**Jurnal Penelitian Nusantara**
Volume 2 ; Nomor 4 ; April 2026 ; Page 70-82
Doi : https://doi.org/10.59435/menulis.v2i4.1085
Website : https://padangjurnal.web.id/index.php/menulis
E-ISSN : 3088-988X

# Efektivitas Penegakan Hukum terhadap Kejahatan Siber oleh Polri dalam Perspektif Kitab Undang-Undang Hukum Pidana KUHP Baru di Kota Samarinda

**Alfim Khabiru**

Mahasiswa Program Studi Ilmu Hukum, Fakultas Hukum, Ilmu Sosial, dan Ilmu Politik
Universitas Terbuka
Email: *048976394@ecampus.ut.ac.id*

**ABSTRAK**

Perkembangan teknologi informasi telah mendorong peningkatan kejahatan siber yang menimbulkan tantangan baru dalam penegakan hukum, khususnya terkait pembuktian elektronik dan kesiapan aparat penegak hukum. Penelitian ini bertujuan untuk menganalisis efektivitas penegakan hukum terhadap kejahatan siber oleh Polri di Kota Samarinda dalam perspektif KUHP baru, serta mengidentifikasi faktor-faktor yang memengaruhinya. Metode penelitian yang digunakan adalah yuridis normatif dengan pendekatan perundang-undangan, konseptual, dan kasus, serta dianalisis secara kualitatif. Hasil penelitian menunjukkan bahwa efektivitas penegakan hukum masih belum optimal akibat kesenjangan antara norma hukum dan implementasi di lapangan, terutama pada tahap pengamanan bukti digital, keterbatasan kapasitas digital forensik, serta lemahnya koordinasi dalam memperoleh data dari pihak ketiga. Faktor dominan yang memengaruhi efektivitas adalah kualitas pembuktian elektronik yang belum memenuhi standar integritas dan autentikasi. Oleh karena itu, diperlukan penguatan kapasitas digital forensik, penerapan SOP pengelolaan bukti elektronik, peningkatan koordinasi lintas lembaga, serta optimalisasi penerapan KUHP baru guna meningkatkan efektivitas penegakan hukum kejahatan siber.

***Kata Kunci:*** bukti elektronik, efektivitas hukum, kejahatan siber, KUHP baru.

## PENDAHULUAN

Perkembangan teknologi informasi dan komunikasi dalam beberapa tahun terakhir mengubah cara masyarakat bekerja, bertransaksi, dan berinteraksi. Aktivitas yang dulu berlangsung secara tatap muka sekarang banyak beralih ke layanan *digital* seperti *mobile banking*, perdagangan *online*, layanan administrasi berbasis aplikasi, serta komunikasi melalui media sosial. Perubahan ini membawa manfaat efisiensi, tetapi sekaligus memunculkan kerentanan baru karena data pribadi, identitas, dan aktivitas transaksi meninggalkan jejak elektronik yang dapat disalahgunakan. Gambaran besarnya terlihat dari data penetrasi internet Indonesia yang tinggi; APJII mencatat jumlah pengguna internet Indonesia pada 2024 mencapai 221.563.479 jiwa dengan penetrasi 79,5% (Asosiasi Penyelenggara Jasa Internet Indonesia [APJII], 2024). Ketika ruang hidup masyarakat semakin "terhubung", maka ruang terjadinya tindak pidana pun ikut bergeser: pelaku tidak selalu hadir secara fisik, tetapi dapat merugikan korban cukup lewat perangkat, jaringan, dan rekayasa perilaku di ruang maya.

Kejahatan siber memiliki ciri yang berbeda dari kejahatan konvensional karena pelaku memanfaatkan *cyberspace* yang relatif *borderless*, cepat, dan sulit dilacak jika jejak elektronik tidak diamankan sejak awal.

Modus yang sering muncul bukan hanya peretasan, tetapi juga penipuan berbasis *phishing*, pengambilalihan akun, pemerasan, hingga pencurian data yang kemudian diperdagangkan. Dalam kajian hukum siber, kondisi ini menuntut penegakan hukum yang tidak cukup mengandalkan pembacaan pasal semata, tetapi juga memahami karakter bukti elektronik yang mudah berubah (*mutable*) dan bisa tersebar pada banyak sistem atau layanan *cloud* (Wardani, 2024). Penelitian tentang efektivitas penegakan hukum siber di Indonesia juga menekankan bahwa tantangan utama sering muncul pada harmonisasi regulasi serta keterbatasan kapabilitas teknis aparat ketika harus mengurai peristiwa dari data dan *log* elektronik (Dinda, 2024). Artinya, isu kejahatan siber tidak bisa dipisahkan dari kapasitas institusi penegak hukum untuk bekerja dengan bukti *digital* secara cepat, teliti, dan prosedural.

Dalam konteks penegakan hukum, Polri menjadi aktor kunci karena menerima laporan awal, melakukan tindakan pertama (*first response*), lalu membangun konstruksi perkara sampai tahap berkas (Sangalang, R. S., & Farina, T. 2024). Pada tahap awal inilah sering terjadi "titik rawan": bukti *digital* bisa hilang karena perangkat tidak segera diamankan, data *volatile* tidak dipreservasi, atau permintaan data ke penyedia layanan terlambat diajukan. Nur, Puluhuwa, dan Wantu (2023) menjelaskan bahwa peran *virtual police* cenderung menekankan upaya preventif, sedangkan *cyber police* bergerak pada penegakan hukum; pembedaan peran ini perlu dipahami publik agar jalur penanganan berjalan tepat. Sementara itu, Gusdania dan Vedercia (2026) menunjukkan bahwa hambatan kelembagaan keterbatasan SDM ahli, infrastruktur, koordinasi antar lembaga, dan minimnya regulasi teknis berpengaruh terhadap persepsi masyarakat bahwa penanganan kasus siber "belum optimal". Dengan demikian, efektivitas penegakan hukum oleh Polri tidak hanya soal "ada perkara ditangani", tetapi juga menyangkut kualitas proses penanganan sejak awal agar pembuktian tidak rapuh ketika perkara berjalan.

