Department of Digital Business
Journal of Artificial Intelligence and Digital Business (RIGGS)
Homepage: https://journal.ilmudata.co.id/index.php/RIGGS
Vol. 5 No. 1 (2026) pp: 11130-11146
P-ISSN: 2963-9298, e-ISSN: 2963-914X

Perbandingan Kewenangan Kepolisian Indonesia dan Singapura Dalam Menangani Penipuan Online

Sitti Rahmani Nur[1], Kamal Hidjaz[2], Mursyid[3]
[1,2,3]Magister Ilmu Hukum Universitas Muslim Indonesia
raniidulfitri06@gmail.com

Abstrak

Sitti Rahmani Nur. 0010 02 60 2024. Perbandingan Kewenangan Kepolisan Indonesia dan Singapura dalam menangani Penipuan Online. Dibimbing oleh bapak H.Kamal Hidjaz selaku pembimbing utama dan Bapak H. Mursyid selaku pembimbing.Penelitian ini bertujuan untuk memahami dan menganalisis kebijakan hukum dan kewenangan kepolisian di Indonesia dan Singapura serta Memahami dan Menganalisis persamaan dan perbedaan pendekatan kepolisian Indonesia dan Singapura dalam upaya pencegahan dan pemidanaan terhadap penipuan online.Penelitian ini menggunakan metode penelitian hukum normatif dengan pendekatan perundang-undangan (statute approach), pendekatan konseptual (conceptual approach), dan pendekatan perbandingan (comparative approach). Bahan hukum primer dan sekunder dianalisis secara kualitatif untuk mengkaji konstruksi norma, ruang lingkup kewenangan, serta desain kelembagaan penegakan hukum di kedua negara.Hasil penelitian menunjukkan bahwa meskipun Indonesia secara normatif memiliki kewenangan luas dalam menangani penipuan online melalui regulasi yang tersebar, namun masih terkendala disharmonisasi aturan, koordinasi lembaga, dan keterbatasan teknologi, sedangkan Singapura didukung kerangka hukum yang lebih terintegrasi, struktur terpusat, dan pendekatan intelligence-led policing yang proaktif, sehingga penanganan yang diberikan oleh integrasi substansi hukum, kelembagaan, budaya hukum, dan dukungan teknologi, serta memerlukan harmonisasi regulasi, penguatan kapasitas digital, dan kerja sama internasional.Sebagai Penulis merekomendasikan agar Indonesia melakukan harmonisasi regulasi dan membangun sistem penegakan hukum siber yang terintegrasi berbasis teknologi, memperkuat kapasitas forensik digital dan koordinasi dengan sektor keuangan, serta mengembangkan pendekatan proaktif, literasi digital, dan kerja sama internasional untuk menghadapi penipuan online yang bersifat transnasional.

***Kata kunci**: Penipuan Online, Kewenangan Kepolisian, Penelitian Hukum Normatif, Perbandingan Hukum, Kejahatan Siber, Harmonisasi Regulasi, Forensik Digital, Kejahatan Transnasional.*

1. Latar Belakang

Kemajuan pesat teknologi informasi secara global telah menghasilkan pergeseran signifikan dalam cara masyarakat berinteraksi dan beraktivitas ekonomi. Ekosistem digital yang meluas memfasilitasi berbagai kegiatan secara daring, mulai dari layanan jasa, komunikasi harian, hingga transaksi finansial. Akan tetapi, di balik kemudahan ini, muncul tantangan serius berupa peningkatan kejahatan berbasis teknologi, khususnya penipuan online (Masdi et al., 2025) .

Asia Tenggara mencatat tren yang meningkat tajam dalam lima tahun terakhir. Wilayah ini merupakan target utama online fraud didorong oleh penetrasi internet yang tinggi, pesatnya ekonomi digital, dan disparitas dalam infrastruktur keamanan siber regional. Meskipun sama-sama berkembang pesat, Indonesia dan Singapura memiliki tantangan unik. Indonesia, dengan populasi pengguna internet terbesar di dunia, menghadapi potensi kejahatan online yang tinggi berdasarkan volume. Sebaliknya, Singapura, yang merupakan pusat finansial dan teknologi dengan digitalisasi ekstrem, menarik perhatian pelaku penipuan online internasional sebagai sasaran strategis (Aurelia, 2024) .

Fenomena penipuan online kini menjadi isu global yang menonjol, dan lonjakan kasus terlihat jelas di Indonesia. Data Otoritas Jasa Keuangan (OJK) menunjukkan bahwa kerugian nasional di Indonesia akibat penipuan online telah mencapai Rp 3,2 triliun pada pertengahan tahun 2025 (Arief, 2025) . Perbedaan intensitas juga terlihat dalam laporan harian: Indonesia mencatat 700–800 kasus per hari, melampaui Singapura yang hanya sekitar 140 laporan per hari. Secara kumulatif, Indonesia Anti Scam Centre (IASC) melaporkan total kerugian korban sekitar Rp 4,6 triliun dari lebih dari 225.000 laporan yang masuk sepanjang tahun 2025.

Perkembangan teknologi informasi yang seharusnya memudahkan aktivitas masyarakat justru diiringi oleh meningkatnya kasus penipuan online, yang menunjukkan bahwa pengawasan, regulasi, dan penegakan hukum belum sepenuhnya mampu mengimbangi kompleksitas kejahatan tersebut. Di Indonesia, penanganan penipuan online masih terkendala oleh lemahnya integrasi antara kepolisian, lembaga keuangan, operator seluler, dan penyedia platform digital, sehingga memperlambat pemblokiran rekening, pelacakan transaksi, dan pengamanan bukti digital, terutama karena korban sering melapor terlambat ketika dana sudah dipindahkan ke berbagai rekening.

Salah satu tantangan utama adalah kerangka hukum pidana di Indonesia yang belum sepenuhnya responsif terhadap karakteristik kejahatan berbasis teknologi, mengingat KUHP yang berlaku tidak mengatur secara spesifik penipuan digital dan UU ITE masih menimbulkan polemik penafsiran karena sifatnya yang umum. Keterbatasan ini, ditambah dengan regulasi keamanan siber dan perlindungan data yang masih berkembang, membatasi efektivitas penegakan hukum terhadap kejahatan penipuan online yang bersifat lintas yurisdiksi dan terus berkembang melalui modus seperti social engineering dan phishing (Faisal et al., 2025).

Penanggulangan penipuan online seharusnya wajib didukung oleh kerangka hukum pidana yang adaptif, menyeluruh, dan sigap terhadap perkembangan teknologi informasi. Sistem hukum yang ideal harus memiliki ketentuan khusus tentang kejahatan digital, mengatur secara jelas cara pengumpulan dan pembuktian bukti elektronik, serta menetapkan prosedur penyidikan yang selaras dengan sifat penipuan online yang berkecepatan tinggi, sulit diidentifikasi (anonim), dan melintasi batas wilayah (Cahyono et al., 2025). Dalam konteks Indonesia, diharapkan instrumen hukum yang ada termasuk KUHP, Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik beserta perubahannya (UU 19/2016), UU Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi, serta UU Nomor 1 Tahun 2024 tentang Informasi dan Transaksi Elektronik dapat bekerja secara sinergis untuk menciptakan kepastian hukum dan memperkuat landasan bagi kepolisian dalam melaksanakan penindakan yang lebih efektif.

Selain aspek hukum, negara harus memastikan harmonisasi regulasi dengan kebijakan keamanan siber nasional, yang mencakup peningkatan kapasitas Badan Siber dan Sandi Negara (BSSN), perbaikan tata kelola data, serta pembentukan prosedur kerja sama internasional untuk mengatasi kejahatan digital lintas batas (Arafat & Wirasto, 2024). Pada level operasional, kepolisian secara ideal harus diperkuat dengan teknologi forensik digital, sistem deteksi ancaman yang terintegrasi, dan alat analisis transaksi keuangan mencurigakan UU Tindak Pidana Pencucian Uang (UU No. 8 Tahun 2010) untuk memfasilitasi pelacakan aliran dana hasil penipuan online. Seluruh instrumen dukungan ini wajib disinkronkan untuk menciptakan sistem penegakan hukum yang adaptif dan responsif terhadap modus kejahatan yang terus berkembang.

Singapura, meskipun memiliki infrastruktur digital yang maju, juga mengalami peningkatan signifikan dalam kasus scam. Pada periode November–Desember 2025, Kepolisian Singapura (Singapore Police Force/SPF) melalui Anti-Scam Command (ASCom) bersama tim operasi gabungan dengan bank-bank lokal berhasil mengungkap operasi besar yang menargetkan berbagai jenis penipuan online, seperti government official impersonation scams (penipuan dengan modus peniruan pejabat), investasi palsu, dan scam pekerjaan. Dalam operasi tersebut, kepolisian mengidentifikasi dan membekukan lebih dari 176 rekening bank yang terkait dengan aktivitas penipuan, serta menyita dana hasil kejahatan dengan nilai lebih dari SGD 539.000. Selain itu, SPF melakukan penyelidikan terhadap 176 orang yang diduga terlibat langsung maupun tidak langsung dalam praktik scam, termasuk pihak-pihak yang berperan dalam pencucian uang. Kepolisian juga menjalin kerja sama dengan perusahaan telekomunikasi dan platform digital untuk menghentikan lebih dari 880 online enabler serta menonaktifkan lebih dari 1.070 nomor ponsel yang digunakan sebagai sarana melakukan penipuan (Singapore Police Force, 2025).

Hal ini menunjukkan bahwa kecanggihan digital dapat menjadi celah eksploitasi. Namun, mekanisme penanganan di Singapura lebih unggul dan terintegrasi, dibuktikan dengan keberadaan Anti-Scam Command (ASCom), kolaborasi real-time dengan sektor perbankan, pemanfaatan data analytics, serta didukung oleh kerangka hukum modern (Computer Misuse Act dan Cybersecurity Act) (Indrawan & Zahira, 2024). Tantangan utama di Singapura terletak pada modus sindikat internasional yang makin canggih, memanfaatkan layanan komunikasi terenkripsi dan rekayasa sosial yang sulit dideteksi secara teknis.

Kedua negara (Singapura dan Indonesia) sama-sama menghadapi lonjakan penipuan online; di Singapura, bahkan infrastruktur digital canggih pun menjadi sasaran empuk. Namun, respons Singapura jauh lebih terintegrasi melalui pembentukan ASCom, kerja sama real-time dengan bank, dan instrumen hukum yang lebih adaptif (Computer Misuse Act dan Cybersecurity Act). Tantangan mereka kini adalah berhadapan dengan sindikat internasional yang menggunakan teknik social engineering dan enkripsi canggih.

DOI: https://doi.org/10.31004/riggs.v5i1.7662

Penanganan penipuan online di Indonesia masih menghadapi kendala utama berupa rendahnya literasi digital masyarakat, sehingga banyak korban mudah terjerat phishing dan investasi bodong, yang berkontribusi pada tingginya angka kasus. Kondisi ini berbeda dengan Singapura yang memiliki tingkat literasi digital lebih baik sehingga memungkinkan pencegahan yang lebih efektif. Meskipun telah banyak kajian mengenai penipuan online, penelitian yang ada umumnya bersifat parsial dan lebih menekankan aspek hukum atau teknologi semata, sementara kajian komprehensif mengenai strategi kepolisian termasuk mekanisme operasional, kesiapan infrastruktur TI, dan proses investigasi digital khususnya di Indonesia, masih relatif terbatas.

