LEX PROGRESSIUM
Organized by Yayasan Pendidikan Dan Pelayanan Kesehatan Rahmat Husada
Email : lexprogressiumjurnal@gmail.com
Website : https://jurnal.dokterlaw.com/index.php/lexprogressium/index

PENEGAKAN HUKUM TERHADAP KEJAHATAN SIBER TERKAIT PERLINDUNGAN DATA PRIBADI DALAM TRANSAKSI *E-COMMERCE*

Article

Author
Tiko Pujo Ashari[1],
Ika Dewi Sartika Saimima[2]

Air Marshal Suryadarma University[1],
Air Marshal Suryadarma University[2]

Email
tikopujoashari2113@gmail.com[1],
ikasaimima@unsurya.ac.id[2]

Data
Submitted : 01-09-2025
Revised : 01-10-2025
Accepted : 01-11-2025

Abstract

The rapid growth of e-commerce in Indonesia has been accompanied by an increase in cybercrime cases, particularly personal data breaches, such as the incidents at BSI, BI, and Tokopedia. This raises serious concerns about consumer data security and public trust. This study aims to identify the roles and strategies of law enforcement officials in addressing cybercrime related to personal data breaches in e-commerce and analyze the obstacles they face in establishing evidence. This research is a normative legal study with a statutory approach. Data were analyzed qualitatively. The discussion shows that law enforcement officials (the Police, the National Cyber and Information Technology Agency (BSSN), and the Communication and Information Technology (Kominfo) PPNS (National Agency for the Protection of Information and Communication Technology) play a role in investigations, digital forensic analysis, and cross-sectoral/international coordination. Strategies implemented include increasing human resource capacity, utilizing advanced technology, strengthening the framework, and implementing proactive and preventative strategies. However, key obstacles to establishing evidence include the transnational nature of cybercrime, the anonymity of perpetrators, digital forensic difficulties (volatile evidence, integrity, concealment techniques), the rapid evolution of modus operandi, limited resources, and the incompleteness of implementing regulations for the PDP Law, which hamper technical details, legal certainty, and clear law enforcement mechanisms.

Keywords: Law Enforcement, Cybercrime, Personal Data Protection, E-Commerce Transactions

Abstrak

Pesatnya pertumbuhan e-commerce di Indonesia diiringi peningkatan kasus kejahatan siber, terutama pelanggaran data pribadi, seperti insiden BSI, BI, dan Tokopedia. Hal ini menimbulkan kekhawatiran serius terhadap keamanan data konsumen dan kepercayaan publik. Penelitian ini bertujuan untuk mengidentifikasi peran dan strategi aparat penegak hukum dalam menangani kejahatan siber terkait pelanggaran data pribadi di e-commerce serta menganalisis kendala pembuktian yang mereka hadapi. Penelitian ini adalah hukum normatif dengan pendekatan perundang-undangan. Data dianalisis secara kualitatif. Pembahasan menunjukkan bahwa aparat penegak hukum (Kepolisian, BSSN, PPNS Kominfo) berperan dalam penyelidikan/penyidikan, analisis forensik digital, dan koordinasi lintas sektor/internasional. Strategi yang dijalankan meliputi peningkatan kapasitas SDM, pemanfaatan teknologi canggih, penguatan kerangka, serta strategi proaktif dan preventif. Namun,

kendala utama dalam pembuktian meliputi sifat kejahatan siber yang transnasional, anonimitas pelaku, kesulitan forensik digital (bukti volatile, integritas, teknik penyembunyian), evolusi modus operandi cepat, keterbatasan sumber daya, dan belum lengkapnya peraturan pelaksana UU PDP yang menghambat detail teknis, kepastian hukum, dan mekanisme penegakan hukum yang jelas.
Kata Kunci: Penegakan Hukum, Kejahatan Siber, Perlindungan Data Pribadi, Transaksi *E-Commerce*

PENDAHULUAN

Perkembangan teknologi informasi dan komunikasi telah membawa perubahan fundamental dalam berbagai aspek kehidupan manusia, termasuk dalam bidang ekonomi. Salah satu manifestasi paling nyata dari revolusi digital ini adalah pesatnya pertumbuhan transaksi *e-commerce* atau perdagangan secara elektronik. Data menunjukkan bahwa volume transaksi *e-commerce* di Indonesia terus meningkat secara signifikan dari tahun ke tahun, menjadikan sektor ini sebagai tulang punggung ekonomi *digital* yang menjanjikan. Kemudahan, efisiensi, dan jangkauan yang tanpa batas telah menarik jutaan masyarakat untuk berpartisipasi dalam aktivitas jual beli daring, mulai dari kebutuhan sehari-hari hingga investasi dan layanan jasa.

Era digital telah membawa perubahan signifikan dalam preferensi dan perilaku belanja, yang memicu peralihan besar-besaran ke platform *e-commerce*. Keunggulan seperti kemudahan akses, ketersediaan produk yang beragam, dan harga yang kompetitif menjadi daya tarik utama *platform* ini. Era *digital* telah membawa perubahan mendalam dalam berbagai aspek kehidupan manusia, terutama dalam pola konsumsi dan interaksi ekonomi melalui platform *e-commerce*. Kemajuan pesat dalam teknologi informasi dan komunikasi telah memberikan berbagai kemudahan bagi masyarakat, terutama dalam mengakses produk dan layanan secara daring. Transformasi digital ini memungkinkan transaksi menjadi lebih cepat, efisien, dan mudah dilakukan kapan saja dan di mana saja. Namun, di balik manfaat yang ditawarkan, terdapat tantangan yang tidak kalah pentingnya untuk diperhatikan. Beberapa tantangan utama mencakup perlindungan hak konsumen, privasi, keamanan data, standar kualitas produk, dan mekanisme penyelesaian sengketa. Perlindungan hak konsumen menjadi sangat penting mengingat banyaknya kasus penipuan atau ketidaksesuaian produk dengan deskripsi yang ditawarkan. Selain itu, keamanan data dan privasi juga menjadi isu sentral, karena semakin banyak data pribadi yang disimpan dan diproses oleh platform digital. Jika

tidak dikelola dengan baik, data ini berpotensi disalahgunakan oleh pihak-pihak yang tidak bertanggung jawab.[1]