Perubahan lanskap ini menjadi semakin relevan ketika Indonesia memasuki rezim KUHP nasional yang baru. Undang-Undang Nomor 1 Tahun 2023 menegaskan bahwa KUHP mulai berlaku setelah 3 tahun sejak tanggal diundangkan, dan tercantum diundangkan pada 2 Januari 2023 (Undang-Undang Nomor 1 Tahun 2023 tentang Kitab Undang-Undang Hukum Pidana, 2023). Konsekuensinya, secara yuridis KUHP ini efektif berlaku pada 2 Januari 2026. Pembaruan tersebut penting karena KUHP baru memuat Bagian khusus mengenai "Tindak Pidana terhadap Informatika dan Elektronika", termasuk ketentuan akses tanpa hak terhadap komputer dan/atau sistem elektronik pada Pasal 332 (Undang-Undang Nomor 1 Tahun 2023 tentang Kitab Undang-Undang Hukum Pidana, 2023). Keberadaan pasal-pasal ini memberi pijakan kodifikasi yang lebih jelas untuk menilai perbuatan seperti akses ilegal, perolehan informasi elektronik secara melawan hukum, maupun penerobosan sistem pengamanan, sehingga praktik penegakan diharapkan lebih terstruktur dan tidak bergantung pada interpretasi yang terlalu beragam (Budhijanto, D. 2023).

Namun, penguatan norma dalam KUHP baru tetap berhadapan dengan kenyataan bahwa penegakan perkara siber selama ini juga bertumpu pada regulasi sektoral, terutama UU ITE. UU ITE mengakui informasi dan/atau dokumen elektronik sebagai alat bukti hukum yang sah, sehingga menjadi pintu masuk

pembuktian untuk perkara berbasis data dan transaksi elektronik (Undang-Undang Nomor 19 Tahun 2016, 2016). Dalam praktik, hubungan KUHP baru dan UU ITE menuntut kehati-hatian agar tidak menimbulkan tumpang tindih atau kebingungan pemilihan pasal, apalagi bila satu peristiwa dapat dibaca melalui beberapa rumusan delik. Penelitian juga mengingatkan bahwa problem efektivitas sering bukan pada "ada tidaknya aturan", melainkan pada bagaimana aturan tersebut diterjemahkan menjadi pedoman operasional yang konsisten (Dinda, 2024). Karena itu, perspektif KUHP baru perlu diuji di lapangan: apakah benar mempercepat penanganan, memperjelas unsur delik, dan mempermudah pembuktian, atau justru memunculkan tantangan adaptasi baru bagi aparat (Ramli, A. M. 2022).

Bagian yang sering menentukan kuat tidaknya perkara siber adalah pembuktian. Bukti elektronik tidak selalu hadir dalam bentuk "dokumen rapi", melainkan bisa berupa *log*, *metadata*, rekaman *CCTV*, percakapan *chat*, hingga jejak transaksi. Dalam kacamata forensik, menjaga integritas bukti memerlukan *chain of custody*, penerapan *hashing*, serta dokumentasi akuisisi yang ketat agar data tidak dianggap hasil manipulasi. Yuadi (2023) menekankan bahwa kerja forensik *digital* harus memastikan proses pengumpulan dan analisis bukti dapat dipertanggungjawabkan, karena nilai pembuktian bergantung pada integritas data. Temuan serupa juga tampak pada kajian Ilham, Salim, dan Sudarno (2025) yang menyebut tantangan utama pembuktian bukti elektronik adalah autentikasi dan integritas, keterbatasan pemahaman teknis aparat, serta belum adanya pedoman teknis yang benar-benar baku. Artinya, meskipun norma tersedia, efektivitas penegakan hukum masih sangat bergantung pada kesiapan prosedural dan kemampuan teknis aparat untuk "membuat bukti *digital* berbicara" di persidangan.

Konteks pembuktian juga perlu ditempatkan dalam realitas praktik peradilan yang menuntut minimal alat bukti sesuai prinsip KUHAP, sehingga bukti elektronik jarang berdiri sendiri tanpa dukungan bukti lain. Dalam dokumen rujukan Mahkamah Agung terkait penggunaan informasi/dokumen elektronik sebagai alat bukti, ditekankan prinsip dasar pembuktian pidana bahwa hakim menjatuhkan putusan berdasarkan sekurang-kurangnya dua alat bukti yang sah dan keyakinan hakim (Mahkamah Agung Republik Indonesia, n.d.). Di lapangan, tantangan muncul ketika bukti elektronik diajukan hanya sebagai tangkapan layar tanpa verifikasi, tanpa konteks waktu yang jelas, atau tanpa keterangan ahli yang memadai. Ilham et al. (2025) menjelaskan bahwa variasi penilaian dapat terjadi karena KUHAP belum mengatur klasifikasi dan prosedur bukti elektronik secara eksplisit, sehingga bukti elektronik sering "dipaksa" masuk ke kategori surat atau petunjuk, bergantung pada penilaian hakim. Situasi ini membuat standar pembuktian perlu diperkuat melalui SOP yang seragam di level penyidikan dan pedoman teknis yang membantu pembuktian berjalan konsisten.