Mayoritas penelitian komparatif antarnegara lebih menekankan perbedaan kerangka hukum dibandingkan kewenangan operasional kepolisian, padahal kepolisian berperan sebagai garda terdepan dalam penanganan penipuan online melalui pengumpulan bukti digital, koordinasi dengan lembaga terkait, dan kerja sama lintas negara. Oleh karena itu, masih terdapat kebutuhan penelitian yang secara khusus membandingkan kewenangan kepolisian Indonesia dan Singapura dengan pendekatan terpadu yang menggabungkan aspek hukum pidana dan teknologi informasi.

Dari perspektif hukum Islam (Syariah), segala bentuk kejahatan digital, termasuk penipuan online yang memanfaatkan AI, deepfake, atau skema money laundering melalui cryptocurrency, dipandang sebagai tindakan yang dilarang keras (haram) karena melanggar prinsip dasar keadilan dan hak milik. Landasan utama pelarangan ini secara eksplisit ditegaskan dalam Surah An-Nisa' (4) ayat 29 dalam Al-Qur'an:

يَا أَيُّهَا الَّذِينَ آمَنُوا لَا تَأْكُلُوا أَمْوَالَكُم بَيْنَكُم بِالْبَاطِلِ إِلَّا أَن تَكُونَ تِجَارَةً عَن تَرَاضٍ مِّنكُمْ

Terjemahan: "Wahai orang-orang yang beriman! Janganlah kamu saling memakan harta sesamamu dengan jalan yang batil (tidak benar), kecuali dalam perdagangan yang berlaku atas dasar suka sama suka di antara kamu (Q.S. An-Nisa: 4).

Penipuan online dikategorikan sebagai memakan harta dengan jalan yang batil (akl al-mal bi al-batil) karena harta diperoleh melalui manipulasi, kebohongan, dan tanpa adanya kerelaan ('an taradin) yang sah dari pihak korban. Penggunaan teknologi canggih untuk tujuan penipuan tersebut secara esensial adalah bentuk ghish (penipuan) yang dilarang, melanggar etika dan merusak amanah (kepercayaan), serta menimbulkan dharar (kerugian) yang harus dihilangkan berdasarkan prinsip-prinsip umum fiqih.

Berangkat dari berbagai isu, kesenjangan normatif, dan perbedaan pendekatan strategis yang jelas antara Indonesia dan Singapura dalam upaya menanggulangi penipuan online, penulis menyimpulkan adanya urgensi untuk melakukan kajian mendalam. Kajian ini difokuskan pada perumusan dan implementasi kewenangan kepolisian kedua negara, ditinjau dari perspektif integrasi hukum pidana dan teknologi informasi. Dengan demikian, penelitian ini diajukan di bawah judul: "Perbandingan Kewenangan Kepolisian Indonesia dan Singapura dalam Menangani Penipuan Online".

1. Metode Penelitian

Penelitian ini menggunakan tipe penelitian hukum normatif (normative legal research), adalah penelitian hukum dalam wilayah ilmu hukum sendiri dalam artiannya yang luas. Dikatakan dalam artiannya yang luas, oleh karena ilmu hukum memang demikian adanya, memasuki segala aspek keilmuan dengan maksud keberfungsian hukum dalam mencapai tujuannya (Qomar et al., 2017).

Penelitian ini merupakan penelitian hukum normatif yang bersifat deskriptif-komparatif dan analitis, yang bertujuan untuk menggambarkan dan membandingkan kebijakan hukum serta kewenangan kepolisian Indonesia dan Singapura dalam menangani tindak pidana penipuan online. Sifat deskriptif digunakan untuk memaparkan pengaturan hukum dan pendekatan kepolisian dalam upaya pencegahan dan pemidanaan, sedangkan sifat komparatif-analitis diterapkan melalui perbandingan norma hukum dan kebijakan kepolisian guna mengidentifikasi persamaan dan perbedaan pendekatan penanganan penipuan online di kedua negara.

3. Hasil dan Diskusi

Bab ini memaparkan hasil penelitian dan pembahasan mengenai kebijakan hukum dan kewenangan kepolisian Indonesia dan Singapura dalam menangani tindak pidana penipuan online, serta persamaan dan perbedaan pendekatan kepolisian kedua negara dalam upaya pencegahan dan pemidanaan terhadap kejahatan tersebut. Analisis dilakukan berdasarkan penelitian hukum normatif dengan menelaah norma hukum yang berlaku, khususnya peraturan perundang-undangan di bidang hukum pidana dan hukum siber, serta kebijakan penegakan hukum yang dijalankan oleh institusi kepolisian di masing-masing negara.

DOI: https://doi.org/10.31004/riggs.v5i1.7662

Pembahasan rumusan masalah pertama difokuskan pada kajian terhadap kerangka kebijakan hukum dan pengaturan kewenangan kepolisian dalam penanganan penipuan online. Di Indonesia, analisis dilakukan dengan mengacu pada ketentuan Kitab Undang-Undang Hukum Pidana, Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik beserta perubahannya, Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi, serta Undang-Undang Nomor 1 Tahun 2024 tentang Kitab Undang-Undang Hukum Pidana. Sementara itu, di Singapura, pembahasan merujuk pada pengaturan dalam *Computer Misuse Act*, *Penal Code*, dan *Cybersecurity Act* yang menjadi dasar hukum kewenangan kepolisian dalam menangani kejahatan siber, termasuk penipuan online. Kajian ini bertujuan untuk mengidentifikasi ruang lingkup dan batas kewenangan kepolisian, serta orientasi kebijakan hukum yang diterapkan dalam menghadapi penipuan berbasis teknologi informasi.

Selanjutnya, pembahasan rumusan masalah kedua diarahkan pada analisis komparatif mengenai persamaan dan perbedaan pendekatan kepolisian Indonesia dan Singapura dalam upaya pencegahan dan pemidanaan penipuan online. Pendekatan pencegahan (non-penal) dianalisis melalui kebijakan edukasi, literasi digital, serta kerja sama lintas lembaga dan sektor yang didukung oleh norma hukum yang berlaku. Adapun pendekatan pemidanaan (penal) dikaji melalui penerapan ketentuan pidana, mekanisme penyidikan dan penindakan, serta penggunaan alat bukti elektronik dalam proses penegakan hukum. Dengan menggunakan teori perbandingan hukum, teori kebijakan pidana, dan teori penegakan hukum, pembahasan ini diharapkan dapat menunjukkan karakteristik normatif dan praktik penegakan hukum di kedua negara, serta implikasinya terhadap penanganan penipuan online secara efektif dan berkeadilan.

1. Kewenangan Kepolisian untuk menentukan kebijakan hukum dalam menangani penipuan online di Indonesia dan singapura

a. Dasar Hukum dan sumber kewenangan *(Legal Basis)*

Dasar Hukum dan Sumber Kewenangan (Legal Basis) atau legalitas formal yang memberikan mandat kepada kepolisian di kedua negara untuk mengambil tindakan atau menentukan kebijakan hukum dalam menangani penipuan online.

1. Analisis Yuridis di Indonesia (Supremasi Hukum Tertulis)

Di Indonesia, kewenangan kepolisian bersumber pada sistem hukum Eropa Kontinental (Civil Law) yang sangat mengandalkan aturan tertulis.

Tingkat keterpaduan antara pengaturan hukum pidana dan hukum siber dalam penanganan penipuan online di Indonesia masih menunjukkan kondisi yang belum sepenuhnya terintegrasi. Regulasi penipuan online di Indonesia bertumpu pada Undang-Undang Informasi dan Transaksi Elektronik (UU ITE) sebagai pusat pengaturan hukum siber yang memuat ketentuan pidana terhadap perbuatan melawan hukum yang dilakukan dengan menggunakan sarana elektronik. UU ITE memberikan perluasan makna tindak pidana penipuan dengan mengakomodasi karakteristik kejahatan siber, khususnya dalam konteks transaksi elektronik dan penyebaran informasi yang menyesatkan di ruang digital. Namun demikian, keberadaan UU ITE tidak menggantikan peran hukum pidana umum, karena dalam praktiknya ketentuan mengenai penipuan online tetap harus dikaitkan dengan pasal-pasal penipuan dalam KUHP serta berbagai peraturan sektoral lainnya, seperti Undang-Undang Perlindungan Konsumen dan regulasi di bidang perdagangan elektronik (Ibrael et al., 2021).

Kondisi ini menunjukkan bahwa pengaturan hukum pidana dan hukum siber di Indonesia masih berjalan secara paralel dan sektoral, tanpa adanya satu kerangka normatif yang komprehensif dan terintegrasi secara sistematis. Akibatnya, penegakan hukum terhadap penipuan online sangat bergantung pada koordinasi antarinstansi penegak hukum dan penafsiran aparat terhadap norma yang tersebar di berbagai peraturan perundang-undangan, sehingga keterpaduan sistem hukum pidana dan hukum siber di Indonesia dapat dikatakan masih bersifat parsial atau belum matang (inchoate).

UU No. 2 Tahun 2002 tentang Polri: Ini adalah sumber kewenangan utama. Pasal 18 ayat (1) memberikan ruang bagi pejabat Polri untuk bertindak menurut penilaiannya sendiri (Diskresi) jika dalam keadaan mendesak demi kepentingan umum.

Kewenangan yang di makasud yaitu :

1) Kewenangan Atributif: Kewenangan ini bersifat Atributif, artinya kekuasaan tersebut melekat langsung pada jabatan kepolisian yang diberikan oleh pembentuk Undang-Undang. Polisi tidak perlu menunggu "instruksi" dari lembaga lain untuk membuat kebijakan teknis seperti Restorative Justice (RJ) dalam kasus penipuan online, selama hal itu untuk kepentingan umum.

DOI: https://doi.org/10.31004/riggs.v5i1.7662

2) Batasan Hukum: Diskresi di Indonesia dibatasi oleh asas-asas umum pemerintahan yang baik dan tidak boleh bertentangan dengan hukum yang lebih tinggi (asas legalitas) Zahra et al. (2025).

b. Analisis Yuridis di Singapura (Perpaduan Statuta dan Tradisi)

Singapura menggunakan sistem Common Law, di mana kewenangan polisi tidak hanya tertulis dalam undang-undang tetapi juga diakui melalui tradisi hukum.

Police Force Act (Chapter 235): Undang-undang ini adalah dasar hukum statuta yang mengatur operasional Singapore Police Force (SPF). SPF diberikan mandat luas untuk memelihara keamanan ekonomi dan ketertiban sosial dari ancaman siber (Singapore Legal Advice, n.d.).

Kedaulatan Common Law: Kepolisian Singapura memiliki diskresi investigasi yang sangat kuat yang berakar pada hukum Inggris. Hakim-hakim di Singapura memberikan ruang bagi polisi untuk melakukan "tindakan pencegahan" (seperti memblokir rekening secara cepat) karena dianggapsebagai bagian dari fungsi Police Prerogative untuk melindungi publik.

Kewenangan Delegatif & Atributif: Selain memiliki kewenangan atributif dari Police Force Act, kepolisian Singapura sering menerima kewenangan Delegatif dari otoritas lain (seperti otoritas moneter/MAS) untuk melakukan intervensi finansial dalam kasus penipuan.

