan Berbasis Transaksi Elektronik. In *Jurnal Penelitian Hukum De Jure* (Vol. 19, Issue 1, p. 31). academia.edu. https://doi.org/10.30641/dejure.2019.v19.31-52

Ramadha, B. S. (2021). *Kemampuan Hukum Pidana Terhadap Kejahatan Siber Terkait Perindungan Data Pribadi di Indonesia*. dspace.uii.ac.id. chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://dspace.uii.ac.id/bitstream/handle/123456789/31626/18912046 Bagus Satryo Ramadha.pdf?sequence=1&isAllowed=y

Saputra, I. R., Sapada, R. R. A., Dzulqarnain, A., & ... (2025). Pengaruh Media Sosial Terhadap Peningkatan Kejahatan Siber dan Tantangan Penegakan Hukum Pidana. *Jurnal Litigasi …*. http://journalstih.amsir.ac.id/index.php/julia/article/view/67

1

SAPUTRI, D. D. M., & SAPUTRI, M. (2022). *KAJIAN KRIMINOLOGIS TERHADAP PELAKU TINDAK PIDANA PEMBUNUHAN KULI PANGGUL PASAR ANGSO DUO KOTA JAMBI (Studi Kasus Nomor: LP/B-12/I …*. repository.unbari.ac.id. http://repository.unbari.ac.id/1254/

Setiawan, W. (2017). Era Digital dan Tantangannya. *Seminar Nasional Pendidikan*, 1–9.

Suratno, U. (2019). Arah Pembaharuan Hukum Nasional Dalam Menghadapi Era Revolusi Industri 4.0. *Yustitia*, *5*(1), 155–169. https://doi.org/10.31943/yustitia.v5i1.65

Togatorop, F. M., Lestarika, D. P., & ... (2025). Analisis Kejahatan Siber Sebagai Kejahatan Perang Berdasarkan Hukum Humaniter Internasional. *Jurnal Kajian Hukum …*. https://jurnal.globalscients.com/index.php/jkhpk/article/view/417

Umbara, A., & Setiawan, D. A. (2022). Analisis Kriminologis Terhadap Peningkatan Kejahatan Siber di Masa Pandemi Covid-19. In *Jurnal Riset Ilmu Hukum* (pp. 81–88). https://doi.org/10.29313/jrih.v2i2.1324