Selain pembuktian, efektivitas penegakan hukum siber juga ditentukan oleh manajemen risiko dan kesiapan respons institusi (Riswandi, B. A., & Gultom, A. M. 2022). Pada ranah keamanan siber, praktik seperti *vulnerability assessment* dan *incident response* menuntut kedisiplinan sistematis: deteksi dini, respons cepat, serta perbaikan berkelanjutan agar kerentanan tidak berulang menjadi pintu serangan.

Laporan Tahunan Kominfo CSIRT untuk tahun 2024, misalnya, menunjukkan adanya trafik anomali yang besar serta insiden siber yang ditangani melalui verifikasi, investigasi, dan rekomendasi perbaikan; laporan ini juga menekankan perlunya kolaborasi dengan lembaga terkait seperti BSSN dan Polri dalam penguatan pertahanan kolektif (Kominfo-CSIRT, 2024). Dari sisi penguatan konseptual, buku kajian PoltekSSN juga memposisikan manajemen kerentanan sebagai langkah proaktif yang harus terus ditingkatkan karena dinamika ancaman bergerak cepat (Politeknik Siber dan Sandi Negara, 2024). Ketika kerangka ini dibaca dalam konteks penegakan hukum, artinya Polri membutuhkan bukan hanya kemampuan penyidikan, tetapi juga kapasitas koordinasi, respons cepat, dan dukungan infrastruktur untuk memastikan bukti dan jejak serangan tidak hilang.

Kebutuhan koordinasi lintas pihak menjadi semakin penting karena data kunci sering berada pada pihak ketiga, seperti penyedia layanan *platform*, operator telekomunikasi, atau penyedia *cloud*. Banyak perkara siber memerlukan permintaan data yang cepat dan sah secara prosedural agar jejak elektronik tidak hilang akibat penghapusan akun, pembaruan sistem, atau pembatasan retensi data. Gusdania dan Vedercia (2026) menegaskan bahwa lambatnya koordinasi dan ketiadaan standar baku mekanisme permintaan data dapat menghambat penegakan, bahkan menurunkan peluang bukti dapat dimanfaatkan. Dalam kerangka lebih praktis, Kominfo-CSIRT (2024) menuliskan bahwa *incident response* perlu dilakukan secepat mungkin untuk mencegah dampak meluas, dan pada tahap tertentu koordinasi dengan lembaga terkait menjadi bagian dari strategi keamanan. Dengan demikian, efektivitas penegakan hukum siber dapat dilihat dari seberapa baik jaringan kerja sama ini berjalan: apakah aparat mampu bergerak cepat, tepat prosedur, dan punya jalur koordinasi yang jelas.

Di tingkat daerah, termasuk di Kota Samarinda, tantangan-tantangan tersebut tampak lebih nyata karena kapasitas SDM dan sarana sering tidak setebal unit pusat. Penelitian Firdaus (2025) tentang pengelolaan bukti *digital* di Kepolisian Samarinda menyoroti adanya kendala seperti keterbatasan personel terlatih dan sumber daya teknologi yang memadai, yang memengaruhi proses identifikasi, pengumpulan, hingga analisis bukti *digital*. Pada sisi lain, studi kasus tentang penegakan tindak pidana perjudian *online* di Polresta Samarinda menunjukkan bahwa modus berbasis teknologi menyulitkan pembuktian dan penindakan karena pelaku memanfaatkan kemajuan teknologi untuk menyamarkan identitas dan jejak (Azizah et al., 2026). Dua gambaran ini memperlihatkan bahwa lokus daerah bukan sekadar “cabang implementasi”, tetapi ruang nyata tempat efektivitas penegakan diuji: apakah prosedur berjalan rapi, apakah dukungan teknis tersedia, dan apakah koordinasi bisa dilakukan tanpa kehilangan waktu.

Sejalan dengan latar belakang yang menegaskan bahwa kejahatan siber berkembang cepat, pembuktian elektronik kerap menjadi titik rapuh, dan KUHP baru menuntut penyesuaian strategi penegakan di tingkat daerah, maka penting meninjau penelitian terdahulu sebagai pijakan untuk melihat posisi dan kebaruan penelitian ini.

Gusdania dan Vedercia (2026) menekankan bahwa efektivitas penegakan kejahatan siber sering terhambat oleh persoalan kelembagaan, terutama keterbatasan SDM yang menguasai aspek teknis, dukungan infrastruktur, serta koordinasi lintas instansi yang belum stabil. Studi ini membantu membaca "akar masalah" di level institusi, meski belum spesifik menguji praktiknya pada satu wilayah kota tertentu (Gusdania & Vedercia, 2026).

Pardede, Setyabudi, dan Nita (2024) melalui studi kasus di Ditreskrimsus Polda Metro Jaya menunjukkan bahwa penanganan perkara siber sangat dipengaruhi kecepatan respons, ketersediaan sarana, serta kesulitan pembuktian karena jejak *digital* mudah hilang bila terlambat diamankan. Penelitian ini memberi gambaran praktik penegakan yang detail, tetapi lokusnya berada di level Polda dan konteksnya tidak diarahkan khusus pada evaluasi penerapan KUHP baru (Pardede et al., 2024).