Adapun persamaan antara kedua negara mengenai dasar hukum dan sumber kewenangannya yaitu :

Mandat Perlindungan: Keduanya memiliki mandat hukum yang sama untuk melindungi warga negara dari kerugian materiil akibat kejahatan ekonomi (penipuan).

Legalitas Diskresi: Keduanya mengakui bahwa hukum tidak bisa mengatur setiap detail kejadian di lapangan, sehingga polisi "wajib" diberi ruang untuk mengambil keputusan sendiri (diskresi) demi kecepatan penanganan.

Tunduk pada Konstitusi: Baik Polri maupun SPF tetap harus mempertanggungjawabkan kebijakan hukum mereka di bawah pengawasan hukum negara masing-masing (Afita et al., 2022).

Adapun perbedaan sumber hukum dan kewenangan kedua negara yaitu :

1) Fleksibilitas Aturan: Singapura lebih fleksibel karena sistem Common Law memungkinkan mereka mengadopsi prosedur baru (seperti kerja sama otomatis dengan Bank) tanpa selalu menunggu revisi Undang-Undang. Di Indonesia, perubahan kebijakan seringkali harus melalui regulasi formal seperti Peraturan Kapolri (Perkap) agar memiliki dasar hukum yang kuat.

2) Fokus Tindakan: Kebijakan hukum di Indonesia lebih sering diarahkan pada penyelesaian masalah sosial (mediasi/RJ), sedangkan di Singapura lebih diarahkan pada kepatuhan sistemik dan pemutusan akses kejahatan secara teknis (Gani et al., 2024).

b. Diskresi dalam Penentuan Prioritas Kasus (Investigative Discretion)

1. Indonesia (Restorative Justice sebagai Kebijakan Utama)

Di Indonesia, Polri telah menggeser paradigma dari sekadar menghukum menjadi pemulihan kerugian korban.

Mekanisme: Berdasarkan Peraturan Kepolisian (Perpol) Nomor 8 Tahun 2021, polisi memiliki kewenangan untuk menghentikan penyidikan penipuan online jika syarat materiil (seperti kerugian telah dikembalikan) dan syarat formil (kesepakatan perdamaian) terpenuhi.

- Prioritas Kasus: Polisi cenderung mendorong penyelesaian di luar pengadilan untuk kasus penipuan dengan nilai kerugian kecil atau yang melibatkan pelaku yang bukan merupakan jaringan sindikat profesional.
- Tujuan Kebijakan: Mengurangi penumpukan perkara di pengadilan (court congestion) dan memastikan hak finansial korban kembali lebih cepat tanpa proses persidangan yang panjang (Chandra et al., 2025).

2. Singapura (Sistem *Warning* yang Terukur)

Singapura melalui Singapore Police Force (SPF) menggunakan pendekatan yang lebih teknokratis dan administratif dalam menangani kasus-kasus tertentu.

Mekanisme Kepolisian Singapura memiliki wewenang untuk memberikan Stern Warning (Peringatan Keras) atau Conditional Warning (Peringatan Bersyarat). Jika pelaku melanggar syarat dalam jangka waktu tertentu (biasanya 12-24 bulan), kasus asalnya akan dibuka kembali.

DOI: https://doi.org/10.31004/riggs.v5i1.7662

Prioritas Kasusnya berbeda dengan Indonesia yang sangat bergantung pada perdamaian antara korban dan pelaku, di Singapura, diskresi ini lebih banyak ditentukan oleh jaksa atau polisi senior berdasarkan profil risiko pelaku. Jika penipuan dianggap sebagai "kesalahan pertama" dengan dampak sosial rendah, warning menjadi pilihan utama.

Tujuan Kebijakannya Efisiensi sumber daya kepolisian agar bisa difokuskan pada pengejaran sindikat scaminternasional yang lebih besar.

Adapun persamaan antara kedua negara yaitu :

1) Prinsip Efisiensi: Keduanya sama-sama mengakui bahwa tidak semua kasus penipuan online harus berakhir di penjara. Ada kebutuhan untuk "menyaring" kasus agar sumber daya negara tidak habis untuk kasus-kasus kecil.

2) Diskresi Pejabat: Penentuan apakah suatu kasus berlanjut atau berhenti sangat bergantung pada penilaian subjektif namun terukur dari penyidik senior/atasan penyidik di kedua negara. Fokus pada Pelaku Non-Residivis: Jalur RJ di Indonesia maupun Warning di Singapura umumnya hanya diberikan kepada pelaku yang baru pertama kali melakukan tindak pidana.

Adapun Perbedaan Titik Tekan Indonesia (Restorative Justice) Singapura (Warnings System)S yarat Utama Harus ada kesepakatan antara korban dan pelaku (Pemulihan Kerugian).Ditentukan oleh otoritas berdasarkan kepentingan publik (Keputusan Polisi/Jaksa).Hasil AkhirKasus dianggap selesai dan "hangus" setelah perdamaian.Kasus "disimpan"; jika berulah lagi, hukuman akan berlipat ganda (Conditional).

Keterlibatan Korban Sangat tinggi; suara korban menentukan apakah kasus lanjut atau tidak.Lebih rendah; polisi yang menentukan apakah demi keadilan kasus cukup diberi peringatan.Landasan KebijakanBerfokus pada keadilan sosial dan sosiologis.Berfokus pada ketertiban hukum dan efisiensi administratif. Dalam pembahasan ini kewenangan kepolisian Indonesia lebih bersifat "mediatif", di mana polisi berperan sebagai fasilitator antara korban dan pelaku. Sementara itu, kewenangan kepolisian Singapura lebih bersifat "direktif", di mana polisi secara mandiri menentukan sanksi alternatif (peringatan) tanpa harus selalu meminta persetujuan korban, asalkan hal tersebut dianggap terbaik menurut standar penegakan hukum mereka. Poin unik yang bisa Anda angkat: Di Indonesia, jika uang kembali, masalah selesai. Di Singapura, meskipun uang kembali, polisi tetap bisa memberikan Conditional Warning sebagai catatan kriminal yang bisa memberatkan pelaku di masa depan (Cahyono et al., 2025).

c. Kewenangan eksekutif dan preventif *(Administrative & Technical Authority)*

Kewenangan ini meninjau sejauh mana kepolisian memiliki otoritas untuk melakukan tindakan teknis seketika, seperti memblokir rekening bank atau akses digital, guna menghentikan peredaran hasil kejahatan sebelum adanya putusan pengadilan.

1. Indonesia (Prosedur Administratif dan Koordinatif)

Di Indonesia, kewenangan Polri dalam pemblokiran aset hasil penipuan online bersifat koordinatif. Berdasarkan UU No. 8 Tahun 2010 tentang Pencegahan dan Pemberantasan TPPU serta aturan turunannya, penyidik Polri memiliki wewenang untuk meminta bank memblokir rekening yang diduga terkait tindak pidana. Namun, dalam praktiknya, proses ini sering kali melewati alur birokrasi yang memakan waktu, di mana polisi harus mengirimkan surat permintaan resmi kepada bank atau melalui Otoritas Jasa Keuangan (OJK) dan BI. Dalam hal pemutusan akses konten (situs/aplikasi), Polri bekerja sama dengan Kementerian Komunikasi dan Digital (dahulu Kominfo) melalui mekanisme pengajuan blokir.

2. Singapura (Otoritas Langsung dan Integrasi Sistem)

Singapura melalui Singapore Police Force (SPF) memiliki kewenangan yang jauh lebih bersifat eksekutif dan terintegrasi secara teknologi. Dengan pembentukan Anti-Scam Centre (ASC) di bawah Commercial Affairs Department, kepolisian memiliki jalur komunikasi langsung (hotline) dan sistem yang terintegrasi dengan bank-bank besar di Singapura. Berdasarkan hukum mereka, polisi memiliki diskresi untuk membekukan rekening yang mencurigakan dalam hitungan menit secara mandiri. Selain itu, melalui undang-undang seperti Online Safety (Miscellaneous Amendments) Act, polisi memiliki kekuatan lebih besar untuk memerintahkan platform media sosial menurunkan konten penipuan secara instan.

Persamaan dalam Kewenangan Preventif Persamaan antara kepolisian Indonesia dan Singapura terletak pada orientasi kebijakan yang mulai bergeser ke arah preventif-administratif. Kedua institusi menyadari bahwa mengejar pelaku setelah uang hilang jauh lebih sulit dibandingkan mencegah uang tersebut keluar dari sistem

DOI: https://doi.org/10.31004/riggs.v5i1.7662

perbankan. Oleh karena itu, baik Polri maupun SPF sama-sama menempatkan kewenangan pemblokiran rekening sebagai instrumen vital dalam penanganan penipuan online. Keduanya juga mengandalkan kolaborasi lintas sektoral dengan institusi finansial dan penyedia jasa telekomunikasi sebagai pilar utama dalam strategi memutus mata rantai penipuan digital.

Perbedaan dalam Kewenangan Preventif, Perbedaan mendasar terletak pada kecepatan eksekusi dan tingkat kemandirian otoritas. Di Indonesia, kewenangan kepolisian cenderung bersifat birokratis-koordinatif, di mana efektivitas pemblokiran sangat bergantung pada kecepatan respons instansi lain (Bank/Kominfo) terhadap surat permohonan kepolisian. Hal ini sering kali menciptakan celah waktu (time gap) yang dimanfaatkan pelaku untuk menguras saldo. Sebaliknya, kepolisian Singapura memiliki kewenangan yang bersifat operasional-mandiri melalui sistem Anti-Scam Centre. Mereka mampu melakukan intervensi teknis secara real-time tanpa terhambat prosedur administrasi yang panjang. Selain itu, di Singapura, kewenangan ini didukung oleh regulasi yang mewajibkan bank untuk bekerja sama secara instan dengan polisi, sedangkan di Indonesia, sinkronisasi antarlembaga masih sering terkendala batasan kerahasiaan bank dan prosedur internal masing-masing institusi (Adhyputra et al., 2024).

Indonesia, unit siber Polri lebih berperan sebagai sub-unit teknis dalam struktur penegakan hukum yang masih konvensional. Sementara itu, di Singapura, unit siber diposisikan sebagai core institution dalam penanganan penipuan online. Perbedaan ini berimplikasi langsung pada kecepatan, konsistensi, dan kualitas penanganan perkara penipuan online.

3. Mekanisme koordinasi internal dan antarlembaga kepolisian indonesia dan Singapura

Mekanisme koordinasi internal dan antarlembaga dalam penanganan penipuan online oleh Kepolisian Negara Republik Indonesia (Polri) telah tersedia secara normatif, namun belum terbangun sebagai sistem koordinasi yang terintegrasi dan responsif. Secara internal, koordinasi penanganan penipuan online melibatkan beberapa unit, terutama Direktorat Tindak Pidana Siber (*Dittipidsiber*) Bareskrim Polri dan Direktorat Reserse Kriminal Khusus (Ditreskrimsus) di tingkat daerah. Namun, hasil penelitian menemukan bahwa hubungan koordinatif antar-unit tersebut masih bersifat hierarkis dan prosedural, sehingga proses pengambilan keputusan dan distribusi kewenangan berjalan relatif lambat.

Dalam konteks koordinasi antarlembaga, Polri berinteraksi dengan sejumlah institusi strategis, seperti PPATK, Otoritas Jasa Keuangan (OJK), perbankan, dan penyedia layanan digital (Willyams & Yusuf, 2024). Akan tetapi, mekanisme koordinasi tersebut umumnya dilakukan melalui prosedur administratif formal dan belum didukung oleh sistem pertukaran data yang bersifat real time. Akibatnya, penanganan penipuan online sering kali terlambat merespons dinamika kejahatan yang bergerak cepat.