Namun, di balik segala kemudahan dan potensi ekonominya, transformasi digital ini juga membuka celah dan menciptakan tantangan baru, terutama dalam konteks keamanan siber. Seiring dengan peningkatan aktivitas daring, modus operandi kejahatan siber pun semakin canggih dan beragam. Salah satu target utama dari kejahatan siber adalah data pribadi, yang merupakan aset berharga di era *digital*. Dalam setiap transaksi *e-commerce*, pengguna mau tidak mau harus menyerahkan sejumlah data pribadinya, seperti nama lengkap, alamat, nomor telepon, informasi pembayaran, hingga riwayat transaksi. Data-data ini, jika jatuh ke tangan yang salah, dapat disalahgunakan untuk berbagai tujuan ilegal, seperti penipuan, pencurian identitas, penyalahgunaan kartu kredit, hingga kejahatan yang lebih serius.

Pada Mei 2023, *ransomware LockBit* menyerang Bank Syariah Indonesia (BSI) dan mencuri data secara besar-besaran. Kelompok tersebut membocorkan sekitar 1,5 *terabyte* data, termasuk informasi pribadi 15 juta nasabah dan 24.437 karyawan BSI. Data ini meliputi informasi pinjaman hingga dokumen internal bank.[2]

Pada 21 Januari 2022, Bank Indonesia (BI) mengumumkan telah terkena serangan *ransomware Conti*. Juru Bicara Badan Siber dan Sandi Negara (BSSN) Anton Setiawan mengatakan, serangan *ransomware Conti* ke Bank Indonesia (BI) sejatinya telah terjadi pada akhir 2021. Serangan menyasar 16 komputer personal di kantor Bank Indonesia (BI) Bengkulu, tanpa merusak sistem krusial atau menyebabkan kerugian finansial. Data yang terkena mencakup pekerjaan personal di komputer kantor. Kelompok Conti mengklaim memiliki data dari Bank Indonesia (BI) dengan ukuran 487,09 *Megabyte* (MB), namun pihak Bank Indonesia (BI) sendiri memastikan tidak ada data sensitif yang bocor.[3]

Tokopedia dilaporkan mengalami peretasan, bahkan jumlahnya diperkirakan 91 juta akun dan 7 juta akun *merchant*, tidak lagi 15 juta seperti diberitakan sebelumnya. Padahal di tahun 2019, Tokopedia mengungkapkan bahwa ada sekitar 91 juta akun aktif di *platform*nya. Artinya hampir semua akun di Tokopedia berhasil diambil datanya oleh peretas. Pelaku menjual

---

[1] I Wayan Cenik Ardika, "*Tinjauan Hukum terhadap* Perlindungan Data Pribadi di Era Digital: Kasus Kebocoran Data Pengguna Layanan E-Commerce", Indonesian Journal of Law and Justice Volume: 2, Number 3, 2025, hlm. 2.

[2] Defara Dhanya, "Daftar Serangan Ransomware ke Lembaga Keuangan Indonesia: BI, BSI dan Terbaru BRI", https://www.tempo.co/sains/daftar-serangan-ransomware-ke-lembaga-keuangan-indonesia-bi-bsi-dan-terbaru-bri-1183490, diakses pada 15 April 2025.

[3] *Ibid.*

data di *darkweb* berupa *user* ID, *e-mail*, nama lengkap, tanggal lahir, jenis kelamin, nomor *handphone* dan *password* yang masih ter-*hash* atau tersandi.[4]

Fenomena ini menimbulkan kekhawatiran serius terhadap perlindungan data pribadi konsumen dalam transaksi *e-commerce*. Kejahatan siber yang menargetkan data pribadi tidak hanya menimbulkan kerugian finansial bagi individu, tetapi juga dapat merusak kepercayaan publik terhadap sistem *e-commerce* itu sendiri, menghambat pertumbuhan ekonomi digital, dan pada akhirnya mengancam stabilitas keamanan siber nasional. Studi dan laporan insiden keamanan menunjukkan peningkatan kasus kebocoran data, serangan *phishing*, *malware*, dan bentuk-bentuk kejahatan siber lainnya yang secara langsung berdampak pada integritas data pribadi pengguna *e-commerce*.

Menyadari urgensi tersebut, Pemerintah Indonesia telah mengambil langkah strategis dengan mengesahkan Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi (UU PDP). Kehadiran UU PDP diharapkan menjadi payung hukum yang komprehensif untuk menjamin hak-hak individu atas data pribadinya, serta memberikan landasan hukum yang kuat bagi penegakan hukum terhadap pelanggaran dan kejahatan terkait data pribadi. Sebelum UU PDP, perlindungan data pribadi tersebar di berbagai peraturan perundang-undangan lain, seperti Undang-Undang Informasi dan Transaksi Elektronik (UU ITE), namun belum secara spesifik dan terintegrasi mengatur seluruh aspek perlindungan data pribadi.