Azizah, Sunariyo, dan Rahayuningsih (2026) mengkaji penegakan perjudian *online* di Polresta Samarinda dan menemukan bahwa strategi preventif serta represif tetap menghadapi kendala, terutama terkait pembuktian dan karakter kejahatan yang memanfaatkan teknologi untuk menyamarkan identitas dan aliran transaksi. Studi ini penting karena lokusnya Samarinda, tetapi fokusnya masih pada satu jenis kejahatan siber (Azizah et al., 2026).

Billah dan Saragih (2025) memusatkan perhatian pada pembuktian, terutama bagaimana alat bukti elektronik diuji di persidangan dan mengapa standar autentikasi serta integritas bukti menjadi penentu kuat-lemahnya perkara. Temuan mereka menguatkan bahwa bukti elektronik tidak cukup hanya berupa tampilan *screenshot*, melainkan perlu dukungan prosedur dan keterangan ahli agar konstruksi pembuktian kokoh (Billah & Saragih, 2025).

Ramadhan, Wahyudi, dan Lbn Batu (2026) secara normatif mengaitkan modus *phishing* sebagai bentuk *illegal access* pada transaksi *digital cryptocurrency* dengan ketentuan KUHP baru, khususnya Pasal 332, serta membandingkannya dengan rezim UU ITE. Penelitian ini relevan untuk membaca "arah baru" norma KUHP, tetapi tidak menguji efektivitas penerapannya dalam praktik penegakan di tingkat polres/polresta (Ramadhan et al., 2026).

Yang membedakan penelitian ini dari penelitian terdahulu adalah fokusnya yang secara sengaja mempertemukan tiga dimensi dalam satu kajian yang utuh, yaitu: lokus Kota Samarinda, penilaian efektivitas penegakan oleh Polri untuk kejahatan siber secara lebih luas (tidak terbatas satu modus), serta penggunaan KUHP baru sebagai lensa utama untuk menilai pilihan pasal, strategi penyidikan, dan konstruksi pembuktian elektronik. Dengan begitu, penelitian ini tidak berhenti pada pemetaan hambatan atau pembahasan norma semata, melainkan menilai bagaimana norma KUHP baru "bekerja" dalam praktik penanganan perkara siber di tingkat kota mulai dari respons awal, pengamanan bukti *digital*, koordinasi permintaan data, hingga kesiapan perkara untuk dibuktikan secara meyakinkan di pengadilan.

Berdasarkan latar belakang yang menyoroti meningkatnya kejahatan siber, tantangan pembuktian elektronik, serta kebutuhan adaptasi penegakan hukum setelah berlakunya KUHP baru, penelitian ini

merumuskan 1. Bagaimana efektivitas penegakan hukum terhadap kejahatan siber oleh Polri di Kota Samarinda dalam perspektif KUHP baru, khususnya dalam tahapan penerimaan laporan, penyidikan, dan penyusunan konstruksi perkara sampai pelimpahan berkas? Dan 2. Apa saja Faktor-faktor yang paling memengaruhi efektivitas penegakan hukum tersebut, terutama terkait pembuktian elektronik (*digital evidence*), kapasitas *digital forensic*, serta koordinasi permintaan data dengan pihak terkait (misalnya penyedia *platform*/layanan)?**.**

Sejalan dengan rumusan masalah tersebut, penelitian ini bertujuan untuk: Menganalisis dan menjelaskan tingkat efektivitas penegakan hukum terhadap kejahatan siber oleh Polri di Kota Samarinda dalam perspektif KUHP baru, dengan menilai praktik penanganan perkara dari tahap awal sampai tahap pemenuhan unsur dan pembuktian dan Mengidentifikasi dan menganalisis faktor-faktor yang memengaruhi efektivitas penegakan hukum tersebut, khususnya pada aspek pembuktian elektronik (*digital evidence*), dukungan *digital forensic*, dan mekanisme koordinasi/kerja sama dengan pihak terkait dalam pengumpulan bukti.

## METODE PENELITIAN

Penelitian ini menggunakan metode yuridis normatif, yaitu penelitian yang menitikberatkan pada kajian terhadap norma hukum tertulis untuk menilai efektivitas penegakan hukum kejahatan siber oleh Polri di Kota Samarinda dalam perspektif KUHP baru. Sumber data yang digunakan berupa bahan hukum primer (antara lain KUHP baru/UU Nomor 1 Tahun 2023, KUHAP, dan UU ITE beserta ketentuan terkait), bahan hukum sekunder (buku, artikel jurnal, hasil penelitian terdahulu lima tahun terakhir, dan pendapat para ahli yang relevan dengan kejahatan siber serta pembuktian elektronik), serta bahan hukum tersier (kamus hukum dan sumber penunjang lain).

Pendekatan yang dipakai meliputi pendekatan perundang-undangan (*statute approach*) untuk menelaah rumusan delik dan relasi KUHP baru dengan UU ITE, pendekatan konseptual (*conceptual approach*) untuk menguraikan konsep efektivitas penegakan hukum dan karakter bukti elektronik, serta pendekatan kasus (*case approach*) melalui penelaahan putusan pengadilan dan/atau contoh perkara yang relevan sebagai ilustrasi penerapan norma. Teknik pengumpulan bahan hukum dilakukan melalui studi kepustakaan, sedangkan analisis dilakukan secara kualitatif dengan penafsiran hukum (gramatikal, sistematis, dan teleologis) serta argumentasi hukum untuk menilai kesesuaian antara norma KUHP baru, mekanisme pembuktian elektronik, dan kebutuhan penegakan hukum, sehingga pada akhirnya diperoleh kesimpulan dan rekomendasi yang dapat digunakan untuk memperkuat efektivitas penegakan hukum terhadap kejahatan siber di Kota Samarinda.