Selain itu, tidak terdapat satu mekanisme koordinasi nasional yang bersifat operasional untuk mengintegrasikan pelaporan korban, penyelidikan, pembekuan dana, dan pemulihan kerugian. Kondisi ini menyebabkan koordinasi berjalan secara sektoral dan bergantung pada inisiatif masing-masing instansi.

Dengan demikian, mekanisme koordinasi internal dan antarlembaga Polri dalam penanganan penipuan online masih bersifat reaktif dan terfragmentasi, belum menjadi sistem penegakan hukum yang terpadu.

Berbeda dengan Indonesia, hasil penelitian menunjukkan bahwa Singapore Police Force (SPF) menerapkan mekanisme koordinasi internal dan antarlembaga yang terpusat, terintegrasi, dan berorientasi pada kecepatan respons. Koordinasi internal dalam SPF tidak terpisah secara kaku antara unit penyelidikan, unit siber, dan unit intelijen. Seluruh fungsi tersebut dijalankan dalam satu kerangka kerja terpadu yang memungkinkan pertukaran informasi secara cepat dan pengambilan keputusan yang efisien.

Dalam koordinasi antarlembaga, SPF melalui Anti-Scam Centre (ASC) berfungsi sebagai simpul koordinasi nasional yang menghubungkan kepolisian dengan lembaga keuangan, penyedia layanan digital, dan otoritas pemerintah lainnya. Hasil penelitian menemukan bahwa mekanisme ini memungkinkan pembekuan rekening dan pelacakan dana dilakukan segera setelah laporan diterima, bahkan sebelum proses penyidikan formal dimulai.

Dengan adanya sistem koordinasi yang terlembaga dan berbasis teknologi, penanganan penipuan online di Singapura berjalan secara proaktif, preventif, dan responsif, tidak terbatas pada penindakan pascakejadian.

Perbedaan mekanisme koordinasi antara Polri dan SPF menunjukkan perbedaan pendekatan sistemik dalam penegakan hukum terhadap kejahatan siber.

Dalam perspektif teori sistem penegakan hukum, efektivitas penanganan kejahatan tidak hanya ditentukan oleh kewenangan normatif, tetapi juga oleh kemampuan institusi untuk membangun koordinasi yang terintegrasi

DOI: https://doi.org/10.31004/riggs.v5i1.7662

(Nuruzzaman & Fatimah, 2025). Polri masih mengandalkan model koordinasi birokratis yang berjenjang, sehingga tidak sejalan dengan karakter penipuan online yang cepat dan lintas sektor.

Sebaliknya, SPF menerapkan pendekatan integrated law enforcement system, di mana koordinasi internal dan antarlembaga dirancang sebagai satu kesatuan operasional. Pendekatan ini sejalan dengan teori governance-based policing, yang menekankan kolaborasi lintas sektor sebagai elemen kunci penegakan hukum modern.

4. Kerja sama lintas sektor dan lintas negara

Perbedaan mendasar antara Indonesia dan Singapura dalam membangun dan mengoperasionalkan kerja sama lintas sektor dan lintas negara dalam penanganan penipuan online.Di Indonesia, kerja sama lintas sektor dalam penanganan penipuan online secara normatif telah diatur melalui berbagai regulasi, antara lain UU ITE, UU Kepolisian, serta kebijakan sektoral di bidang komunikasi dan keuangan. Polri secara formal dapat berkoordinasi dengan Kementerian Komunikasi dan Informatika, Otoritas Jasa Keuangan, perbankan, dan penyelenggara sistem elektronik. Namun, dalam praktiknya, kerja sama tersebut masih bersifat reaktif, parsial, dan berbasis permintaan, terutama setelah laporan pidana diajukan. Tidak ditemukan mekanisme operasional yang bersifat permanen dan terintegrasi dalam satu sistem penanganan penipuan online.

Pada level lintas negara, Polri bergantung pada mekanisme kerja sama internasional konvensional seperti Mutual Legal Assistance (MLA), Interpol, dan kerja sama bilateral (Ramadanti, 2024). Proses ini cenderung memakan waktu panjang dan kurang adaptif terhadap karakter kejahatan penipuan online yang bersifat cepat, lintas yurisdiksi, dan menggunakan infrastruktur digital global.

Sebaliknya, Singapura menunjukkan model kerja sama lintas sektor dan lintas negara yang lebih terstruktur dan proaktif. Singapore Police Force (SPF) memiliki kerja sama institusional yang erat dengan otoritas keuangan, penyedia layanan digital, operator telekomunikasi, dan platform daring melalui skema pertukaran data dan respons cepat. Dalam konteks lintas negara, SPF secara aktif terlibat dalam jaringan kerja sama regional dan internasional, tidak hanya dalam kerangka penegakan hukum formal, tetapi juga melalui operational task force, joint investigation, dan real-time intelligence sharing.

Perbedaan kewenangan kerja sama lintas sektor dan lintas negara antara Indonesia dan Singapura mencerminkan dua paradigma kebijakan hukum pidana yang berbeda dalam merespons penipuan online. Indonesia masih menempatkan kerja sama tersebut sebagai instrumen pendukung penyidikan yang bersifat reaktif, sehingga koordinasi antarlembaga dan mitra internasional umumnya baru berjalan setelah kerugian terjadi dan pelaku sulit dilacak. Kondisi ini sejalan dengan temuan penelitian terdahulu yang menunjukkan bahwa penegakan hukum siber di Indonesia masih terfragmentasi akibat pendekatan sektoral dan ketergantungan pada mekanisme MLA yang kurang adaptif terhadap karakter kejahatan siber yang cepat dan lintas batas.

Sebaliknya, Singapura mengadopsi pendekatan *whole-of-government* dan *whole-of-society* dengan menempatkan kerja sama lintas sektor dan lintas negara sebagai elemen sentral penegakan hukum siber yang berorientasi pada *risk management* dan *harm prevention*. Pendekatan ini sejalan dengan teori *networked governance*, yang menegaskan bahwa kejahatan siber tidak dapat ditangani secara unilateral oleh negara. Perbedaan paradigma kebijakan ini menjelaskan mengapa efektivitas penanganan dan pemulihan kerugian korban penipuan online di Singapura relatif lebih tinggi dibandingkan Indonesia, bukan semata karena perbedaan kapasitas teknis kepolisian, melainkan karena pilihan desain kebijakan hukum pidana yang lebih adaptif dan terintegrasi.

d. Struktur Organisasi dan Spesialisasi *(Institutional Capacity)*

1. Indonesia (Model Direktorat yang Tersebar *(Dittipidsiber)*

Perbedaan Di Indonesia, penanganan penipuan online dipusatkan pada Direktorat Tindak Pidana Siber (Dittipidsiber) di bawah Bareskrim Polri.

Struktur Organisasi ini bersifat hierarkis dari tingkat Mabes hingga Polda (Unit Siber). Kebijakan hukum yang lahir cenderung bersifat penegakan hukum murni (law enforcement), di mana fokus utamanya adalah penyidikan tindak pidana setelah laporan masuk.

Meskipun telah memiliki unit khusus, tantangan utama di Indonesia adalah luas wilayah geografi yang besar, sehingga kebijakan penanganan seringkali mengalami hambatan distribusi personel yang memiliki kompetensi siber secara merata hingga ke tingkat Polres.

DOI: https://doi.org/10.31004/riggs.v5i1.7662

2. Singapura (Model Hub Terintegrasi / *Anti-Scam Centre*)

Sistem Singapura memiliki struktur yang lebih modern dan bersifat kolaboratif-sentralistik. SPF membentuk Anti-Scam Centre (ASC) di bawah Commercial Affairs Department (CAD) dan Anti-Scam Command.

Struktur: Berbeda dengan direktorat siber biasa, ASC bertindak sebagai hub di mana personel kepolisian, perwakilan bank, dan penyedia layanan digital duduk dalam satu atap.

Kapasitas: Struktur ini memungkinkan lahirnya kebijakan yang bersifat intervensi cepat. Polisi tidak bekerja sendiri; mereka mengintegrasikan fungsi intelijen keuangan dengan kekuatan kepolisian untuk merespons serangan penipuan secara terpusat dan masif.

Persamaan antara kepolisian Indonesia dan Singapura terlihat pada adanya kesadaran akan pentingnya spesialisasi. Kedua negara telah membentuk unit khusus siber dan ekonomi yang terpisah dari kepolisian konvensional (reserse umum). Hal ini menunjukkan bahwa baik Polri maupun SPF mengakui bahwa penipuan online adalah kejahatan tingkat tinggi yang memerlukan keahlian teknis (technical expertise) di luar ilmu kepolisian dasar. Kedua institusi juga terus meningkatkan investasi pada pengembangan sumber daya manusia melalui pelatihan forensik digital dan analisis data untuk mendukung kebijakan hukum yang mereka jalankan.

Adapun Perbedaan dalam Struktur Organisasi terletak pada sifat dan jangkauan operasionalnya. Struktur kepolisian Indonesia bersifat sektoral dan reaktif, di mana Direktorat Siber bekerja dalam koridor penyidikan hukum pidana yang formal dan cenderung terpisah dari institusi keuangan. Akibatnya, kebijakan yang dihasilkan seringkali terbatas pada proses pengejaran pelaku (hilir). Sebaliknya, struktur kepolisian Singapura bersifat holistik dan proaktif melalui pembentukan Anti-Scam Command yang mengintegrasikan polisi dengan sektor swasta (Bank dan Telco). Struktur ini memungkinkan Singapura menjalankan kebijakan "pencegahan instan" yang tidak hanya fokus pada penangkapan pelaku, tetapi juga pada penyelamatan aset korban secara real-time. Singkatnya, organisasi kepolisian Indonesia dirancang untuk menyelidiki kejahatan, sedangkan organisasi kepolisian Singapura dirancang untuk menghentikan kejahatan saat sedang berlangsung (Cahyono et al., 2025).

2. Persamaan Dan Perbedaan Pendekatan Kepolisian Indonesia Dan Singapura Dalam Upaya Pencegahan Terhadap Penipuan Online

a. Pendekatan Pencegahan (Non-Penal).

1) Strategi pencegahan yang digunakan oleh kepolisian

Perbedaan mendasar dalam strategi pencegahan penipuan online yang diterapkan oleh Kepolisian Indonesia dan Kepolisian Singapura. Di Indonesia, strategi pencegahan yang dilakukan oleh Kepolisian Negara Republik Indonesia (Polri) masih didominasi oleh pendekatan konvensional dan edukatif, seperti sosialisasi kepada masyarakat, publikasi imbauan melalui media massa dan media sosial, serta pengembangan layanan pengaduan daring. Upaya pencegahan ini bersifat reaktif dan belum sepenuhnya terintegrasi dengan mekanisme deteksi dini berbasis teknologi.

Penelitian juga menemukan bahwa pencegahan penipuan online di Indonesia belum ditempatkan sebagai bagian utama dari kebijakan penegakan hukum pidana, melainkan sebagai aktivitas pendukung di luar proses penyidikan dan pemidanaan. Keterbatasan integrasi data, keterbatasan kewenangan preventif, serta fragmentasi koordinasi antarinstansi menyebabkan strategi pencegahan Polri lebih berorientasi pada peningkatan kesadaran masyarakat daripada pengendalian risiko kejahatan secara sistematis.