Meskipun kerangka hukum telah diperkuat dengan UU PDP, penegakan hukum terhadap kejahatan siber yang terkait dengan perlindungan data pribadi dalam transaksi *e-commerce* masih menghadapi berbagai tantangan kompleks. Tantangan ini meliputi karakteristik kejahatan siber yang lintas batas (*transnasional*), sifat anonimitas pelaku, kesulitan pembuktian forensik digital, kecepatan evolusi modus operandi kejahatan, hingga keterbatasan sumber daya dan kapasitas aparat penegak hukum. Selain itu, sinkronisasi antara regulasi sektoral dengan UU PDP, serta koordinasi antar lembaga penegak hukum (seperti Kepolisian, Kementerian Komunikasi dan Informatika, Badan Siber dan Sandi Negara, dan lembaga terkait lainnya) juga menjadi faktor krusial dalam efektivitas penegakan hukum.

Penelitian ini terlihat bahwa evaluasi mendalam tentang efektivitas strategi dalam penanganan kasus-kasus *ecommerce* kurang efektif dan memerlukan perbaikan. Kurangnya eksplorasi mendalam tentang perspektif korban kejahatan siber terkait data pribadi sehingga

[4] CNN Indonesia, "Kronologi Lengkap 91 Juta Akun Tokopedia Bocor dan Dijual", https://www.cnnindonesia.com/teknologi/20200503153210-185-499553/kronologi-lengkap-91-juta-akun-tokopedia-bocor-dan-dijual, diakses pada 15 April 2025.

ada kendala yang dihadapi korban yang pada akhirnya mempersulit proses pembuktian oleh aparat penegak hukum.

Penelitian mengenai penegakan hukum terhadap kejahatan siber terkait perlindungan data pribadi dalam transaksi *e-commerce* menjadi sangat relevan. Penelitian ini diharapkan tidak hanya mengidentifikasi permasalahan dan kendala-kendala yang dihadapi aparat penegak hukum dalam pembuktian terkait perlindungan data pribadi dalam transaksi *e-commerce*, mengevaluasi peran dan strategi aparat penegak hukum, serta merumuskan rekomendasi kebijakan dan langkah-langkah solutif untuk memperkuat perlindungan data pribadi dan menciptakan lingkungan *e-commerce* yang aman dan terpercaya bagi seluruh masyarakat Indonesia.

Telah diketahui bahwa beberapa kalangan sebelumnya telah melakukan penelitian tentang berbagai pandangan terhadap penegakan hukum terhadap kejahatan siber terkait perlindungan data pribadi dalam transaksi *e-commerce*. Namun, terdapat perbedaan antara penelitian yang dilakukan oleh Peneliti dan penelitian sebelumnya. Beberapa referensi yang berkaitan dengan penelitian ini meliputi:

1) Terdapat jurnal yang ditulis oleh Erna Priliasari dengan judul "Perlindungan Data Pribadi Konsumen Dalam Transaksi *E-Commerce* Menurut Peraturan Perundang-undan Di Indonesia", Jurnal Rechts Vinding, Vol. 12 No. 2, Agustus 2023. Persamaan antara penelitian ini dan penelitian tersebut terletak pada fokus kajian terhadap perlindungan data pribadi konsumen dalam transaksi *e-Commerce*, perbedaannya terletak pada pendekatan penelitian; di mana penelitian tersebut mengkaji tanggung jawab *marketplace* terhadap kebocoran data pribadi konsumen, sementara penelitian yang dilakukan oleh Peneliti lebih menitikberatkan pada peran dan strategi yang dijalankan oleh aparat penegak hukum dalam menangani kasus kejahatan siber yang berkaitan dengan pelanggaran data pribadi dalam konteks *e-commerce* di Indonesia.
2) I Wayan Cenik Ardika meneliti tentang "Tinjauan Hukum terhadap Perlindungan Data Pribadi di Era Digital: Kasus Kebocoran Data Pengguna Layanan *E-Commerce*", *Indonesian Journal of Law and Justice* Volume: 2, *Number* 3, 2025. Persamaan antara penelitian ini dan penelitian tersebut terletak pada fokus kajian terhadap Perlindungan data pribadi konsumen dalam transaksi *e-commerce*, perbedaannya terletak pada pendekatan penelitian; di mana penelitian tersebut mengkaji tanggung jawab perusahaan, efektivitas regulasi yang berlaku, serta hak konsumen dalam menghadapi kasus-kasus kebocoran data, sementara penelitian yang dilakukan oleh Peneliti lebih menitikberatkan pada peran dan strategi yang dijalankan oleh aparat penegak hukum dalam

menangani kasus kejahatan siber yang berkaitan dengan pelanggaran data pribadi dalam konteks *e-commerce* di Indonesia.

METODE PENELITIAN

Jenis penelitian hukum normatif yaitu suatu proses untuk menemukan suatu aturan hukum, prinsip-prinsip hukum, maupun doktrin-doktrin hukum guna menjawab isu hukum yang dihadapi.[5] Sedangkan pendekatan penelitian yang dilakukan peneliti yaitu pendekatan perundang-undangan (*Statue Approach*) dalam penelitian hukum normatif. Sesuai dengan jenis penelitiannya, maka dalam penelitian ini menggunakan jenis data sekunder.[6] Teknik pengumpulan data dalam penelitian hukum normatif dilakukan dengan studi pustaka terhadap bahan-bahan hukum, baik bahan hukum primer, bahan hukum sekunder, maupun bahan hukum tersier dan atau bahan non-hukum. Dalam penelitian ini pengolahan menggunakan analisis kualitatif.

HASIL PENELITIAN DAN PEMBAHASAN

1. Peran dan Strategi Yang Dijalankan Oleh Aparat Penegak Hukum Dalam Menangani Kasus Kejahatan Siber Yang Bberkaitan Dengan Pelanggaran Data Pribadi Dalam Konteks E-Commerce di Indonesia

Aparat penegak hukum, seperti Kepolisian Republik Indonesia, Badan Siber dan Sandi Negara (BSSN), dan Kementerian Komunikasi dan Informatika (Kominfo), memiliki peran sentral dalam penanganan kejahatan siber yang berkaitan dengan pelanggaran data pribadi dalam konteks *e-commerce* di Indonesia. Peran dan strategi yang dijalankan meliputi berbagai aspek, mulai dari pencegahan hingga penindakan.

1) Peran Aparat Penegak Hukum

Aparat penegak hukum menjalankan berbagai peran strategis untuk memastikan perlindungan data pribadi dan menindak pelaku kejahatan siber:

a) Penyelidikan dan Penyidikan Tindak Pidana Siber

1) Kepolisian Negara Republik Indonesia

Melalui unit khusus seperti Direktorat Tindak Pidana Siber Bareskrim Polri, Kepolisian berwenang penuh untuk menerima laporan, melakukan penyelidikan, dan menyidik kasus-kasus pelanggaran data pribadi. Kewenangan ini diatur dalam Undang-Undang Nomor 8 Tahun 1981 tentang

[5] Peter Mahmud Marzuki, *Penelitian Hukum*, (Jakarta, Kencana, 2010), hlm 35
[6] Soerjono Soekanto, *Pengantar Penelitian Hukum*, (Jakarta: Universitas Indonesia, 2008), hlm. 11

Hukum Acara Pidana (KUHAP). Selain itu, Undang-undang (UU) Nomor 1 Tahun 2024 tentang Perubahan Kedua atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik memperkuat dasar hukum ini, terutama pada Pasal 30 (tentang akses ilegal), Pasal 31 (*intersepsi ilegal*), Pasal 32 (perubahan, perusakan, atau penghilangan informasi atau dokumen elektronik), Pasal 33 (gangguan terhadap sistem elektronik), Pasal 34 (pembuatan *malware*), dan Pasal 35 (penyebaran informasi yang merugikan).[7] Dengan hadirnya UU PDP, tindak pidana terkait data pribadi diatur lebih spesifik mulai dari Pasal 48 hingga Pasal 51 UU PDP, yang mencakup penyalahgunaan data pribadi, pencurian identitas, pemalsuan data pribadi, dan penggunaan data pribadi secara melawan hukum.

2) Penyidik Pegawai Negeri Sipil (PPNS) di Kementerian/Lembaga

Beberapa kementerian atau lembaga, seperti Kominfo, memiliki PPNS yang diberikan kewenangan untuk melakukan penyidikan terhadap pelanggaran UU ITE dan UU PDP sesuai dengan lingkup tugas mereka. Hal ini memungkinkan penanganan kasus yang lebih spesifik dan terkoordinasi

b) Analisis Forensik Digital

Pembuktian dalam kasus siber sangat bergantung pada bukti digital.[8]

1) Badan Siber dan Sandi Negara (BSSN)

Sebagai lembaga negara yang bertanggung jawab atas keamanan siber nasional, BSSN memainkan peran krusial dalam membantu aparat penegak hukum dengan analisis forensik digital. Ini melibatkan identifikasi, akuisisi, dan analisis bukti digital dari berbagai sumber seperti komputer, jaringan, dan perangkat seluler yang terkait dengan insiden pelanggaran data. Keahlian BSSN sangat penting untuk mengungkap jejak digital pelaku dan membangun bukti yang kuat yang dapat digunakan di pengadilan.

2) Pusat Laboratorium Forensik (Puslabfor) Polri

Puslabfor juga memiliki unit khusus yang menangani barang bukti digital, menyediakan dukungan ilmiah yang diperlukan untuk proses penyidikan dan memastikan validitas bukti di mata hukum.

[7] Nabila Aulia Agustin, "*Studi Literatur: Ancaman Cybercrime di Indonesia dan Pentingnya Pemahaman akan Fenomena Kejahatan Digital*", Jamastika, Volume 3 Nomo 1 April 2024

[8] Muhammad Rafi Ilmuna Ihsan dan Apriade Voutama, "*Penerapan Metode NIST Dalam Analisis Forensik Digital Pasca Serangan Siber (Studi Kasus:Pt.Analis Digital Forensik)*", CyberSecurity dan Forensik Digital, Vol. 8, No. 1, Mei 2025

c) Koordinasi Lintas Sektoral dan Internasional

Kejahatan siber seringkali tidak mengenal batas yurisdiksi.[9]

1) Kerja Sama Antar Lembaga

Koordinasi yang erat antara Kepolisian, BSSN, Kominfo, Otoritas Jasa Keuangan (OJK) (khususnya untuk sektor keuangan), Bank Indonesia (BI) (untuk sistem pembayaran), dan bahkan penyedia platform e-commerce sangatlah penting. Pasal 63 UU PDP secara eksplisit menyatakan bahwa penegakan hukum terkait data pribadi dapat dilakukan oleh penyidik Polri, PPNS, atau penyidik lainnya sesuai ketentuan peraturan perundang-undangan. Koordinasi ini memastikan penanganan kasus yang holistik, mulai dari pelacakan, penindakan, hingga pemulihan dampak

2) Kerja Sama Internasional

Mengingat sifat kejahatan siber yang seringkali lintas negara, kerja sama dengan lembaga penegak hukum internasional seperti Interpol menjadi esensial. Hal ini memungkinkan pelacakan dan penindakan pelaku yang beroperasi di luar yurisdiksi Indonesia, serta pertukaran informasi intelijen yang vital

2) Strategi Penegakan Hukum dalam Penanganan Kejahatan Siber Terkait Pelanggaran Data Pribadi

a) Peningkatan Kapasitas Sumber Daya Manusia (SDM)

Dalam perang melawan kejahatan siber, sumber daya manusia adalah aset terpenting. Para pelaku kejahatan siber terus berinovasi, sehingga aparat penegak hukum harus memiliki keahlian yang setara atau bahkan melebihi mereka. Beberapa analisis penulis dalam strategi penegakan hukum dalam penanganan kejahatan siber yaitu:

1) Pelatihan dan Sertifikasi

Aparat penegak hukum, mulai dari penyidik Kepolisian, analis forensik di BSSN, hingga jaksa penuntut umum, harus menjalani pelatihan intensif dan berkelanjutan. Pelatihan ini tidak hanya mencakup aspek hukum dan prosedur penyidikan, tetapi juga teknologi informasi terbaru, modus

[9] SIP Law Firm, "Ini Perbedaan Cyber Crime dan Digital Law", https://siplawfirm.id/ini-perbedaan-cyber-crime-dan-digital-law/?lang=id#:~:text=Cyber%20crime%20juga%20dapat%20diartikan,untuk%20menangani%20atau%20mengatasi%20cybercrime., diakses pada 18 Juli 2025

operandi kejahatan siber, dan teknik forensik digital. Sertifikasi internasional di bidang forensik digital, seperti *Certified Digital Forensics Examiner* (CDFE) *atau Certified Hacking Forensic Investigator* (CHFI), sangat didorong untuk meningkatkan kapabilitas dan kredibilitas mereka di mata hukum. Program pelatihan harus dirancang agar relevan dengan perkembangan teknologi dan tren kejahatan siber.

2) Pengadaan Ahli

Mengingat kompleksitas kasus kejahatan siber, aparat penegak hukum perlu merekrut atau melibatkan ahli-ahli di bidang keamanan siber dan forensik digital. Ahli-ahli ini bisa berasal dari kalangan profesional swasta, akademisi, atau bahkan pensiunan praktisi siber. Kehadiran mereka sangat membantu dalam menganalisis data yang rumit, menafsirkan bukti digital, dan memberikan kesaksian ahli di pengadilan untuk kasus-kasus yang sangat kompleks.

b) Pemanfaatan Teknologi Canggih

Teknologi adalah pedang bermata dua: digunakan oleh pelaku kejahatan, tetapi juga merupakan alat paling efektif untuk melawan mereka. Aparat penegak hukum harus menguasai dan memanfaatkan teknologi terkini.

1) Alat Forensik Digital

Pengadaan dan pemanfaatan perangkat lunak dan keras forensik digital terkini sangatlah vital. Alat-alat ini memungkinkan penyidik untuk melakukan akuisisi, analisis, dan pelaporan bukti digital dengan cepat dan akurat. Contohnya termasuk perangkat untuk pemulihan data dari perangkat yang rusak, analisis malware, dan penelusuran jejak komunikasi. Investasi dalam teknologi ini akan mempercepat proses investigasi dan meningkatkan kualitas bukti yang terkumpul.[10]

2) Sistem Pemantauan dan Deteksi Dini

Mengembangkan atau mengimplementasikan sistem pemantauan dan deteksi dini adalah langkah proaktif. Sistem ini dapat mendeteksi anomali atau indikasi serangan siber pada infrastruktur vital, termasuk platform *e-commerce*. Dengan sistem ini, potensi pelanggaran data bisa terdeteksi sebelum

[10] Maulia Inayah Ansar, "Apa itu Digital Forensik? Fungsi, Tujuan, dan Tahapannya", https://digitalsolusigrup.co.id/digital-forensik-adalah/, diakses pada 18 Juli 2025

menyebabkan kerusakan besar, memungkinkan respons cepat untuk mitigasi dan penindakan.

3) Analisis Big Data dan Kecerdasan Buatan (AI)

Memanfaatkan analisis big data dan kecerdasan buatan (AI) adalah strategi mutakhir. Teknologi ini dapat digunakan untuk menganalisis volume data siber yang sangat besar, mengidentifikasi pola-pola kejahatan, melacak asal-usul serangan, mengidentifikasi tren modus operandi pelaku, dan bahkan memprediksi potensi serangan di masa depan. AI juga dapat membantu dalam proses identifikasi anomali yang luput dari pengamatan manusia, sehingga aparat penegak hukum dapat lebih proaktif dalam menghadapi ancaman

c) Penguatan Kerangka Hukum dan Regulasi

Kerangka hukum yang jelas, kuat, dan adaptif sangat penting untuk memberikan landasan bagi tindakan penegakan hukum.

1) Implementasi UU PDP

Setelah disahkannya Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi (UU PDP), langkah selanjutnya adalah memastikan implementasi yang efektif. Hal ini berarti menerbitkan peraturan pelaksana yang komprehensif, seperti Peraturan Pemerintah (PP) dan Peraturan Presiden (Perpres). Peraturan-peraturan ini akan memberikan panduan yang lebih jelas tentang tata cara perlindungan data, kewajiban pengendali data pribadi, hak-hak subjek data, serta mekanisme penegakan hukum. Secara spesifik, peraturan ini akan menguraikan lebih lanjut ketentuan dalam Bab VII UU PDP tentang Sanksi Administratif (Pasal 57 - Pasal 62), yang mencakup denda administratif dan penghentian pengolahan data pribadi, serta Bab VIII UU PDP tentang Ketentuan Pidana (Pasal 67 - Pasal 73), yang mengatur hukuman penjara dan denda bagi pelaku tindak pidana terkait data pribadi.

2) Sinkronisasi Regulasi

Penting untuk memastikan adanya harmonisasi antara UU PDP dengan peraturan perundang-undangan lain yang relevan, seperti UU ITE, UU Perbankan, dan peraturan sektoral lainnya. Ini bertujuan untuk menghindari tumpang tindih regulasi atau kekosongan hukum yang dapat mempersulit penegakan hukum. Sinkronisasi akan menciptakan sistem hukum yang kohesif dan efektif dalam melindungi data pribadi.

d) Strategi Proaktif dan *Preventif*

Pendekatan reaktif saja tidak cukup. Aparat penegak hukum harus mengambil langkah-langkah preventif dan proaktif untuk mencegah terjadinya kejahatan siber.[11]

1) Patroli Siber

Melakukan patroli siber secara rutin adalah bentuk pengawasan aktif. Petugas memantau aktivitas ilegal di dunia maya, termasuk penjualan data pribadi di dark web atau forum-forum *underground*. Patroli ini membantu mengidentifikasi ancaman sejak dini dan memungkinkan penegak hukum untuk mengambil tindakan sebelum kerusakan meluas.

2) Audit Keamanan

Aparat penegak hukum juga dapat mendorong dan, jika perlu, mewajibkan platform e-commerce untuk secara berkala melakukan audit keamanan sistem mereka oleh pihak ketiga yang independen. Ini sejalan dengan Pasal 39 UU PDP yang mengamanatkan pengendali data pribadi untuk melakukan evaluasi berkala terhadap efektivitas langkah pengamanan yang mereka terapkan. Audit ini membantu mengidentifikasi celah keamanan sebelum dieksploitasi oleh peretas

3) Pembangunan Kesadaran

Melakukan kampanye masif untuk meningkatkan kesadaran masyarakat tentang risiko kejahatan siber dan cara melindungi data pribadi mereka sendiri. Ini termasuk edukasi tentang *phishing*, *malware*, pentingnya kata sandi yang kuat, dan tidak mudah percaya pada penawaran yang mencurigakan. Masyarakat yang cerdas dan waspada adalah garis pertahanan pertama melawan kejahatan siber.

2. Kendala-Kendala Yang Dihadapi Aparat Penegak Hukum Dalam Pembuktian Terkait Perlindungan Data Pribadi Dalam Transaksi *E-Commerce*

Pembuktian dalam kasus kejahatan siber terkait pelanggaran data pribadi memiliki karakteristik unik dan kompleksitas tinggi yang seringkali menjadi hambatan bagi aparat penegak hukum. Kendala-kendala ini bersumber dari sifat kejahatan itu sendiri, keterbatasan sumber daya, hingga aspek hukum dan teknis.

1) Karakteristik Kejahatan Siber yang Lintas Batas (*Transnasional*)

[11] Duarif dan Moh. Saleh, "*Pencegahan dan Penindakan Tindak Pidana Siber oleh Kepolisian Resort Teluk Bintuni*", Unes Law Review Vol. 6, No. 4, Juni 2024

Kejahatan siber seringkali tidak terikat oleh batas geografis negara, sehingga penanganan dan pembuktiannya menjadi sangat sulit.[12]

a) Yurisdiksi Hukum yang Berbeda

Pelaku kejahatan siber dapat beroperasi dari negara mana pun di dunia. Hal ini menimbulkan masalah yurisdiksi, di mana hukum suatu negara mungkin tidak berlaku di negara lain. Proses pelacakan, penangkapan, dan ekstradisi pelaku memerlukan kerja sama lintas negara yang kompleks dan seringkali memakan waktu lama. Misalnya, jika data pribadi masyarakat Indonesia diretas oleh kelompok siber di negara lain, aparat penegak hukum Indonesia harus melalui prosedur hukum dan diplomatik yang rumit untuk mendapatkan bantuan investigasi atau penindakan

b) Kerja Sama Internasional yang Rumit

Meskipun ada lembaga seperti Interpol, proses permintaan data atau bantuan penegakan hukum antarnegara dapat terhambat oleh perbedaan sistem hukum, birokrasi, atau bahkan kepentingan politik. Kejahatan siber transnasional sering kali memanfaatkan celah hukum antarnegara (*jurisdictional arbitrage*)

2) Sifat Anonimitas Pelaku

Pelaku kejahatan siber memiliki berbagai cara untuk menyembunyikan identitas mereka, membuat pelacakan menjadi sangat sulit.[13]

a) Penggunaan Teknologi Anonimitas

Pelaku sering menggunakan *Virtual Private Network* (VPN), *Tor Network, proxy server*, atau *cryptocurrency* untuk menyembunyikan alamat IP dan identitas mereka, serta mempersulit pelacakan transaksi keuangan ilegal. Jejak digital mereka sangat minim atau terenkripsi, membuat identifikasi dan penangkapan menjadi tantangan besar.

b) Penggunaan Identitas Palsu/Curian

[12] Risma Siti Maesaroh, "*Tantangan Keamanan Siber dan Implikasinya terhadap Hukum Kenegaraan: Tinjauan atas Peran Negara dalam Menjamin Ketahanan Digital*", Jurnal Hukum Kenegaraan dan Politik Islam Vol. 4, No. 2, Desember 2024

[13] PT Indodax Nasional Indonesia., "Anonimitas adalah Privasi Digital, Ini Cara Menjaganya!", https://indodax.com/academy/anonimitas-adalah-privasi-digital/#:~:text=&text=VPN%20memungkinkan%20pengguna%20menyembunyikan%20alamat,(ISP)%20atau%20situs%20web.&text=Tor%20(The%20Onion%20Router)%20bekerja,menjaga%20anonimitas%20saat%20menjelajahi%20internet.&text=Mata%20uang%20kripto%20menawarkan%20berbagai,%2C%20penerima%2C%20dan%20jumlah%20transaksi., dikases pada 18 Juli 2025

Pelaku dapat menggunakan identitas palsu atau mencuri identitas orang lain (*spoofing*) untuk melakukan aksinya, sehingga mempersulit aparat penegak hukum untuk mengidentifikasi pelaku sebenarnya.

3) Kesulitan Pembuktian Forensik Digital

Bukti digital adalah tulang punggung kasus kejahatan siber, namun pengumpulan dan analisisnya memiliki tantangan tersendiri.[14]

a) Sifat Bukti Digital yang *Volatile* dan *Fleeting*

Data digital sangat *volatile* (mudah berubah) dan *fleeting* (mudah hilang). Bukti dapat dengan mudah dimodifikasi, dihapus, atau terhapus secara otomatis seiring waktu atau karena tindakan pengguna. Hal ini menuntut kecepatan dan keakuratan dalam akuisisi bukti.

b) Integritas dan Otentisitas Bukti

Memastikan integritas dan otentisitas bukti digital sangat krusial agar dapat diterima di pengadilan. Proses akuisisi harus dilakukan dengan metode forensik yang terstandardisasi dan diaudit untuk menghindari tuduhan manipulasi. Pasal 5 UU ITE menyatakan bahwa informasi atau dokumen elektronik yang sah merupakan alat bukti hukum yang sah, namun keabsahannya sangat bergantung pada prosedur pengumpulan dan penjaminan integritasnya.

c) Kecanggihan Teknik Penyembunyian Data

Pelaku menggunakan teknik canggih seperti *enkripsi, steganography* (menyembunyikan data dalam *file* lain), atau fragmentasi data untuk menyembunyikan informasi penting, mempersulit proses analisis forensik.

d) Keterbatasan Perangkat dan Sumber Daya Forensik

Meskipun ada upaya peningkatan, ketersediaan perangkat forensik digital terkini dan jumlah ahli forensik yang memadai masih menjadi kendala di beberapa unit penegak hukum.

4) Kecepatan Evolusi Modus Operandi Kejahatan

Dunia siber berkembang sangat cepat, begitu pula dengan modus operandi kejahatan.[15]

---

[14] Amsori, "*Tantangan dan Peran Digital Forensik dalam Penegakan Hukum terhadap Kejahatan di Ranah Digital*", Journal Humaniora: Jurnal Hukum dan Ilmu Sosial, Volume 02, No.01, Januari 2024

[15] Marzuki Ismail, "*Digital Policing: Studi Pemanfaatan Teknologi Dalam Pelaksanaan Tugas Intilejen Kepolisian Untuk Mencegah Kejahatan Siber (Cybercrime*)", Jurnal Ilmu Kepolisian, Volume 17 / Nomor 3 / Desember 2023

a) Modus Baru yang Terus Muncul

Pelaku kejahatan siber terus mengembangkan teknik dan modus operandi baru, seperti varian *ransomware* yang lebih canggih, *phishing* yang lebih personal, atau eksploitasi celah keamanan *zero-day*. Hal ini menuntut aparat penegak hukum untuk selalu *up-to-date* dan beradaptasi dengan cepat.

b) Kesenjangan Pengetahuan dan Teknologi

Seringkali terdapat kesenjangan antara pengetahuan dan teknologi yang dimiliki penegak hukum dengan yang digunakan oleh para pelaku kejahatan.

5) Keterbatasan Sumber Daya dan Kapasitas Aparat Penegak Hukum

Faktor internal juga berkontribusi pada kendala pembuktian.

a) Kekurangan SDM Berkeahlian Khusus

Meskipun ada unit siber, jumlah penyidik dan analis forensik yang memiliki keahlian khusus dalam kejahatan siber dan data pribadi masih terbatas dibandingkan dengan volume kasus yang terus meningkat.

b) Anggaran dan Infrastruktur

Keterbatasan anggaran dapat menghambat pengadaan teknologi forensik canggih, pembaruan perangkat keras dan lunak, serta pelaksanaan pelatihan berkelanjutan bagi personel. Infrastruktur yang tidak memadai juga bisa menjadi kendala.

6) Sinkronisasi Regulasi dan Koordinasi Antar Lembaga

UU PDP adalah payung hukum yang mengatur prinsip-prinsip umum, hak subjek data, kewajiban pengendali dan prosesor data, serta sanksi pidana dan administratif. Namun, sebagai undang-undang yang bersifat lex generalis, banyak detail teknis dan operasional yang memerlukan pengaturan lebih lanjut dalam peraturan pelaksana. Ini sangat krusial karena:

a) Detail Teknis Pelaksanaan

Banyak ketentuan dalam UU PDP yang bersifat umum dan membutuhkan penjabaran teknis. Misalnya, mengenai mekanisme sertifikasi dan audit sistem perlindungan data, standar keamanan data minimum, prosedur notifikasi kegagalan perlindungan data, atau tata cara pemrosesan data sensitif. Tanpa aturan yang jelas, pelaku usaha dan organisasi akan kesulitan dalam menerapkan kewajiban mereka.

b) Kepastian Hukum

Ketiadaan peraturan pelaksana menciptakan ketidakpastian hukum bagi semua pihak. Pengendali data tidak memiliki panduan pasti tentang bagaimana

mematuhi ketentuan UU PDP, sementara subjek data tidak sepenuhnya memahami hak-hak mereka atau bagaimana mekanisme pengaduan dan penyelesaian sengketa bekerja. Hal ini juga berisiko menimbulkan interpretasi yang beragam dan inkonsistensi dalam praktik.

c) Mekanisme Penegakan Hukum yang Jelas

Salah satu aspek paling vital yang membutuhkan peraturan pelaksana adalah terkait penegakan hukum. Pasal 63 UU PDP secara eksplisit menyatakan bahwa penegakan hukum pelanggaran data pribadi dapat dilakukan oleh Kepolisian Negara Republik Indonesia, Pejabat Penyidik Pegawai Negeri Sipil (PPNS), atau penyidik lainnya. Namun, rincian mengenai prosedur penyidikan, mekanisme koordinasi antarlembaga penyidik, serta pembagian kewenangan dan tanggung jawab masih belum diatur secara spesifik.

KESIMPULAN

Aparat penegak hukum di Indonesia, yang terdiri dari Kepolisian, BSSN, dan PPNS di Kementerian/Lembaga, memainkan peran vital dalam menangani kejahatan siber terkait pelanggaran data pribadi di *e-commerce*. Peran ini mencakup penyelidikan dan penyidikan berdasarkan KUHAP, UU ITE, dan UU PDP; analisis forensik digital oleh BSSN dan Puslabfor Polri; serta koordinasi lintas sektoral dan internasional. Strategi yang dijalankan meliputi peningkatan kapasitas SDM (pelatihan, sertifikasi, pengadaan ahli), pemanfaatan teknologi canggih (alat forensik, deteksi dini, AI dan big data), penguatan kerangka hukum (implementasi dan sinkronisasi UU PDP), serta strategi proaktif dan *preventif* (patroli siber, audit keamanan, pembangunan kesadaran publik).

Pembuktian kasus kejahatan siber terkait pelanggaran data pribadi dalam transaksi *e-commerce* menghadapi berbagai kendala signifikan. Kendala utama meliputi karakteristik transnasional kejahatan siber yang menyulitkan yurisdiksi dan kerja sama internasional, sifat anonimitas pelaku melalui teknologi canggih dan identitas palsu, serta kesulitan pembuktian forensik digital karena sifat bukti yang *volatile*, tantangan integritas, dan teknik penyembunyian data. Selain itu, kecepatan evolusi modus operandi kejahatan, keterbatasan sumber daya dan kapasitas aparat penegak hukum (SDM dan anggaran), dan belum lengkapnya sinkronisasi regulasi serta koordinasi antarlembaga (khususnya ketiadaan peraturan pelaksana UU PDP yang rinci) turut memperumit proses pembuktian.

SARAN

Berdasarkan kesimpulan yang telah dirumuskan di atas, maka dapat disarankan sebagai berikut :

Segera sahkan Peraturan Pelaksana UU PDP untuk memberikan panduan teknis dan prosedural yang jelas bagi penegak hukum dan pelaku industri.

Perlunya sinergi yang lebih kuat antara Kepolisian, BSSN, Kominfo, dan lembaga terkait lainnya melalui SOP yang jelas

DAFTAR PUSTAKA

Amsori. "Tantangan dan Peran Digital Forensik dalam Penegakan Hukum terhadap Kejahatan di Ranah Digital." *Journal Humaniora: Jurnal Hukum dan Ilmu Sosial*, Vol. 2, No. 1, 2024.

Ansar, Maulia Inayah. "Apa itu Digital Forensik? Fungsi, Tujuan, dan Tahapannya." Digital Solusi Grup, diakses 18 Juli 2025.

Ardika, I Wayan Cenik. "Tinjauan Hukum terhadap Perlindungan Data Pribadi di Era Digital: Kasus Kebocoran Data Pengguna Layanan E-Commerce." *Indonesian Journal of Law and Justice*, Vol. 2, No. 3, 2025.

CNN Indonesia. "Kronologi Lengkap 91 Juta Akun Tokopedia Bocor dan Dijual." CNN Indonesia, diakses 15 April 2025.

Dhanya, Defara. "Daftar Serangan Ransomware ke Lembaga Keuangan Indonesia: BI, BSI dan Terbaru BRI." Tempo.co, diakses 15 April 2025.

Duarif, dan Moh. Saleh. "Pencegahan dan Penindakan Tindak Pidana Siber oleh Kepolisian Resort Teluk Bintuni." *Unes Law Review*, Vol. 6, No. 4, 2024.

Ihsan, Muhammad Rafi Ilmuna, dan Apriade Voutama. "Penerapan Metode NIST dalam Analisis Forensik Digital Pasca Serangan Siber (Studi Kasus: PT Analis Digital Forensik)." *CyberSecurity dan Forensik Digital*, Vol. 8, No. 1, 2025.

Indodax Nasional Indonesia, PT. "Anonimitas adalah Privasi Digital, Ini Cara Menjaganya!" Indodax Academy, diakses 18 Juli 2025.

Ismail, Marzuki. "Digital Policing: Studi Pemanfaatan Teknologi dalam Pelaksanaan Tugas Intelijen Kepolisian untuk Mencegah Kejahatan Siber (Cybercrime)." *Jurnal Ilmu Kepolisian*, Vol. 17, No. 3, 2023.

Marzuki, Peter Mahmud. *Penelitian Hukum*. Jakarta: Kencana, 2010.

Maesaroh, Risma Siti. "Tantangan Keamanan Siber dan Implikasinya terhadap Hukum Kenegaraan: Tinjauan atas Peran Negara dalam Menjamin Ketahanan Digital." *Jurnal Hukum Kenegaraan dan Politik Islam*, Vol. 4, No. 2, 2024.

SIP Law Firm. “Ini Perbedaan Cyber Crime dan Digital Law.” SIP Law Firm, diakses 18 Juli 2025.

Soekanto, Soerjono. *Pengantar Penelitian Hukum*. Jakarta: Universitas Indonesia, 2008.

Agustin, Nabila Aulia. “Studi Literatur: Ancaman Cybercrime di Indonesia dan Pentingnya Pemahaman akan Fenomena Kejahatan Digital.” *Jamastika*, Vol. 3, No. 1, 2024.