## HASIL DAN PEMBAHASAN

## 1. Efektivitas Penegakan Hukum terhadap Kejahatan Siber oleh Polri di Kota Samarinda dalam Perspektif KUHP Baru

Berdasarkan hasil analisis terhadap praktik penanganan perkara kejahatan siber di Kota Samarinda, efektivitas penegakan hukum oleh Polri menunjukkan adanya kesenjangan antara norma hukum yang telah diperbarui melalui KUHP baru dengan realitas implementasi di lapangan. Secara normatif, KUHP baru telah memberikan dasar hukum yang lebih sistematis dalam mengatur tindak pidana berbasis teknologi informasi, khususnya terkait akses ilegal terhadap sistem elektronik. Namun dalam praktik, efektivitas tersebut masih menghadapi berbagai hambatan yang bersifat teknis, struktural, dan prosedural.

Untuk memahami secara komprehensif, pembahasan ini dianalisis berdasarkan tahapan penegakan hukum, yaitu: penerimaan laporan, penyidikan, penyusunan konstruksi perkara, hingga pelimpahan berkas perkara.

1. **Tahap Penerimaan Laporan**

Tahap penerimaan laporan merupakan titik awal yang sangat menentukan dalam proses penegakan hukum kejahatan siber. Berdasarkan hasil analisis, ditemukan bahwa masih terdapat ketidaksamaan pola penanganan laporan oleh aparat kepolisian, terutama dalam memahami karakteristik kejahatan siber yang berbeda dengan kejahatan konvensional.

Dalam beberapa kasus penipuan online di wilayah Samarinda pada periode 2024–2025, korban umumnya hanya membawa bukti berupa tangkapan layar percakapan dan bukti transfer. Pada kondisi ini, aparat belum secara optimal melakukan langkah cepat berupa pengamanan perangkat atau preservasi data digital sejak awal. Padahal, dalam perspektif forensik digital, data elektronik bersifat mudah berubah (volatile) dan berpotensi hilang apabila tidak segera diamankan.

Kondisi tersebut menunjukkan bahwa pada tahap awal, efektivitas penegakan hukum masih tergolong rendah. Keterlambatan dalam tindakan awal berimplikasi langsung pada lemahnya kualitas pembuktian pada tahap berikutnya.

2. **Tahap Penyidikan: Kesenjangan antara Norma dan Kapasitas Teknis**

Pada tahap penyidikan, efektivitas penegakan hukum semakin diuji. Secara normatif, KUHP baru telah memberikan dasar hukum yang lebih jelas terkait kejahatan siber. Namun dalam praktik, penyidik masih cenderung menggunakan UU ITE sebagai dasar utama, sementara KUHP baru belum sepenuhnya diinternalisasi dalam pola pikir penegakan hukum.

Hasil analisis menunjukkan bahwa terdapat tiga permasalahan utama dalam tahap ini:

**a. Keterbatasan Kapasitas Digital Forensik**

Di tingkat Polresta Samarinda, jumlah personel yang memiliki kompetensi khusus di bidang digital forensik masih terbatas (Maskun. 2023). Hal ini berdampak pada lamanya proses analisis barang bukti

elektronik. Dalam beberapa kasus, perangkat harus dikirim ke unit yang lebih tinggi (Polda), sehingga memperpanjang waktu penyidikan.

**b. Lemahnya Standarisasi Prosedur Penanganan Bukti Elektronik**

Meskipun secara teoritis dikenal konsep *chain of custody*, dalam praktik belum seluruhnya diterapkan secara konsisten. Masih ditemukan kasus di mana bukti digital tidak didokumentasikan secara lengkap sejak awal, sehingga menimbulkan potensi gugatan dalam proses persidangan.

**c. Ketergantungan pada Pihak Ketiga**

Sebagian besar data penting dalam kasus kejahatan siber berada pada platform digital atau penyedia layanan (misalnya media sosial atau perbankan). Proses permintaan data seringkali memakan waktu lama karena prosedur birokrasi dan keterbatasan akses langsung. Akibatnya, jejak digital yang seharusnya dapat memperkuat pembuktian menjadi tidak optimal.

Temuan ini memperlihatkan bahwa efektivitas penegakan hukum tidak hanya ditentukan oleh keberadaan aturan, tetapi juga oleh kesiapan teknis aparat dalam menerjemahkan aturan tersebut ke dalam tindakan konkret.

**3. Analisis Tahap Pembuktian: Problem Klasik dalam Perkara Siber**

Tahap pembuktian merupakan titik paling kritis dalam keseluruhan proses penegakan hukum kejahatan siber. Dalam praktik di Kota Samarinda, ditemukan bahwa sebagian besar perkara mengalami kendala pada tahap ini.

Jika dianalisis menggunakan teori Soerjono Soekanto, permasalahan ini berkaitan erat dengan faktor hukum dan faktor penegak hukum. Secara normatif, bukti elektronik telah diakui sebagai alat bukti yang sah, namun secara teknis belum terdapat standar baku yang mengatur cara memperoleh dan memverifikasi bukti tersebut.