Sebaliknya, Singapura menerapkan strategi pencegahan yang terstruktur, berbasis teknologi, dan terintegrasi dalam kebijakan penegakan hukum siber. Hasil penelitian menunjukkan bahwa Singapore Police Force (SPF) mengembangkan pendekatan pencegahan melalui sistem deteksi dini, pemantauan transaksi mencurigakan, kolaborasi erat dengan sektor perbankan dan platform digital, serta intervensi cepat untuk menghentikan aliran dana hasil penipuan. Keberadaan Anti-Scam Centre (ASC) menjadi instrumen utama yang mengintegrasikan fungsi pencegahan, respons cepat, dan pemulihan kerugian korban.

Perbedaan strategi pencegahan tersebut dapat dijelaskan melalui teori kebijakan hukum pidana dan pencegahan kejahatan. Di Indonesia, pendekatan Polri masih mencerminkan *social prevention* yang menitikberatkan pada edukasi dan peningkatan kesadaran masyarakat, sehingga kurang efektif menghadapi penipuan online yang terorganisasi, lintas batas, dan berbasis teknologi. Temuan ini sejalan dengan penelitian terdahulu yang menunjukkan bahwa strategi pencegahan siber di Indonesia masih parsial dan belum terintegrasi dalam sistem penegakan hukum digital.

Sebaliknya, strategi pencegahan SPF sejalan dengan teori *situational crime prevention* dan *risk-based policing* yang menekankan intervensi struktural dan penggunaan teknologi untuk mengurangi peluang dan dampak

DOI: https://doi.org/10.31004/riggs.v5i1.7662

kejahatan. Penelitian sebelumnya membuktikan bahwa pencegahan berbasis teknologi dan kerja sama lintas sektor lebih efektif dibandingkan pendekatan edukatif semata. Dengan demikian, meskipun kedua negara mengakui pentingnya pencegahan, perbedaan terletak pada tingkat integrasi dan orientasi kebijakan, di mana Polri masih memposisikan pencegahan sebagai fungsi tambahan, sedangkan SPF menjadikannya pilar utama pengendalian kejahatan siber.

2) Peran edukasi, literasi digital, dan keterlibatan masyarakat.

Kepolisian Indonesia maupun Kepolisian Singapura sama-sama mengakui pentingnya edukasi, literasi digital, dan keterlibatan masyarakat sebagai bagian dari strategi pencegahan penipuan online. Di Indonesia, Kepolisian Negara Republik Indonesia (Polri) menjalankan peran edukatif melalui sosialisasi, kampanye publik, penyebaran imbauan di media massa dan media sosial, serta kerja sama terbatas dengan lembaga pendidikan dan komunitas masyarakat. Pendekatan ini menempatkan masyarakat sebagai objek perlindungan yang perlu diberi pemahaman agar tidak menjadi korban kejahatan penipuan online.

Namun, hasil penelitian juga menunjukkan bahwa peran edukasi dan literasi digital di Indonesia belum terintegrasi secara sistematis dengan kebijakan penegakan hukum pidana. Program edukasi cenderung bersifat sporadis, bergantung pada inisiatif institusional, dan belum diukur secara jelas dampaknya terhadap penurunan tingkat kejahatan. Keterlibatan masyarakat lebih banyak dibatasi pada pelaporan pascakejadian, bukan sebagai aktor aktif dalam sistem pencegahan dini.

Sebaliknya, di Singapura, edukasi dan literasi digital diposisikan sebagai bagian integral dari kebijakan pencegahan penipuan online yang terstruktur. Singapore Police Force (SPF) secara aktif melibatkan masyarakat melalui kampanye nasional anti-scam, kerja sama intensif dengan sektor pendidikan, komunitas lokal, serta platform digital. Masyarakat tidak hanya dipandang sebagai korban potensial, tetapi sebagai mitra strategis dalam deteksi dini dan penyebaran informasi mengenai modus penipuan terbaru.

Perbedaan tersebut dapat dijelaskan melalui teori pencegahan kejahatan dan teori partisipasi masyarakat dalam penegakan hukum. Pendekatan Polri masih mencerminkan paradigma pencegahan klasik yang menitikberatkan pada perubahan perilaku individu melalui edukasi (*social prevention*). Penelitian terdahulu menunjukkan bahwa pendekatan ini memiliki keterbatasan ketika dihadapkan pada kejahatan siber yang kompleks dan adaptif, karena kesadaran masyarakat saja tidak cukup tanpa dukungan sistem dan teknologi yang memadai.

Sebaliknya, pendekatan SPF sejalan dengan teori *community-based crime prevention* dan *networked governance*, yang menempatkan masyarakat sebagai bagian dari ekosistem penegakan hukum. Penelitian sebelumnya menunjukkan bahwa keterlibatan aktif masyarakat, jika dikombinasikan dengan teknologi dan koordinasi kelembagaan, mampu meningkatkan efektivitas pencegahan penipuan online secara signifikan. Oleh karena itu, efektivitas pendekatan Singapura tidak semata bergantung pada tingkat literasi digital masyarakat, tetapi pada desain kebijakan hukum yang mengintegrasikan edukasi, partisipasi publik, dan kewenangan kepolisian dalam satu sistem pencegahan yang kohesif.

Dengan demikian, persamaan antara Indonesia dan Singapura terletak pada pengakuan terhadap pentingnya edukasi dan literasi digital. Namun, perbedaannya terletak pada posisi strategis peran tersebut dalam kebijakan penegakan hukum. Di Indonesia, edukasi dan keterlibatan masyarakat masih bersifat komplementer, sementara di Singapura menjadi pilar utama dalam strategi pencegahan penipuan online. Perbedaan ini menegaskan bahwa keberhasilan pencegahan berbasis masyarakat sangat ditentukan oleh sejauh mana kebijakan hukum pidana mampu mengintegrasikan peran publik ke dalam sistem penegakan hukum siber secara menyeluruh.

3) Kolaborasi dengan sektor swasta dan penyedia layanan digital

kolaborasi dengan sektor swasta dan penyedia layanan digital menjadi salah satu pembeda utama pendekatan Kepolisian Indonesia dan Kepolisian Singapura dalam menangani penipuan online. Di Indonesia, Kepolisian Negara Republik Indonesia (Polri) telah menjalin kerja sama dengan perbankan, operator telekomunikasi, dan platform digital, terutama dalam konteks pelacakan aliran dana dan pemutusan akses komunikasi pelaku. Namun, kerja sama tersebut pada umumnya bersifat ad hoc, terbatas pada tahap penyidikan, dan sangat bergantung pada permintaan resmi berbasis prosedur hukum.

Penelitian menemukan bahwa keterbatasan dasar hukum yang eksplisit serta kuatnya pendekatan sektoral menyebabkan kolaborasi Polri dengan sektor swasta belum terintegrasi secara sistematis dalam strategi pencegahan dan pemidanaan. Penyedia layanan digital cenderung diposisikan sebagai pihak pendukung proses pembuktian, bukan sebagai mitra strategis dalam deteksi dini dan pengendalian risiko penipuan online.

DOI: https://doi.org/10.31004/riggs.v5i1.7662

Sebaliknya, Singapura menunjukkan pola kolaborasi yang lebih terstruktur dan berkelanjutan antara Singapore Police Force (SPF) dengan sektor swasta dan penyedia layanan digital. Hasil penelitian mengungkapkan bahwa SPF memiliki mekanisme kerja sama langsung dengan lembaga keuangan, platform e-commerce, dan penyedia layanan digital untuk melakukan pemantauan transaksi mencurigakan, pembekuan rekening secara cepat, serta penutupan akun pelaku. Kolaborasi ini tidak hanya dilakukan pada tahap pemidanaan, tetapi telah menjadi bagian integral dari strategi pencegahan penipuan online.

Perbedaan tersebut dapat dijelaskan melalui teori kebijakan hukum pidana dan teori *networked governance*. Dalam konteks Indonesia, pendekatan penegakan hukum masih menempatkan negara sebagai aktor utama yang bekerja secara hierarkis, sementara sektor swasta diposisikan sebagai pihak eksternal yang membantu proses penyidikan. Penelitian terdahulu menunjukkan bahwa pendekatan ini kurang efektif dalam menghadapi kejahatan siber yang bergantung pada infrastruktur dan data yang dikuasai oleh aktor non-negara.

Sebaliknya, pendekatan Singapura sejalan dengan teori *networked governance* dan *public–private partnership*, yang menekankan pentingnya kolaborasi negara dan aktor non-negara dalam mengelola risiko kejahatan modern. Penelitian sebelumnya menunjukkan bahwa keterlibatan aktif sektor swasta dan penyedia layanan digital secara signifikan meningkatkan efektivitas pencegahan dan pemidanaan penipuan online, khususnya dalam menghentikan aliran dana dan memutus jaringan pelaku secara cepat.

Dengan demikian, persamaan antara Indonesia dan Singapura terletak pada pengakuan bahwa kolaborasi dengan sektor swasta merupakan kebutuhan dalam penanganan penipuan online. Namun, perbedaannya terletak pada posisi strategis kolaborasi tersebut dalam kebijakan penegakan hukum. Polri masih memandang kerja sama dengan sektor swasta sebagai instrumen pendukung, sementara SPF menempatkannya sebagai pilar utama dalam strategi pencegahan dan pemidanaan. Perbedaan ini menegaskan bahwa efektivitas penanganan penipuan online sangat ditentukan oleh sejauh mana kebijakan hukum pidana mampu mengintegrasikan peran aktor non-negara ke dalam sistem penegakan hukum siber secara komprehensif.

b. Pendekatan Pemidanaan (Penal)

1) Pola penyidikan dan penindakan terhadap pelaku penipuan online

Pola penyidikan dan penindakan penipuan online yang dilakukan oleh Kepolisian Negara Republik Indonesia (Polri) dan Singapore Police Force (SPF) memiliki perbedaan mendasar baik dari aspek struktur kelembagaan, penggunaan teknologi, maupun orientasi kebijakan penegakan hukum.

Di Indonesia, penyidikan penipuan online oleh Polri masih didominasi oleh pendekatan reaktif dan laporan-based, yaitu penyidikan baru berjalan secara aktif setelah adanya laporan dari korban. Proses penyelidikan umumnya mengikuti mekanisme hukum pidana konvensional dengan penyesuaian terbatas pada alat bukti elektronik sebagaimana diatur dalam UU ITE. Dalam praktiknya, penanganan perkara penipuan online sering terkendala oleh keterbatasan kapasitas forensik digital, fragmentasi kewenangan antar unit, serta hambatan yurisdiksi ketika pelaku atau server berada di luar wilayah Indonesia.

Sebaliknya, SPF menerapkan pola penyidikan yang bersifat proaktif, intelligence-led, dan berbasis risiko (risk-based enforcement). Penindakan tidak selalu menunggu laporan korban, tetapi dapat dipicu oleh analisis data transaksi mencurigakan, laporan dari bank dan penyedia platform digital, serta pemantauan sistemik terhadap modus penipuan yang sedang berkembang. SPF memiliki unit khusus dengan kewenangan teknis dan legal yang terintegrasi, memungkinkan penindakan cepat seperti pembekuan rekening, pemblokiran akun, dan penelusuran aset hasil kejahatan secara lintas sektor.