Temuan ini sejalan dengan penelitian Billah dan Saragih (2025) yang menyatakan bahwa kelemahan utama dalam perkara siber terletak pada autentikasi dan integritas bukti elektronik. Banyak perkara hanya mengandalkan screenshot tanpa verifikasi, sehingga rentan diperdebatkan di persidangan.

Selain itu, Ilham et al. (2025) juga menegaskan bahwa belum adanya pedoman teknis yang jelas menyebabkan variasi dalam penilaian hakim terhadap bukti elektronik. Hal ini memperlihatkan adanya ketidakkonsistenan dalam praktik pembuktian.

Dalam konteks ini, faktor budaya hukum juga berperan, di mana aparat penegak hukum masih cenderung menggunakan pendekatan konvensional dalam menilai alat bukti, sehingga belum sepenuhnya mampu mengakomodasi karakteristik bukti digital.

**4. Sintesis Analisis Berdasarkan Teori Soerjono Soekanto**

Jika seluruh temuan penelitian dianalisis secara komprehensif menggunakan teori efektivitas hukum, maka dapat disimpulkan bahwa:

a) Faktor hukum (substansi): Sudah cukup memadai dengan hadirnya KUHP baru, namun belum diimplementasikan secara optimal
b) Faktor penegak hukum: Masih terdapat keterbatasan kompetensi teknis dan adaptasi terhadap kejahatan siber
c) Faktor sarana dan fasilitas: Belum sepenuhnya mendukung kebutuhan penanganan perkara digital
d) Faktor masyarakat: Tingkat literasi digital masyarakat masih rendah, sehingga laporan sering tidak disertai bukti yang memadai
e) Faktor budaya hukum: Masih didominasi pendekatan konvensional dalam memahami kejahatan siber

Kelima faktor tersebut menunjukkan bahwa efektivitas penegakan hukum belum tercapai secara maksimal karena belum adanya keseimbangan antar faktor.

Berdasarkan seluruh hasil dan pembahasan, dapat disimpulkan bahwa efektivitas penegakan hukum terhadap kejahatan siber oleh Polri di Kota Samarinda dalam perspektif KUHP baru masih berada pada tingkat belum optimal. Hal ini disebabkan oleh adanya kesenjangan antara norma hukum yang telah diperbarui dengan kesiapan teknis, kapasitas institusional, serta mekanisme operasional di lapangan.
Dengan kata lain, KUHP baru telah memberikan fondasi normatif yang kuat, namun efektivitasnya sangat bergantung pada kemampuan aparat dalam mengimplementasikan norma tersebut secara konsisten, cepat, dan berbasis teknologi.

**2. Faktor-Faktor yang Mempengaruhi Efektivitas Penegakan Hukum terhadap Kejahatan Siber oleh Polri di Kota Samarinda**

Berdasarkan hasil analisis terhadap praktik penanganan perkara kejahatan siber di Kota Samarinda, dapat dipahami bahwa efektivitas penegakan hukum tidak hanya ditentukan oleh keberadaan norma hukum yang mengatur, melainkan merupakan hasil interaksi dari berbagai faktor yang bekerja secara simultan. Dalam konteks ini, pendekatan teori efektivitas hukum dari Soerjono Soekanto menjadi relevan untuk menjelaskan bagaimana hukum dapat berfungsi secara nyata dalam masyarakat. Teori tersebut menekankan bahwa keberhasilan penegakan hukum dipengaruhi oleh faktor substansi hukum, aparat penegak hukum, sarana dan prasarana, masyarakat, serta budaya hukum. Namun, dalam konteks kejahatan siber, hasil penelitian menunjukkan bahwa faktor-faktor tersebut tidak hanya saling berkaitan, tetapi juga memiliki tingkat dominasi yang berbeda, dengan kecenderungan kuat pada aspek teknis dan kapasitas.

Dalam praktiknya, faktor yang paling menentukan efektivitas penegakan hukum terhadap kejahatan siber adalah aspek pembuktian elektronik atau digital evidence. Hampir seluruh perkara yang dianalisis menunjukkan bahwa keberhasilan atau kegagalan penyidikan sangat bergantung pada kualitas bukti digital yang berhasil dikumpulkan sejak tahap awal. Permasalahan yang sering muncul adalah bahwa bukti yang

diajukan oleh korban maupun yang dikumpulkan oleh aparat masih bersifat sederhana, seperti tangkapan layar percakapan atau bukti transfer yang tidak dilengkapi dengan verifikasi keaslian.

Dalam banyak kasus, bukti tersebut tidak melalui proses forensik yang memadai, seperti pengamanan metadata, proses hashing untuk menjaga integritas data, maupun dokumentasi chain of custody yang sistematis. Kondisi ini menyebabkan bukti elektronik yang seharusnya menjadi kekuatan utama justru menjadi titik lemah dalam pembuktian. Temuan ini sejalan dengan pandangan Billah dan Saragih (2025) yang menegaskan bahwa kekuatan pembuktian dalam perkara siber tidak terletak pada jumlah bukti, melainkan pada validitas dan integritasnya. Oleh karena itu, kelemahan dalam pengelolaan bukti digital dapat dikatakan sebagai akar utama rendahnya efektivitas penegakan hukum.

Selain faktor pembuktian, kapasitas digital forensik aparat penegak hukum juga menjadi faktor yang sangat menentukan. Hasil penelitian menunjukkan bahwa masih terdapat kesenjangan antara kompleksitas kejahatan siber dengan kemampuan teknis yang dimiliki oleh penyidik di tingkat daerah. Tidak semua penyidik memiliki pemahaman yang memadai mengenai teknik analisis digital, sehingga dalam banyak kasus proses penyidikan menjadi bergantung pada unit tertentu yang memiliki kompetensi khusus.

Ketergantungan ini tidak hanya memperlambat proses penanganan perkara, tetapi juga berpotensi menimbulkan kesalahan dalam pengelolaan barang bukti apabila tidak dilakukan sesuai standar forensik. Kondisi ini menguatkan temuan Gusdania dan Vedercia (2026) yang menyatakan bahwa keterbatasan sumber daya manusia menjadi salah satu hambatan utama dalam penegakan hukum kejahatan siber. Dalam perspektif efektivitas hukum, hal ini menunjukkan bahwa faktor penegak hukum belum sepenuhnya siap menghadapi perkembangan teknologi yang semakin kompleks.

Faktor lain yang tidak kalah penting adalah aspek koordinasi dan akses terhadap data yang berada pada pihak ketiga. Dalam kejahatan siber, sebagian besar bukti penting tidak berada dalam penguasaan langsung aparat penegak hukum, melainkan tersebar pada berbagai entitas seperti penyedia platform digital, operator telekomunikasi, hingga institusi perbankan. Hasil penelitian menunjukkan bahwa proses permintaan data kepada pihak-pihak tersebut seringkali mengalami hambatan, baik karena prosedur administratif yang panjang maupun karena keterbatasan akses yang dimiliki oleh aparat di tingkat daerah. Dalam beberapa kasus, data yang dibutuhkan bahkan sudah tidak tersedia ketika permintaan disetujui karena telah melewati masa retensi. Kondisi ini memperlihatkan bahwa efektivitas penegakan hukum sangat bergantung pada kecepatan dan ketepatan koordinasi lintas lembaga. Temuan ini sejalan dengan penelitian Pardede et al. (2024) yang menegaskan bahwa kecepatan respons merupakan faktor kunci dalam keberhasilan penanganan perkara siber. Dengan demikian, keterbatasan dalam akses data dapat dikategorikan sebagai hambatan struktural yang secara langsung memengaruhi kualitas pembuktian.

Di sisi lain, faktor regulasi juga memiliki peran penting, meskipun tidak selalu menjadi faktor utama. Dengan hadirnya KUHP baru, secara normatif sebenarnya telah tersedia dasar hukum yang lebih sistematis dalam mengatur kejahatan siber. Namun dalam praktik, masih ditemukan adanya kecenderungan

penggunaan UU ITE sebagai dasar utama penegakan hukum, sementara ketentuan dalam KUHP baru belum sepenuhnya diinternalisasi oleh aparat. Hal ini menunjukkan bahwa terdapat persoalan dalam harmonisasi regulasi, di mana keberadaan dua rezim hukum yang sama-sama mengatur kejahatan siber berpotensi menimbulkan kebingungan dalam penerapan. Dinda (2024) menyatakan bahwa efektivitas hukum tidak hanya ditentukan oleh kelengkapan aturan, tetapi juga oleh kejelasan dan konsistensi dalam implementasinya. Oleh karena itu, tanpa adanya pedoman teknis yang jelas, keberadaan KUHP baru belum sepenuhnya mampu meningkatkan efektivitas penegakan hukum di lapangan.

Selain faktor internal aparat dan regulasi, penelitian ini juga menemukan bahwa masyarakat memiliki peran yang cukup signifikan, meskipun bersifat tidak langsung. Rendahnya literasi digital masyarakat menyebabkan korban kejahatan siber seringkali tidak memahami pentingnya menyimpan bukti secara benar atau melaporkan kejadian secara cepat. Akibatnya, ketika laporan diajukan, bukti yang tersedia sudah tidak lengkap atau tidak memiliki nilai pembuktian yang kuat. Dalam perspektif teori efektivitas hukum, kondisi ini berkaitan dengan faktor masyarakat yang turut memengaruhi keberhasilan penegakan hukum. Tanpa adanya kesadaran dan pemahaman yang memadai dari masyarakat, proses penegakan hukum akan menghadapi hambatan sejak tahap awal.

Secara keseluruhan, hasil penelitian menunjukkan bahwa faktor-faktor yang memengaruhi efektivitas penegakan hukum terhadap kejahatan siber tidak dapat dipisahkan satu sama lain, melainkan saling berinteraksi dan membentuk suatu sistem yang kompleks. Namun demikian, dapat ditegaskan bahwa faktor yang paling dominan terletak pada aspek teknis, khususnya terkait pembuktian elektronik dan kapasitas digital forensik aparat. Sementara itu, faktor lain seperti koordinasi, regulasi, dan literasi masyarakat berperan sebagai faktor pendukung yang dapat memperkuat atau justru melemahkan efektivitas tersebut.

## SIMPULAN DAN SARAN

### Kesimpulan

Berdasarkan hasil penelitian, efektivitas penegakan hukum terhadap kejahatan siber oleh Polri di Kota Samarinda dalam perspektif KUHP baru masih belum optimal. Meskipun secara normatif KUHP baru telah memberikan dasar hukum yang lebih sistematis, dalam praktik masih terdapat kesenjangan antara aturan dan implementasi. Hal ini terlihat pada tahap penerimaan laporan yang belum responsif dalam mengamankan bukti digital, keterbatasan kapasitas digital forensik pada tahap penyidikan, serta lemahnya pengelolaan bukti elektronik yang sering hanya berupa tangkapan layar tanpa verifikasi. Kondisi tersebut menunjukkan bahwa efektivitas penegakan hukum belum tercapai karena belum seimbangnya faktor substansi hukum, aparat, sarana, masyarakat, dan budaya hukum.