2) Penanganan kejahatan siber lalu lintas

konteks penanganan penipuan online lintas batas (cross-border cyber fraud), baik Indonesia maupun Singapura sama-sama menghadapi tantangan yurisdiksi, perbedaan sistem hukum, serta kompleksitas pelacakan aliran dana digital. Namun, pendekatan yang ditempuh kedua negara menunjukkan perbedaan signifikan dalam kapasitas respons dan integrasi kerja sama internasional.

Di Indonesia, kewenangan penanganan kejahatan siber lintas batas berada pada Kepolisian Negara Republik Indonesia, khususnya melalui Bareskrim Polri dan Divisi Hubungan Internasional (Divhubinter). Kerja sama internasional dilakukan melalui mekanisme mutual legal assistance (MLA), ekstradisi, serta kerja sama kepolisian internasional melalui INTERPOL.

Di Singapura, kewenangan berada pada Singapore Police Force, terutama Commercial Affairs Department (CAD). Singapura juga aktif dalam jaringan kerja sama internasional, baik dalam kerangka ASEAN,

DOI: https://doi.org/10.31004/riggs.v5i1.7662

INTERPOL, maupun perjanjian bilateral. Posisi Singapura sebagai pusat keuangan regional memperkuat urgensi dan kapasitasnya dalam membangun sistem koordinasi lintas negara.

c. Pola Penegakan Hukum Kepolisian

1) Model Penegakan Hukum (reaktif, proaktif, atau kombinasi)

perbedaan paling mendasar antara Indonesia dan Singapura dalam menangani penipuan online terletak pada model penegakan hukum yang diterapkan, yaitu apakah bersifat reaktif, proaktif, atau kombinasi keduanya.

Di Indonesia, kewenangan penanganan penipuan online berada pada Kepolisian Negara Republik Indonesia, khususnya Direktorat Tindak Pidana Siber Bareskrim Polri dan unit siber di tingkat wilayah. Secara umum, model penegakan hukum yang diterapkan masih dominan bersifat reaktif, yakni penegakan hukum berjalan setelah adanya laporan dari korban.

Sebaliknya, di Singapura, kewenangan berada pada Singapore Police Force melalui Commercial Affairs Department (CAD). Model yang diterapkan cenderung merupakan kombinasi proaktif dan represif, dengan penekanan kuat pada pencegahan dini dan deteksi berbasis intelijen.

a. Model Penegakan Hukum di Indonesia: Dominasi Reaktif

Hasil penelitian menunjukkan bahwa pendekatan Indonesia terhadap penipuan online memiliki karakteristik sebagai berikut:

- Berbasis laporan (complaint-driven system)

Proses hukum umumnya dimulai setelah korban melapor. Tanpa laporan, aparat jarang melakukan investigasi mandiri kecuali dalam kasus besar atau viral.

- Fokus pada penindakan pasca-kejadian

Penyidikan, penangkapan, dan proses peradilan dilakukan setelah kerugian terjadi.

- Upaya preventif bersifat normatif dan edukatif

Pencegahan lebih banyak berupa imbauan publik, kampanye literasi digital, dan kerja sama terbatas dengan platform digital.

Secara struktural, pendekatan ini menunjukkan bahwa hukum pidana difungsikan terutama sebagai alat represif (penal control) setelah delik terjadi.

b. Model Penegakan Hukum di Singapura: Kombinasi Proaktif dan Represif

Berbeda dengan Indonesia, Singapura menunjukkan model kombinasi dengan ciri-ciri:

- Deteksi dini melalui sistem intelijen dan analisis transaksi mencurigakan
  Aparat tidak hanya menunggu laporan korban, tetapi memanfaatkan sistem monitoring keuangan dan digital.
- Peringatan publik dan intervensi sebelum kerugian meluas
  Polisi secara rutin mengeluarkan scam alerts dan peringatan berbasis tren terbaru.
- Represif yang cepat dan konsisten Ketika tindak pidana teridentifikasi, proses penegakan hukum dilakukan dengan cepat dan terstandarisasi.

Model ini memperlihatkan bahwa fungsi pencegahan (preventive policing) berjalan seiring dengan fungsi penindakan (law enforcement).

2) Pendekatan teknologi dalam proses penegakan hukum

Hasil penelitian menunjukkan bahwa Indonesia telah mengadopsi teknologi digital forensik dalam proses penyidikan penipuan online, antara lain melalui pemeriksaan perangkat elektronik di laboratorium forensik digital, pelacakan aliran dana dengan berkoordinasi bersama pihak perbankan, serta pemblokiran situs atau akun digital melalui kerja sama dengan otoritas terkait di bawah koordinasi Kepolisian Negara Republik Indonesia.

Meskipun demikian, pemanfaatan teknologi tersebut masih menghadapi sejumlah kendala struktural. Integrasi data antar lembaga belum berjalan secara optimal sehingga pertukaran informasi seringkali tidak berlangsung secara real-time. Selain itu, keterbatasan sumber daya manusia yang memiliki keahlian teknis lanjutan di bidang digital forensik dan analisis data turut memengaruhi efektivitas penanganan perkara. Prosedur administratif yang panjang juga kerap memperlambat respons terhadap kejahatan digital yang berlangsung sangat cepat. Dalam konteks ini, teknologi di Indonesia cenderung berfungsi sebagai alat pembuktian (evidentiary tool) setelah tindak

DOI: https://doi.org/10.31004/riggs.v5i1.7662

pidana terjadi, bukan sebagai instrumen deteksi dini yang terintegrasi secara sistemik dalam model pencegahan kejahatan.

Sebaliknya, Singapura menunjukkan model pemanfaatan teknologi yang lebih terintegrasi dan berorientasi preventif di bawah kewenangan Singapore Police Force. Teknologi tidak hanya digunakan untuk kepentingan pembuktian di tahap penyidikan, tetapi juga untuk melakukan analisis otomatis terhadap pola transaksi mencurigakan, memantau tren penipuan digital secara berkala, serta menyampaikan peringatan publik berdasarkan data dan pola kejahatan terbaru.

Integrasi yang erat antara sistem kepolisian dan sektor keuangan memungkinkan deteksi serta intervensi dilakukan dengan cepat sebelum kerugian korban semakin meluas. Dengan demikian, teknologi di Singapura berfungsi tidak hanya sebagai instrumen penindakan, tetapi sekaligus sebagai sarana pencegahan yang sistemik dan berbasis intelijen.

Berdasarkan hasil penelitian, terdapat sejumlah persamaan dan perbedaan yang signifikan antara Indonesia dan Singapura dalam pemanfaatan teknologi untuk penanganan penipuan online. Persamaannya, kedua negara sama-sama memanfaatkan teknologi digital forensik dalam proses pembuktian perkara penipuan online serta menjalin kerja sama dengan sektor perbankan dan penyedia layanan digital dalam pelacakan transaksi keuangan dan jejak elektronik. Namun demikian, terdapat perbedaan mendasar dalam orientasi dan tingkat integrasinya. Indonesia cenderung menggunakan teknologi sebagai instrumen represif yang diaktifkan setelah tindak pidana terjadi, sedangkan Singapura memanfaatkannya sebagai alat deteksi dini dan pencegahan berbasis analisis data. Integrasi sistem digital antar lembaga di Singapura juga lebih kuat dan terkoordinasi dibandingkan Indonesia, sehingga memungkinkan pertukaran informasi berlangsung lebih cepat dan efisien. Kecepatan respons berbasis teknologi di Singapura relatif lebih tinggi karena struktur birokrasi yang lebih ringkas dan terpusat.

Secara analitis dapat disimpulkan bahwa efektivitas penegakan hukum terhadap penipuan online tidak semata-mata ditentukan oleh ketersediaan perangkat teknologi, melainkan oleh kemampuan negara mengintegrasikan teknologi tersebut ke dalam sistem penegakan hukum yang responsif, terkoordinasi, dan berbasis data. Dengan demikian, reformasi kebijakan di Indonesia perlu diarahkan pada penguatan integrasi sistem digital lintas lembaga, peningkatan kapasitas sumber daya manusia di bidang forensik siber, serta transformasi dari model pemanfaatan teknologi yang bersifat reaktif menuju model yang lebih preventif dan prediktif dalam kerangka penegakan hukum modern.

3) Konsinstensi Pelaksanaan Kepolisian

konsistensi pelaksanaan kewenangan kepolisian dalam menangani penipuan online menjadi salah satu indikator utama yang membedakan pendekatan Indonesia dan Singapura. Secara normatif, kedua negara telah memberikan kewenangan yang cukup jelas kepada institusi kepolisian untuk melakukan penyelidikan, penyidikan, penangkapan, penyitaan, hingga koordinasi lintas lembaga dalam perkara penipuan berbasis elektronik. Namun, tingkat konsistensi implementasinya menunjukkan perbedaan yang signifikan.

Di Indonesia, kewenangan tersebut berada pada Kepolisian Negara Republik Indonesia melalui Direktorat Tindak Pidana Siber Bareskrim Polri serta unit siber pada tingkat Polda dan Polres. Secara normatif, kewenangan telah diatur dalam KUHAP, KUHP, dan UU ITE. Akan tetapi, penelitian menunjukkan adanya variasi pelaksanaan kewenangan antar wilayah, baik dalam kecepatan respons, kualitas penyidikan, maupun koordinasi dengan lembaga lain.

Sebaliknya, di Singapura, kewenangan berada pada Singapore Police Force, khususnya Commercial Affairs Department (CAD). Pelaksanaan kewenangan relatif lebih terpusat dan seragam, dengan standar operasional prosedur (SOP) yang konsisten serta pengawasan internal yang ketat.

d. Persamaan dan Perbedaan Pendekatan

1) Persamaan Pendekatan Kepolisian Indonesia

Hasil Penelitian ini menemukan bahwa meskipun Indonesia dan Singapura memiliki perbedaan dalam kapasitas institusional dan desain kebijakan kriminal, terdapat sejumlah persamaan mendasar dalam pendekatan kepolisian terhadap pencegahan dan pemidanaan penipuan online.

Di Indonesia, penanganan penipuan online berada di bawah kewenangan Kepolisian Negara Republik Indonesia melalui Direktorat Tindak Pidana Siber Bareskrim Polri dan unit siber di tingkat kewilayahan. Di Singapura, kewenangan tersebut dijalankan oleh Singapore Police Force, khususnya melalui Commercial Affairs Department (CAD).

Berdasarkan hasil penelitian, persamaan pendekatan kedua negara dapat diuraikan sebagai berikut:

DOI: https://doi.org/10.31004/riggs.v5i1.7662

a. Kriminalisasi Ekspresif terhadap Penipuan Online

Kedua negara secara eksplisit mengkualifikasikan penipuan online sebagai tindak pidana. Indonesia mengaturnya melalui kombinasi KUHP dan UU ITE, sedangkan Singapura mengaturnya melalui Penal Code dan regulasi terkait kejahatan siber. Hal ini menunjukkan bahwa keduanya memandang penipuan berbasis elektronik sebagai ancaman serius terhadap ketertiban umum dan stabilitas ekonomi.

b. Kepolisian sebagai Leading Sector Penegakan Hukum

Baik Indonesia maupun Singapura menempatkan kepolisian sebagai aktor utama dalam penyelidikan dan penyidikan perkara penipuan online. Kepolisian memiliki kewenangan untuk melakukan pelacakan digital, penyitaan perangkat elektronik, serta koordinasi dengan lembaga keuangan dan otoritas digital.

c. Penggunaan Pendekatan Penal sebagai Instrumen Utama

Kedua negara menjadikan hukum pidana sebagai instrumen utama dalam merespons penipuan online. Pemidanaan berupa penjara dan denda tetap menjadi mekanisme utama untuk memberikan efek jera (deterrence).

d. Kerja Sama dengan Sektor Keuangan dan Penyedia Layanan Digital

Dalam praktiknya, kedua negara menyadari bahwa keberhasilan penanganan penipuan online sangat bergantung pada koordinasi dengan perbankan dan platform digital. Pelacakan aliran dana serta identifikasi akun pelaku menjadi bagian penting dalam proses pembuktian.

2) Perbedaan Pendekatan dalam pencegahan dan pemidanaan

Penelitian ini menemukan bahwa perbedaan paling menonjol antara Indonesia dan Singapura dalam menangani penipuan online terletak pada orientasi kebijakan pencegahan (crime prevention model).

Di Indonesia, pencegahan cenderung bersifat normatif dan edukatif. Kepolisian Negara Republik Indonesia melalui Direktorat Tindak Pidana Siber dan fungsi humas melakukan sosialisasi, imbauan publik, serta literasi digital untuk meningkatkan kewaspadaan masyarakat. Pencegahan masih berkarakter *reactive-preventive*, yakni dilakukan setelah muncul tren kasus atau laporan masyarakat. Sistem deteksi dini belum sepenuhnya terintegrasi secara nasional, dan koordinasi lintas lembaga sering bersifat sektoral.

Sebaliknya, Singapura menunjukkan pendekatan pencegahan yang lebih sistemik dan proaktif. Singapore Police Force melalui Commercial Affairs Department (CAD) mengembangkan sistem pemantauan tren scam secara berkala, analisis pola transaksi mencurigakan, serta kampanye publik berbasis data aktual. Pencegahan tidak hanya dilakukan dalam bentuk edukasi, tetapi juga melalui intervensi dini terhadap aliran dana mencurigakan sebelum kerugian semakin besar.

Dengan demikian, perbedaan mendasar dalam aspek pencegahan terletak pada tingkat integrasi teknologi, kecepatan respons, dan model koordinasi lintas lembaga.

Dalam aspek pemidanaan, perbedaan juga terlihat dalam konsistensi, orientasi, dan efektivitas implementasi.

Di Indonesia, pemidanaan mengikuti prosedur KUHAP dengan diskresi hakim yang relatif luas. Ancaman pidana dalam KUHP dan UU ITE tergolong signifikan, namun dalam praktik terjadi variasi putusan antar wilayah. Proses pemidanaan sering memakan waktu panjang karena harus melalui tahapan formal yang ketat. Selain itu, pemulihan kerugian korban (asset recovery) belum selalu optimal akibat lambatnya pembekuan dana.

Di Singapura, pemidanaan cenderung lebih terstandarisasi dan konsisten. Sistem peradilan menekankan efek jera (deterrence) dengan kepastian hukuman yang tinggi. Proses pembekuan aset dilakukan secara cepat melalui koordinasi erat antara kepolisian dan otoritas keuangan, sehingga memperkuat efektivitas pemidanaan tidak hanya dalam menghukum pelaku, tetapi juga dalam memulihkan kerugian korban.

3) Faktor Hukum dan Kelembagaan yang mempengaruhi Perbedaan Pendekatan

Penelitian ini menemukan bahwa perbedaan pendekatan antara Kepolisian Negara Republik Indonesia dan Singapore Police Force dalam menangani penipuan online tidak semata-mata disebabkan oleh perbedaan kapasitas teknologi atau sumber daya, melainkan terutama dipengaruhi oleh faktor hukum dan desain kelembagaan masing-masing negara.

Dari aspek hukum, Indonesia mendasarkan penanganan penipuan online pada kombinasi norma dalam Kitab Undang-Undang Hukum Pidana dan rezim khusus seperti Undang-Undang Informasi dan Transaksi Elektronik.

DOI: https://doi.org/10.31004/riggs.v5i1.7662

Namun, karakter regulasi ini masih bersifat sektoral dan tersebar, sehingga implementasinya sering kali memerlukan koordinasi lintas lembaga yang kompleks. Selain itu, mekanisme pembekuan rekening, pemblokiran akses digital, dan pelacakan lintas yurisdiksi kerap membutuhkan prosedur administratif yang relatif panjang.

Sebaliknya, Singapura mengatur penanganan penipuan online dalam kerangka hukum yang lebih terintegrasi, antara lain melalui Computer Misuse Act dan Penal Code, yang memberikan dasar hukum tegas bagi tindakan preventif maupun represif. Regulasi tersebut diperkuat dengan kewenangan administratif yang memungkinkan pembekuan dana dan intervensi cepat terhadap rekening mencurigakan tanpa prosedur birokrasi berlapis.

Dari sisi kelembagaan, Indonesia menganut struktur kepolisian yang luas dan terdesentralisasi, dengan pembagian kewenangan dari tingkat pusat hingga daerah. Sementara itu, Singapura memiliki struktur kepolisian yang relatif terpusat dan terintegrasi, sehingga alur komando, pengambilan keputusan, serta koordinasi lintas unit berlangsung lebih ringkas.

4. Kesimpulan

Meskipun kepolisian Indonesia dan Singapura memiliki mandat yang sama dalam melindungi masyarakat dari penipuan online, keduanya menerapkan strategi kewenangan yang berbeda secara fundamental Indonesia lebih menitikberatkan pada diskresi yang bersifat sosiologis-mediatif melalui mekanisme Restorative Justice guna mencapai pemulihan hubungan sosial, sementara Singapura menerapkan kewenangan yang bersifat teknokratis-proaktif melalui integrasi sistem Anti-Scam Centre yang memungkinkan intervensi teknis secara instan. Perbedaan ini mencerminkan bahwa kepolisian Indonesia masih mengedepankan prosedur koordinasi formal berbasis aturan tertulis (Civil Law), sedangkan kepolisian Singapura lebih mengandalkan efisiensi operasional dan kemandirian otoritas berbasis tradisi Common Law untuk memutus mata rantai kejahatan siber secara lebih lincah.Persamaan pendekatan kepolisian Indonesia dan Singapura terletak pada penggunaan hukum pidana sebagai instrumen utama dalam menindak penipuan online, dengan kepolisian sebagai garda terdepan dalam proses penyelidikan hingga pelimpahan perkara. Keduanya juga menerapkan upaya preventif melalui edukasi publik dan kerja sama dengan sektor keuangan serta teknologi.Perbedaannya, Indonesia masih cenderung bersifat reaktif dan berbasis laporan dengan koordinasi yang belum sepenuhnya real-time, sedangkan Singapura menerapkan pendekatan proaktif berbasis intelligence-led policing yang didukung analisis data, pemantauan transaksi, dan kolaborasi cepat lintas sektor. Perbedaan ini dipengaruhi oleh kesiapan institusional, literasi digital, dukungan teknologi, dan integrasi kebijakan pidana yang lebih kuat di Singapura.

Referensi

1. Kementrian Agama RI. 2014. *Al-qur'an dan terjemahnya*. Solo: Tiga Serangkai.
2. Arief, Barda Nawawi. 2010. ***Bunga Rampai Kebijakan Hukum Pidana*.** Jakarta: Kencana Prenada Media Group.
3. ___. 2003. ***Kapita Selekta Hukum Pidana***. Bandung: Citra Aditya Bakti.
4. Budiyanto. 2025. ***Pengantar Cybercrime dalam Sistem Hukum Pidana di Indonesia*.** Banten: PT Sada Kurnia Pustaka.
5. Casey, E. 2011. ***Digital Evidence and Computer Crime: Forensic Science, Computers and the Internet.*** Academic Press.
6. Creswell. 2020. ***Qualitative Inquiry & Research Design***. edisi 2020.
7. Dempsey, John S., & Linda S. Forst. 2019***. Police Administration*. Belmont: Wadsworth Publishing.**
8. Djanggih, Hardianto. 2025. ***KRIMINOLOGI*.** Makassar: PT. Nas media Indonesia.
9. Hamzah, Andi. 2008. ***Penegakan Hukum Lingkungan***. Jakarta: Sinar Grafika.
10. Hardjasoemantri, Koesnadi. 2006. ***Hukum Tata Lingkungan***. Yogyakarta: Gadjah Mada University Press.
11. Hasibuan, Edi Saputra. 2021. ***Hukum kepolisian dan criminal policy dalam penegakan hukum*.** PT. RajaGrafindo Persada-Rajawali Pers.
12. Hatta, Moh. 2009. ***Beberapa Masalah Penegakan Hukum Pidana umum dan Pidana Khusus*.** Yogyakarta: Liberty Cet.1.
13. Heinz Ealau & Kenneth Prewitt. 2017. dikutip dalam Solichin Abdul Wahab, ***Analisis Kebijaksanaan: Dari Formulasi ke Implementasi Kebijaksanaan Negara*.** Jakarta: Bumi Aksara.
14.
15. Hutabarat, Mario Valentino. 2024. ***Perlindungan Hukum terhadap Korban Tindak Pidana Phising Menurut Undang-Undang Nomor 19 Tahun 2016 tentang Perubahan atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik*.** Diss. FAKULTAS HUKUM, UNIVERSITAS ISLAM SUMATERA UTARA.
16. Kenedi, John. 2017. ***Buku Kebijakan Hukum Pidana (Penal Policy) Dalam Sistem Penegakan Hukum Di Indonesia***. Pustaka Pelajar.
17. Lawrence F. Travis. 2020. ***Introduction to Criminal Justice***. New York: Routledge.
18. M. Yahya Harahap. 2018. ***Pembahasan Permasalahan dan Penerapan KUHAP: Penyidikan dan Penuntutan*.** Jakarta: Sinar Grafika.
19. Mappaselleng, Nur Fadhilah. 2018. ***Rethinking Cyber Crime***. Arti Bumi Intaran, Yogyakarta. https://opac-library.unhas.ac.id/opac/detail-opac?id=68860
20. Maskun & Wiwik Meilarati. 2017. ***Aspek Hukum Penipuan Berbasis Internet*.** Keni Media.
21. McQuade, S. C. 2009. **Understanding & Managing Cybercrime**. Sage Publications.
22. Michael D. Reisig & John P. Crank. 2018. **Police Organization & Management.** Cincinnati: Anderson Publishing.
23. Moore, Mark H. 1995. **Creating Public Value: Strategic Management in Government**. Cambridge: Harvard University Press.

DOI: https://doi.org/10.31004/riggs.v5i1.7662

24. Muhtar, Sitti Murniati, M. Iqbal Sultan, & Muhammad Fitrah Ramadhan. 2023. **Penegakan Hukum dalam Tindak Pidana Penipuan Online**. Divya Media Pustaka.
25. Muladi & Barda Nawawi Arief. 1992. **Teori-Teori dan Kebijakan Pidana**. Bandung: Alumni.
26. Nafis, M Raihan. 2023. **Studi Perbandingan Hukum Tentang Pengaturan Tindak Pidana Cyberbullying di Indonesia, Singapura, Dan Malaysia.** Universitas Islam Negeri Sunan Ampel Fakultas Syariah dan Hukum Jurusan Hukum Publik Islam Program Studi Hukum Surabaya.
27. Napitupulu, Eben Jamin. 2024. **Kedudukan Kepolisian Negara Republik Indonesia Dalam Sistem Ketatanegaraan Indonesia.**
28. Nurdin, Boy. 2021. **Kedudukan dan fungsi hakim dalam penegakan hukum di Indonesia.** Bandung: Penerbit Alumni.
29. Nurhayati, et.al. 2024. **Buku Referensi Ekonomi Global 4.0.** Jambi: PT. Sonpedia Publishing Indonesia.
30. Qamar, Nurul & Farah Syah Rezah. 2017. **Etika Profesi Hukum.** Makassar: CV.Social Politic Genius. https://penerbitsign.com/single-buku/etika-profesi-hukum-empat-pilar-hukum
31. Qamar, Nurul, et.al. 2017. **Metode Penelitian Hukum. Makassar**: CV.Social Politic Genius.
32. Putri, Safira Diana. 2021. **Tugas dan fungsi kepolisian dalam perannya sebagai penegak hukum menurut Undang-Undang Nomor 2 Tahun 2002 tentang kepolisian.**
33. Raharjo, Satjipto. 2000. **Ilmu Hukum**. Bandung: PT. Citra Aditya Bakti.
34. Ravena, Dey. 2017. **Kebijakan Kriminal**: [Criminal Policy]. Jakarta: Prenada Media.
35. Rusmini, Andin. 2021. **Gambaran Kepolisian Republik Indonesia Dalam Sistem Penegakan Hukum di Indonesia**.
36. Shelley, L. I. 2014. **Dirty Entanglements: Corruption, Crime, & Terrorism**. Cambridge University Press.
37. Singapore Police Force. **SPF Annual Report 2023/2024.**
38. Soekanto. 2019. **Pengantar Penelitian Hukum**. edisi revisi 2019.
39. Soedarto. 1986. **Kapita Selekta Hukum Pidana.** Bandung: Alumni.
40. Sudarto. 1983. **Hukum Pidana dan Perkembangan** Masyarakat: Kajian Hukum Pidana di Indonesia. Bandung: Sinar Baru.
41. Sulubara, Seri Mughni, Virdyra Tasril, & Nurkhalisah. 2025. **Perlindungan Hukum Tindak Pidana Cybercrime dalam Cyberlaw di Indonesia.** Medan: Tahta Media Group.
42. Sunarno, Siswanto. 2008. **Hukum Pemerintah Daerah di Indonesia**. Jakarta: Sinar Grafika.
43. Supriyono. 2000. **Sistem Pengendalian Manajemen**. Edisi Pertama. Yogyakarta: BPFE.
44. Sutiyoso, Bambang. 2004. **Aktualita Hukum dalam Era Reformasi.** Jakarta: Grafindo Persada.
45. Teguh Prasetyo dan Abdul Halim Barkatullah. 2005. **Politik Hukum Pidana: Kajian Kebijakan Kriminalisasi dan Dekriminalisasi.** Yogyakarta: Pustaka Pelajar.
46. Wall, D. S. 2007. **Cybercrime: The Transformation of Crime in the Information Age. Polity Press.**
47. Zaidan, M. Ali. 2021. **Kebijakan kriminal.** Jakarta: Sinar Grafika (Bumi Aksara).
48. Jurnal
49. Afdhali, Dino Rizka & Taufiqurrohman Syahuri. 2023. **Idealitas Penegakkan Hukum Ditinjau Dari Perspektif Teori Tujuan Hukum.** Collegium Studiosum Journal 6.2: 555-561.
50. Al Kautsar, Izzy & Danang Wahyu Muhammad. 2022. **Sistem hukum modern Lawrance M. Friedman: Budaya hukum dan perubahan sosial masyarakat dari industrial ke digital.** Sapientia Et Virtus 7.2: 84-99.
51. Anakotta, Marthsian Y. 2019. **Kebijakan Sistem Penegakan Hukum Terhadap Penanggulangan Tindak Pidana Terorisme Melalui Pendekatan Integral.** Jurnal Belo 5.1: 46-66.
52. Andasia, Junaidy, Roy Marthen Moonti & Ibrahim Ahmad. 2025. **Implementasi Fungsi Preventif dan Represif dalam Patroli Kepolisian di Tingkat Polsek.** Politika Progresif: Jurnal Hukum, Politik dan Humaniora 2.2: 327-343.
53. Arafat, Muhammad & Alexander Tito Enggar Wirasto. 2024. **Kebijakan kriminal dalam penanganan siber di era digital**: Studi kasus di Indonesia. Equality: Journal of Law and Justice 1.2: 220-241.
54. Aurelia, Angel. 2024. **Analisis Pengimplementasian "Asean Cyber Security Framework"** DI SINGAPURA TAHUN 2020. Journal of Social and Economics Research 6.1: 2168-2179.
55. Brantingham, P. J., & Faust, F. L. (1976). **A Conceptual Model of Crime Prevention.** *Crime & Delinquency*, 22(3), 284–296.
56. Cahyono, Soetardi Tri, Wina Erni, & Taufik Hidayat. 2025. **Rikonstruksi Hukum Pidana Terhadap Kejahatan Siber (Cyber Crime) Dalam Sistem Peradilan Pidana Indonesia: Rekonstruksi Hukum Pidana terhadap Kejahatan Siber (Cyber Crime) dalam Sistem Peradilan Pidana Indonesia**. Dame Journal of Law 1.1.
57. Devianty, Farah Gitty. 2017. **Peran Kepolisian Sektor Gedebage Bandung dalam Rangka Memelihara Kamtibmas dan Penegakan Hukum Berdasarkan Undang-Undang Nomor 2 Tahun 2002 Tentang Kepolisian Negara Republik Indonesia.** Wacana Paramarta: Jurnal Ilmu Hukum 16.1: 47-66.
58. Dodi Syahputra. 2021. **Implementasi Kebijakan Kriminal dalam Penanggulangan Kejahatan di Indonesia.** Jurnal Pembangunan Hukum Indonesia 3.2: 180.
59. Edi Setiadi & B. Arief Sidharta. 2018. **Hukum Kepolisian di Indonesia.** Bandung: Refika Aditama.
60. Faisal, Nurhalisa, Aan Aswari, & Muhammad Azham Ilham. 2025. **Penegakan Hukum Terhadap Eksistensi Tindak Pidana Pemalsuan Identitas di Era Digital.** Jurnal LEGAL DIALOGICA 1.1.
61. Fuah, Marfuah. 2024. **Efektivitas Dan Fungsi Hukum Dalam Masyarakat Perspektif Filsafat Hukum**. Desiderata Law Review 1.2: 35-44.
62. Ginting, Yuni Priskila, et al. 2024. **Sosialisasi Perbandingan Hukum Pidana: Tindak Pidana ITE di Indonesia dan Singapura**. Jurnal Pengabdian West Science 3.04: 429-442.
63. Goldstein, H. (1990). ***Problem-Oriented Policing***. Temple University Press.
64. Indrawan, Jerry & Azila Zahira. 2024. **Revolutions in Military Affairs (RMA) Policy in Countering the Threat of Terrorism and Cyber Crime in Singapore.** Mandala: Jurnal Ilmu Hubungan Internasional 7.1: 18-39.
65. Ismanto, Dedi, Ivan Najjar Alavi, & Fauziah Lubis. 2024. **Kebijakan Hukum Pidana/Penal Policy.** Innovative: Journal Of Social Science Research 4.4: 16351-16361.
66. Kharisma, Dian, Ni Luh Putu Erika Swandiani, & Andi Nur Azizah Ardan Paliwang. 2025. **The Role of Interpol in Addressing Transnational Cybercrime: A Review of Global Law Enforcement Collaboration in Southeast Asia.** Perkara: Jurnal Ilmu Hukum dan Politik 3.2: 860-875.
67. Masdi, Andi Syawal, Syamsul Alam, & Rustan. 2025. **Upaya Hukum Dalam Penanggulangan Tindak Pidana Penipuan Daring Oleh Kepolisian.** Jurnal Legal Dialogica 1.1. https://jurnal.fh.umi.ac.id/index.php/legal/article/view/1468
68. Muhammad Taufik Rusyd. 2025. **Perbandingan Hukum Siber Indonesia dengan Negara ASEAN: Suatu Kajian Normatif.** Universitas Surakarta Jurnal Kolaboratif Sains 8.1: 40-48.

DOI: https://doi.org/10.31004/riggs.v5i1.7662

69. Qamar, Nurul. 2023. **Posisi Strategis Legislasi dalam Rantai Kebijakan Kriminal: Analisis Kebijakan Hukum Pidana Baru**. Jurnal Hukum Pidana Kontemporer 7.1: 45. https://books.google.co.id/books?hl=en&lr=&id=TAQHEAAAQBAJ&oi=fnd&pg=PA1&dq=info:FgCQbPV_plMJ:scholar.google.com&ots=hW4vVueGy5&sig=754NCzMCTAf7y5SkRw8bZ7hdw7I&redir_esc=y#v=onepage&q&f=false
70. Rahakbauw, Isro'Kurniawan, & Ika Arini Batubara. 2024. **Analisis Potensi Ancaman Siber pada Bidang Ekonomi di Indonesia.** Jurnal Kajian Stratejik Ketahanan Nasional 7.1.
71. Setiawan, Dian Alan. 2024. **Strategi Penanggulangan Kejahatan Ekonomi Berbasis Teknologi: Studi Komparatif Antara Indonesia, Amerika, Dan Eropa**. Masalah-Masalah Hukum 53.1: 79-90.
72. Suharyadi, Said Sampara, dan Kamri Ahmad. 2020. **Kejahatan Dunia Maya (Cyber Crime) Dalam Prespektif Hukum Islam.** Journal of Lex Generalis (JLG) 1.5: 102.
73. Wahid, Abdul. 2023. **Policy Formulation of Fraud Offenses in the New Penal Code Concept for Combating Technology-Related Crimes**. Rechtsidee 11.2: 10-21070.
74. Zweigert, K., & Kötz, H. (1998). ***Introduction to Comparative Law* (3rd ed.).** Oxford University Press. (Karya klasik yang meletakkan dasar metodologi dan fungsi utama perbandingan hukum).
75. Undang-Undang Republik Indonesia Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik, sebagaimana telah diubah dengan Undang-Undang Nomor 19 Tahun 2016 tentang Perubahan atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik.
76. Undang-Undang Republik Indonesia Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi.
77. Undang-Undang Republik Indonesia Nomor 1 Tahun 2024 tentang Perubahan Kedua atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik.
78. Computer Misuse Act (Singapura, Bab 50A, Edisi Revisi 2007).
79. Cybersecurity Act (Singapura, Undang-Undang No. 9 Tahun 2018).
80. Arief, Teuku Muhammad Valdy. 2025. Penipuan Online Rugikan Warga Rp 3,2 Triliun, OJK: Sudah Memprihatinkan. Kompas.com, diakses 26 November2025 (https://money.kompas.com/read/2025/06/26/191154226/penipuan-online-rugikan-warga-rp-32-triliun-ojk-sudah-memprihatinkan.).
81. Kominfo RI. 2023. **Laporan Keamanan Siber**.
82. Surah An--Nisa' Ayat 4 Arab, Latin, Terjemahan dan Tafsir | Baca di TafsirWeb. diakses 26 November 2025.
UNODC. 2021. Global Cybercrime Report.

DOI: https://doi.org/10.31004/riggs.v5i1.7662