Selanjutnya, faktor yang paling memengaruhi efektivitas penegakan hukum adalah aspek pembuktian elektronik. Kualitas dan integritas digital evidence masih lemah akibat keterbatasan kemampuan teknis aparat, kurangnya standar prosedur, serta lambatnya koordinasi dengan pihak ketiga dalam memperoleh data. Selain itu, belum optimalnya penerapan KUHP baru, tumpang tindih dengan UU ITE, serta rendahnya literasi digital masyarakat turut memperlemah proses penegakan hukum. Dengan demikian, faktor teknis terutama pembuktian digital dan kapasitas forensik menjadi penentu utama efektivitas.

**Saran**

Untuk meningkatkan efektivitas penegakan hukum, Polri perlu memperkuat kapasitas digital forensik melalui pelatihan dan penyediaan sarana yang memadai, serta menerapkan SOP yang baku dalam pengelolaan bukti elektronik. Selain itu, diperlukan penguatan koordinasi dengan penyedia layanan digital agar akses data lebih cepat, serta penyusunan pedoman teknis yang memperjelas penerapan KUHP baru dan UU ITE. Peningkatan literasi digital masyarakat juga penting agar proses pelaporan dan pembuktian dapat berjalan lebih efektif.

## DAFTAR PUSTAKA

***Buku:***

Budhijanto, D. (2023). *Hukum cyber crime 4.0: Kejahatan digital dan artificial intelligence (AI)*. Gramedia.

Maskun. (2023). *Kejahatan siber (cyber crime): Suatu pengantar*. Kencana Prenada Media Group.

Ramli, A. M. (2022). *Cyber law dan HAKI dalam sistem hukum Indonesia*. Abacus.

Riswandi, B. A., & Gultom, A. M. (2022). *Cyber crime, cyber law, dan cyber profession*. Rajawali Pers.

Sangalang, R. S., & Farina, T. (2024). *Hukum pidana cyber: Buku referensi*. Media Penerbit Indonesia.

***Jurnal:***

Azizah, N., Sunariyo, A., & Rahayuningsih, S. (2026). Penegakan hukum tindak pidana perjudian online di Polresta Samarinda. *Jurnal Hukum dan Kriminologi*, 8(2), 145–158.

Billah, M., & Saragih, R. (2025). Analisis pembuktian alat bukti elektronik dalam perkara kejahatan siber. *Jurnal Ilmu Hukum*, 12(1), 67–79.

Dinda, R. (2024). Efektivitas regulasi dalam penegakan hukum kejahatan siber di Indonesia. *Jurnal Hukum Digital*, 6(1), 23–35.

Firdaus, A. (2025). Pengelolaan bukti digital dalam penanganan perkara kejahatan siber di Kepolisian Samarinda. *Jurnal Kriminologi Indonesia*, 10(1), 88–102.

Gusdania, L., & Vedercia, M. (2026). Hambatan kelembagaan dalam penegakan hukum kejahatan siber di Indonesia. *Jurnal Hukum dan Teknologi*, 9(1), 45–60.

Ilham, M., Salim, A., & Sudarno. (2025). Tantangan pembuktian bukti elektronik dalam sistem peradilan pidana. *Jurnal Penegakan Hukum*, 11(2), 101–115.

Nur, M., Puluhuwa, F., & Wantu, F. (2023). Peran virtual police dan cyber police dalam penegakan hukum di ruang digital. *Jurnal Hukum Siber*, 5(2), 55–68.

Pardede, H., Setyabudi, R., & Nita, D. (2024). Efektivitas penanganan perkara kejahatan siber di Ditreskrimsus Polda Metro Jaya. *Jurnal Hukum dan Peradilan*, 13(1), 89–105.

Ramadhan, R., Wahyudi, A., & Lbn Batu, T. (2026). Analisis hukum phishing sebagai bentuk illegal access dalam perspektif KUHP baru. *Jurnal Hukum Teknologi*, 7(1), 34–48.

Wardani, S. (2024). Karakteristik bukti elektronik dalam pembuktian perkara siber. *Jurnal Hukum Modern*, 6(2), 77–90.

Yuadi, I. (2023). Forensik digital dalam pembuktian tindak pidana berbasis teknologi informasi. *Jurnal Forensik Hukum*, 4(1), 12–25.

***Peraturan perundang-undangan:***

Asosiasi Penyelenggara Jasa Internet Indonesia. (2024). *Laporan survei penetrasi internet Indonesia 2024*. APJII.

Kominfo-CSIRT. (2024). *Laporan tahunan keamanan siber Indonesia 2024*. Kementerian Komunikasi dan Informatika.

Mahkamah Agung Republik Indonesia. (n.d.). *Pedoman penggunaan informasi dan/atau dokumen elektronik sebagai alat bukti dalam persidangan*. Mahkamah Agung RI.

Politeknik Siber dan Sandi Negara. (2024). *Kajian keamanan siber dan manajemen kerentanan*. PoltekSSN.

Undang-Undang Nomor 1 Tahun 2023 tentang Kitab Undang-Undang Hukum Pidana.

Undang-Undang Nomor 19 Tahun 2016 tentang Perubahan atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik.