

Kebijakan Hukum Pidana atas Hoax dan Disinformasi Berbasis Proxy Asing di Indonesia

Okki Prasetyo Raharjo^{1*}, Kuswandi², & I Ketut Adi Purnama³

^{1,2,3}Magister Ilmu Hukum, Universitas Suryakencana, Jawa Barat, Indonesia


*Email Korespondensi: okkiprasetyoraharjo@gmail.com

| HISTORI ARTIKEL | Abstrak |
|---|--|
| <p>Submit/Naksah Diterima: 2025-12-23</p> <p>Disetujui untuk Reviuw: 2025-12-25</p> <p>Proses Reviuw: 2025-12-25</p> <p>Revisi oleh Penulis: 2026-03-05</p> <p>Dinyatakan Layak Terbit: 2026-03-30</p> <p>Diterbitkan: 2026-03-31</p> | <p>Era digital telah mengubah paradigma komunikasi dan penyebaran informasi secara fundamental. Kemudahan akses internet dan media sosial membawa dampak negatif berupa maraknya penyebaran hoax dan disinformasi. Hoax dan disinformasi bukan sekadar permasalahan teknis komunikasi, melainkan telah berkembang menjadi ancaman serius terhadap keamanan nasional. Kompleksitas permasalahan semakin meningkat dengan adanya penggunaan jaringan proxy asing. Penelitian ini merupakan penelitian hukum normatif. Pendekatan yang digunakan meliputi pendekatan perundang-undangan (<i>statute approach</i>), pendekatan konseptual (<i>conceptual approach</i>), serta pendekatan perbandingan (<i>comparative approach</i>). Hasil penelitian menunjukkan bahwa pengaturan hukum pidana Indonesia terhadap penyebaran hoax dan disinformasi melalui jaringan proxy asing masih belum memadai. Kemudian, terdapat kendala yuridis dalam proses penegakan hukum berupa keterbatasan yurisdiksi ekstrateritorial dan ketidakjelasan unsur delik, kendala teknis terkait kapasitas digital forensik dan kompleksitas</p> |

¹ **Penulis pertama** berperan sebagai kontributor utama dalam penelitian dan penulisan artikel. Kontribusinya meliputi perumusan ide dan fokus penelitian, penyusunan latar belakang dan rumusan masalah, pengumpulan serta pengolahan bahan hukum primer dan sekunder, analisis yuridis terhadap pengaturan penyebaran hoax dan disinformasi melalui jaringan proxy asing dalam perspektif kejahatan terhadap keamanan negara, serta penulisan draf awal artikel hingga penyusunan kesimpulan dan rekomendasi penelitian.

² **Penulis kedua** memberikan kontribusi akademik substantif melalui penguatan kerangka konseptual dan metodologis penelitian, khususnya dalam pendekatan hukum pidana dan keamanan negara. Penulis kedua juga berperan dalam melakukan penelaahan kritis terhadap argumentasi hukum, memperdalam analisis normatif terhadap KUHP, UU ITE, dan regulasi terkait, serta memberikan masukan ilmiah dalam proses revisi dan penyempurnaan substansi artikel agar memenuhi standar kualitas akademik dan kelayakan publikasi jurnal ilmiah.

³ **Penulis ketiga** berkontribusi dalam validasi akademik dan penajaman analisis hasil penelitian, khususnya terkait konsep fungsionalisasi hukum pidana, yurisdiksi ekstrateritorial, dan tantangan penegakan hukum terhadap kejahatan siber yang mengancam keamanan negara. Selain itu, penulis ketiga berperan dalam penelaahan akhir naskah, memastikan konsistensi sistematika penulisan, ketepatan penggunaan teori dan konsep hukum pidana, serta kesesuaian artikel dengan kaidah penulisan ilmiah jurnal.

| | |
|--|--|
|  Lisensi: Creative Commons Attribution 4.0 International (CC BY 4.0) | enkripsi, kendala kelembagaan akibat fragmentasi kewenangan, serta hambatan kerja sama internasional. |
| | Kata Kunci: Disinformasi; Hoax; Hukum Pidana; Proxy Asing. |
| | <p style="text-align: center;">Abstract</p> <p><i>The digital era has fundamentally changed the paradigm of communication and information dissemination. Easy access to the internet and social media has had a negative impact in the form of the rampant spread of hoaxes and disinformation. Hoaxes and disinformation are not merely technical communication problems, but have developed into a serious threat to national security. The complexity of the problem is further exacerbated by the use of foreign proxy networks. This research is normative legal research. The approaches used include the statute approach, the conceptual approach, and the comparative approach. The results of the study show that Indonesian criminal law regulations on the spread of hoaxes and disinformation through foreign proxy networks are still inadequate. Furthermore, there are juridical obstacles in the law enforcement process in the form of limited extraterritorial jurisdiction and unclear elements of crime, technical obstacles related to digital forensics capacity and the complexity of encryption, institutional obstacles due to fragmentation of authority, and obstacles to international cooperation.</i></p> <p>Keywords: Criminal Law; Disinformation; Foreign Proxies; Hoaxes.</p> |

A. PENDAHULUAN

Era digital telah mengubah paradigma komunikasi dan penyebaran informasi secara fundamental. Kemudahan akses internet dan media sosial memberikan ruang yang sangat luas bagi setiap individu untuk menyebarkan informasi tanpa batas geografis dan temporal. Namun, kemudahan ini juga membawa dampak negatif berupa maraknya penyebaran hoax dan disinformasi yang dapat mengancam stabilitas sosial, politik, dan keamanan Negara (Shao et al., 2018).

Hoax dan disinformasi bukan sekadar permasalahan teknis komunikasi, melainkan telah berkembang menjadi ancaman serius terhadap keamanan nasional. Berbagai penelitian menunjukkan bahwa penyebaran informasi palsu dapat memicu konflik sosial, merusak kepercayaan publik terhadap institusi negara, mengintervensi proses demokrasi, bahkan dapat digunakan sebagai instrumen

perang informasi oleh aktor-aktor asing untuk melemahkan kedaulatan negara (Aziz, 2025; Brennen et al., 2020; Nurdin & Nugraha, 2025; Suriadi Hari, 2025).

Kompleksitas permasalahan semakin meningkat dengan adanya penggunaan jaringan proxy asing dalam penyebaran hoax dan disinformasi. Proxy merupakan teknologi yang memungkinkan pengguna untuk menyembunyikan identitas dan lokasi sebenarnya dengan menggunakan server perantara yang berlokasi di negara lain. Teknologi ini sering disalahgunakan oleh pelaku tindak pidana siber untuk menghindari deteksi dan penindakan hukum, serta mempersulit proses penyidikan karena jejak digital yang terputus atau tertutup oleh infrastruktur asing.

Fenomena penggunaan proxy asing dalam penyebaran hoax dan disinformasi menunjukkan adanya dimensi transnasional dalam kejahatan siber yang mengancam keamanan negara. Hal ini memunculkan pertanyaan mendasar tentang efektivitas hukum pidana Indonesia dalam menanggulangi ancaman tersebut dan kendala dalam pelaksanaan penegakan hukumnya.

Berbagai penelitian menunjukkan bahwa hoax dan disinformasi tidak lagi sekadar persoalan etika komunikasi, melainkan telah berkembang menjadi ancaman strategis. Studi mengenai *information disorder* (Wardle & Derakhshan, 2017) menekankan kompleksitas bentuk disinformasi dalam ekosistem digital. Penelitian lain (Vosoughi, 2018) membuktikan bahwa informasi palsu menyebar lebih cepat dibandingkan informasi benar di media sosial.

Dalam konteks keamanan negara, hoax dan disinformasi dapat menjadi instrumen *warfare* informasi (*information warfare*) yang digunakan untuk mencapai tujuan politik tertentu, seperti melemahkan legitimasi pemerintah, memecah belah masyarakat, atau mengintervensi proses demokrasi. Beberapa negara bahkan telah mengembangkan kemampuan operasi informasi (*information operations*) sebagai bagian dari strategi pertahanan dan keamanan nasional (Brennen et al., 2020).

Penggunaan proxy memiliki berbagai fungsi legitimate, seperti meningkatkan keamanan jaringan, mengoptimalkan kecepatan akses, melakukan

filtering konten, atau mengakses konten yang dibatasi secara geografis (geo-blocking). Namun, teknologi ini juga dapat disalahgunakan untuk tujuan kejahatan, termasuk penyebaran hoax dan disinformasi. Pelaku kejahatan siber sering menggunakan proxy asing dengan berbagai alasan diantaranya menghindari deteksi oleh aparat penegak hukum Indonesia, mempersulit proses penyidikan karena keterbatasan yurisdiksi, menyembunyikan identitas sebenarnya, dan menciptakan ilusi bahwa konten berasal dari luar negeri untuk menghindari regulasi domestik (BSSN, 2020). Dalam perkembangannya, teknologi proxy telah berkembang menjadi lebih kompleks dengan munculnya *Virtual Private Network* (VPN), *The Onion Router* (TOR), dan *proxy chain* yang menggunakan *multiple proxy servers* secara berlapis. Teknologi-teknologi ini membuat pelacakan jejak digital menjadi sangat sulit atau bahkan tidak mungkin dilakukan tanpa kerjasama internasional.

Penyebaran hoax dan disinformasi dapat dikategorikan sebagai ancaman terhadap keamanan negara dalam dimensi politik dan sosial. Secara politik, disinformasi dapat merusak legitimasi pemerintah, mengintervensi proses demokrasi, dan melemahkan kohesi sosial. Secara sosial, hoax dapat memicu konflik horizontal, disintegrasi bangsa, dan erosi kepercayaan publik terhadap institusi Negara (Persily, 2017).

Di Indonesia, kajian hukum umumnya berfokus pada penerapan Undang-Undang Nomor 19 Tahun 2016 tentang Perubahan atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE) dalam menjerat pelaku penyebaran hoax. Beberapa penelitian menyoroti problematika multitafsir norma, potensi *overcriminalization*, serta risiko pelanggaran kebebasan berekspresi. Namun demikian, kajian-kajian tersebut masih terbatas pada aspek normatif penerapan pasal-pasal tertentu dan belum secara komprehensif menganalisis dimensi transnasional penyebaran hoax melalui penggunaan jaringan proxy asing.

Padaahal, perkembangan modus operandi menunjukkan bahwa pelaku penyebaran hoax dan disinformasi semakin memanfaatkan teknologi penyamaran

identitas seperti proxy server, Virtual Private Network (VPN), dan jaringan anonim seperti TOR. Penggunaan proxy asing menciptakan hambatan serius dalam proses pelacakan digital, memperumit pembuktian, serta menimbulkan persoalan yurisdiksi lintas negara. Dimensi ini belum banyak dibahas dalam penelitian hukum pidana Indonesia, khususnya dalam kaitannya dengan konsep kejahatan terhadap keamanan negara sebagaimana diatur dalam Bab I Buku II KUHP.

Disisi lain, kebebasan berekspresi merupakan hak fundamental yang dijamin oleh konstitusi dan instrumen hak asasi manusia internasional. Pasal 28E ayat (3) UUD 1945 menjamin setiap orang berhak atas kebebasan berserikat, berkumpul, dan mengeluarkan pendapat. Namun, kebebasan ini bukan tanpa batas. Pasal 28J ayat (2) UUD 1945 menegaskan bahwa dalam menjalankan hak dan kebebasannya, setiap orang wajib tunduk kepada pembatasan yang ditetapkan dengan undang-undang dengan maksud semata-mata untuk menjamin pengakuan serta penghormatan atas hak dan kebebasan orang lain dan untuk memenuhi tuntutan yang adil sesuai dengan pertimbangan moral, nilai-nilai agama, keamanan, dan ketertiban umum dalam suatu masyarakat demokratis. Menurut konteks internasional, Article 19 *International Covenant on Civil and Political Rights* (ICCPR) mengatur bahwa kebebasan berekspresi dapat dibatasi untuk menghormati hak atau reputasi orang lain, melindungi keamanan nasional, ketertiban umum, kesehatan atau moral publik. Prinsip pembatasan ini harus memenuhi syarat-syarat: diatur dalam hukum (*prescribed by law*), memiliki tujuan legitimate, dan proporsional (*necessary in a democratic society*) (Nations, 1966).

Tantangan dalam penanggulangan hoax dan disinformasi adalah menemukan keseimbangan yang tepat antara perlindungan keamanan negara dengan penghormatan terhadap kebebasan berekspresi. Pengaturan yang terlalu luas dan ambigu dapat menimbulkan *chilling effect* terhadap kebebasan berekspresi dan berpotensi disalahgunakan untuk membungkam kritik dan oposisi politik.

Oleh sebab itu, penelitian ini akan membahas mengenai bagaimana pengaturan hukum pidana Indonesia terhadap penyebaran hoax dan disinformasi melalui jaringan proxy asing sebagai kejahatan terhadap keamanan negara,

bagaimana kendala dalam penegakan hukum pidana terhadap hoax dan disinformasi, serta bagaimana fungsionalisasi hukum dapat dioptimalkan untuk menanggulangi penyebaran hoax dan disinformasi yang bersifat transnasional, dengan tetap menjamin perlindungan hak kebebasan berekspresi

B. METODE PENELITIAN

Penelitian ini merupakan penelitian hukum normative (*normative legal research*) yang mengkaji hukum sebagai norma (*das sollen*). Pendekatan yang digunakan meliputi pendekatan perundang-undangan (*statute approach*) untuk menelaah ketentuan terkait penyebaran hoaks, disinformasi, dan kejahatan terhadap keamanan negara; pendekatan konseptual (*conceptual approach*) untuk menganalisis doktrin serta teori hukum pidana dan hukum teknologi informasi; serta pendekatan perbandingan (*comparative approach*) secara terbatas untuk membandingkan pengaturan hukum di beberapa negara dalam penanggulangan hoaks dan disinformasi (Irwansyah, 2021). Bahan hukum yang digunakan terdiri atas bahan hukum primer, antara lain Kitab Undang-Undang Hukum Pidana (KUHP), Undang-Undang Informasi dan Transaksi Elektronik (UU ITE), dan Undang-Undang Intelijen Negara; bahan hukum sekunder berupa buku, jurnal ilmiah, dan hasil penelitian terdahulu yang relevan; serta bahan hukum tersier seperti kamus hukum dan media massa. Pengumpulan bahan hukum dilakukan melalui studi kepustakaan. Analisis dilakukan secara kualitatif dengan teknik interpretasi sistematis, gramatikal, dan teleologis, disertai argumentasi hukum serta analisis sinkronisasi dan harmonisasi peraturan perundang-undangan untuk memperoleh kesimpulan dan rekomendasi yang komprehensif.

C. HASIL DAN PEMBAHASAN

1. Pengaturan Hukum Pidana Indonesia Terhadap Penyebaran Hoax dan Disinformasi Melalui Jaringan Proxy Asing

Permasalahan utama dalam penelitian ini terletak pada pertanyaan apakah sistem hukum pidana Indonesia saat ini telah memadai dalam menjangkau

penyebaran hoax dan disinformasi yang dilakukan melalui jaringan proxy asing, serta bagaimana model reformulasi norma yang selaras dengan standar pembatasan hak asasi manusia. Pertanyaan ini menjadi relevan karena perkembangan modus operandi kejahatan siber menunjukkan adanya penggunaan teknologi penyamaran identitas digital lintas yurisdiksi untuk menghindari penegakan hukum nasional.

Pengaturan mengenai berita bohong dan disinformasi dalam hukum pidana Indonesia tersebar dalam berbagai regulasi, yaitu KUHP, Undang-Undang Nomor 1 Tahun 1946, serta Undang-Undang Informasi dan Transaksi Elektronik (UU ITE). Namun, peraturan yang terpisah-pisah justru membuat aturan hukumnya tidak selaras satu sama lain dan keterbatasan daya jangkau terhadap cara-cara kejahatan baru yang menggunakan teknologi penyamaran identitas (anonimitas).

Kitab Undang-Undang Hukum Pidana (KUHP) sebagai induk peraturan hukum pidana Indonesia mengatur beberapa ketentuan yang relevan dengan penyebaran hoax dan disinformasi, khususnya dalam konteks kejahatan terhadap keamanan negara security (Arief, 2016). Dalam Undang-Undang Nomor 1 Tahun 2023 (KUHP) terdapat pasal tentang penyiaran atau penyebarluasan berita/pemberitahuan bohong yang mengakibatkan kerusuhan dalam masyarakat, sebagaimana diatur dalam Pasal 263 dan Pasal 264 yang mengatur mengenai penyiaran atau penyebarluaskan berita atau pemberitahuan padahal patut diduga atau diketahuinya bahwa berita atau pemberitahuan tersebut bohong yang mengakibatkan kerusuhan dalam masyarakat (Auli, 2024).

Sedangkan, menurut Pasal 264, setiap orang yang menyiarkan berita yang tidak pasti, berlebih-lebihan, atau yang tidak lengkap sedangkan diketahuinya atau patut diduga, bahwa berita demikian dapat mengakibatkan kerusuhan di masyarakat, dipidana dengan pidana penjara paling lama 2 tahun atau pidana denda paling banyak kategori III, yaitu Rp50 juta (Auli, 2024).

Unsur delik hoax menitikberatkan pada adanya kesengajaan perbuatan penyebaran Informasi palsu atau menyesatkan serta potensi menimbulkan keresahan atau kerugian bagi masyarakat (Alaini, 2026). Secara teori hukum

pidana, konstruksi ini menunjukkan bahwa delik tersebut merupakan delik materiil yang mensyaratkan akibat nyata. Permasalahan muncul ketika penyebaran dilakukan melalui jaringan proxy asing, karena pembuktian unsur “menyiarkan” dan “kesengajaan” menjadi kompleks. Identitas pelaku tersamarkan, lokasi perbuatan tidak berada secara fisik dalam yurisdiksi Indonesia, dan akibatnya seringkali bersifat digital serta terdistribusi (Wadjo et al., 2025).

Mahkamah Konstitusi dalam Putusan Mahkamah Konstitusi Nomor 76/PUU-XV/2017, ketiadaan berbagai penjelasan yang memadai atas unsur-unsur tindak pidana Pasal 28 ayat (2) tersebut menjadikan ketentuan ini sebagai pasal yang cukup kontroversial dan eksekutif ketika diterapkan. Berbagai ekspresi yang dianggap merupakan kritik, misalnya pernyataan Jerinx dan laporan jurnalistik, dapat dengan mudah dijerat dengan tuduhan menimbulkan rasa kebencian. Penafsiran unsur-unsur tindak pidana Pasal 28 ayat (2) ini kemudian tidak konsisten dan minim rujukan jelas dan pasti (Arianto et al., 2026).

Putusan tersebut menegaskan pentingnya penafsiran ketat terhadap norma pidana guna mencegah kriminalisasi berlebihan. Penegasan tersebut menunjukkan bahwa perluasan interpretasi terhadap norma lama untuk menjangkau modus proxy asing berpotensi bertentangan dengan asas legalitas, khususnya prinsip *lex certa*. Dengan demikian, permasalahan bukan sekadar kurangnya norma, melainkan ketidakmampuan konstruksi delik yang ada untuk menjangkau teknik penyamaran digital lintas negara.

UU ITE sebagai *lex specialis* memang memperluas cakupan hukum pidana ke ranah elektronik. Pasal 28 ayat (2) mengatur penyebaran informasi yang menimbulkan kebencian berdasarkan SARA, sementara Pasal 2 mengatur yurisdiksi ekstrateritorial apabila perbuatan tersebut menimbulkan akibat hukum di Indonesia (Oktabiantoro & Wulan, 2024). Namun demikian, norma tersebut tidak secara eksplisit mengatur penggunaan sarana penyamaran identitas digital sebagai bagian dari unsur delik ataupun sebagai faktor pemberatan pidana.

Putusan Mahkamah Konstitusi Nomor 50/PUU-VI/2008, Mahkamah menegaskan bahwa pembatasan terhadap kebebasan berekspresi harus memenuhi

prinsip kehati-hatian dan tidak boleh bersifat multitafsir (Putra & Wisnubroto, 2013). Oleh karena itu, kriminalisasi terhadap penggunaan proxy atau VPN secara umum tanpa pembatasan yang jelas berpotensi melanggar asas proporsionalitas dan mengancam kebebasan berekspresi yang dijamin konstitusi.

Apabila dianalisis melalui teori pertanggungjawaban pidana, penggunaan proxy asing bukanlah inti perbuatan melawan hukum, melainkan sarana untuk menghindari identifikasi dan yurisdiksi (Sukmareni et al., 2026). Oleh sebab itu, pendekatan yang lebih tepat bukanlah mengkriminalisasi teknologi tersebut secara umum, melainkan mengintegrasikannya sebagai unsur pemberat dalam konteks adanya kesengajaan menyebarkan informasi palsu yang mengancam keamanan negara.

Untuk mengatasi problem tersebut, penelitian ini menawarkan model reformulasi norma yang tidak sekadar memperluas kriminalisasi, tetapi dirancang memenuhi asas legalitas dan proporsionalitas. Rumusan delik yang diusulkan mensyaratkan: (1) adanya penyebaran informasi yang diketahui palsu; (2) dilakukan dengan sengaja; (3) menggunakan sarana penyamaran identitas digital lintas yurisdiksi; dan (4) menimbulkan atau berpotensi menimbulkan gangguan terhadap keamanan negara. Unsur penyamaran digital tidak berdiri sendiri, melainkan terikat pada pembuktian *mens rea* dan tujuan destabilisasi.

Aturan lainnya juga terlihat dalam UU Intelijen Negara dan UU Pertahanan Negara. Kedua undang-undang ini memang mengakui adanya ancaman non-militer seperti perang informasi, tetapi tidak menyediakan aturan pidana yang jelas dan bisa langsung diterapkan. Akibatnya, muncul kekosongan pengaturan khusus terhadap penyebaran disinformasi yang menggunakan penyamaran identitas lintas negara dan dapat mengancam keamanan negara.

Usulan norma tersebut diuji dengan empat prinsip pembatasan HAM: *legality*, *legitimate aim*, *necessity*, dan *proportionality*. Rumusannya harus jelas dan tidak multitafsir (*legality*), bertujuan melindungi keamanan nasional yang sah menurut hukum internasional (*legitimate aim*), hanya diterapkan pada ancaman serius terhadap stabilitas negara (*necessity*), dan pemberatan pidana dibatasi pada

kondisi terorganisir atau melibatkan dukungan pihak asing (*proportionality*) (Rizkia et al., 2025).

Maka, pada perumusan model delik yang secara khusus mengatur penyamaran identitas digital lintas yurisdiksi dengan mengintegrasikan unsur perbuatan, kesengajaan, dan uji pembatasan HAM dalam satu analisis. Dengan demikian, penelitian ini tidak hanya menunjukkan adanya kekosongan hukum, tetapi juga menawarkan rumusan norma yang lebih tepat dan selaras dengan prinsip konstitusional.

2. Kendala Penegakan Hukum Pidana terhadap Penyebaran Hoaks melalui Penggunaan Proxy Asing

Penegakan hukum pidana terhadap penyebaran hoaks yang dilakukan melalui penggunaan proxy asing menghadapi problem yang tidak semata-mata teknis, melainkan bersifat struktural, normatif, dan transnasional (Firganefi & Diska Nabila, 2024). Permasalahan ini menjadi relevan karena meskipun Indonesia telah memiliki instrumen hukum seperti KUHP dan UU ITE yang mengatur penyebaran informasi bohong, efektivitasnya dalam konteks kejahatan siber lintas batas negara masih menunjukkan celah yang signifikan. Oleh karena itu, analisis terhadap kendala penegakan hukum harus diletakkan dalam kerangka uji unsur delik, asas legalitas, efektivitas pembuktian, serta prinsip pembatasan hak asasi manusia.

Persoalan pertama terletak pada problem yurisdiksi. Pasal 2 UU ITE mengadopsi prinsip ekstrateritorialitas, yang secara normatif memungkinkan hukum Indonesia diberlakukan terhadap perbuatan yang memiliki akibat hukum di wilayah Indonesia meskipun dilakukan dari luar negeri (Wildanah & Rivai, 2025). Namun, secara praktis, keberlakuan tersebut hanya mencerminkan kewenangan membuat norma, bukan kewenangan menegakkan norma. Ketika pelaku berada di luar negeri dan menggunakan infrastruktur server asing, penegakan hukum Indonesia tidak memiliki kewenangan langsung untuk melakukan penangkapan atau penyitaan barang bukti. Kondisi ini menciptakan enforcement gap antara norma dan implementasinya (Rahmad & Anggita, 2025).

Masalah yurisdiksi tersebut semakin kompleks apabila diuji dalam konteks unsur delik, beberapa ketentuan dalam KUHP dan UU ITE menggunakan frasa yang tidak jelas dan multitafsir, seperti "menimbulkan keonaran" atau "kebencian berdasarkan SARA". Ketidakjelasan ini dapat menimbulkan ketidakpastian hukum dan berpotensi disalahgunakan untuk kriminalisasi terhadap kritik atau pendapat yang sah.

Dalam tindak pidana penyebaran hoaks, unsur *actus reus* berupa "menyebarkan informasi" relatif mudah dibuktikan ketika konten digital tersedia. Akan tetapi, dalam praktik penggunaan proxy chain, VPN berlapis, atau jaringan anonimisasi, keterkaitan antara pelaku dan perbuatan menjadi tidak linear (Candra & Dinata, 2025). Identitas digital dapat dimanipulasi melalui *spoofing* atau penggunaan akun anonim, sehingga pembuktian hubungan kausal antara subjek hukum dan konten menjadi sangat bergantung pada kemampuan digital forensik.

Selain problem kejelasan norma, terdapat pula konflik normatif antar regulasi. Pengaturan mengenai penyebaran berita bohong tersebar dalam KUHP, UU ITE, serta peraturan lain yang memiliki *threshold* pembuktian berbeda. Perbedaan ini berpotensi menimbulkan inkonsistensi penerapan hukum. Secara teori, kondisi tersebut bertentangan dengan asas kepastian hukum dan prinsip *lex specialis derogat legi generali* apabila tidak diterapkan secara konsisten. Perbedaan dan tumpang tindih antar aturan membuat sistem hukum pidana menjadi tidak selaras dan kurang efektif dalam menangani kejahatan siber (Purnomo & M, 2021).

Pada tataran teknis, kendala pembuktian menjadi hambatan utama. Sistem pembuktian dalam KUHP masih berorientasi pada alat bukti konvensional, sementara pembuktian digital memerlukan standar khusus seperti integritas metadata, *hashing*, *forensic imaging*, serta *chain of custody digital*. Tanpa standar prosedural yang seragam dan terinstitusionalisasi, alat bukti digital rentan dipersoalkan secara formil di persidangan (Abbas, 2026). Selain itu, perkembangan teknologi enkripsi end-to-end dan sistem anonimisasi membuat intersepsi maupun pelacakan identitas pelaku semakin sulit dilakukan. Ketika teknologi berkembang lebih cepat daripada adaptasi regulasi, hukum berada dalam posisi reaktif dan

tertinggal (Indarta, 2025). Keterbatasan kapasitas digital forensik aparat penegak hukum Indonesia masih menghadapi keterbatasan dalam hal kapasitas dan peralatan digital forensik. Pelacakan pelaku yang menggunakan proxy chain, VPN berlapis, atau TOR network memerlukan keahlian khusus dan *tools* yang canggih. Banyak penyidik yang belum memiliki sertifikasi digital *forensic examiner* atau *computer hacking forensic investigator*.

Kendala tersebut diperparah oleh aspek kelembagaan. Penegakan hukum terhadap kejahatan siber melibatkan banyak institusi: Polri (khususnya Direktorat Tindak Pidana Siber Bareskrim), Kementerian Komunikasi dan Informatika, Badan Siber dan Sandi Negara (BSSN), Badan Intelijen Negara (BIN), dan lembaga lainnya. Fragmentasi kewenangan ini sering menimbulkan tumpang tindih atau justru kekosongan tanggung jawab (*grey area*) (Edmon, 2013). Dalam perspektif teori sistem hukum, efektivitas penegakan hukum tidak hanya ditentukan oleh substansi norma, tetapi juga struktur dan kultur hukum. Ketika koordinasi antar lembaga belum optimal, respons terhadap penyebaran hoaks yang bergerak sangat cepat di ruang digital menjadi tidak sebanding dengan laju distribusi informasi itu sendiri.

Lebih jauh lagi, kerja sama internasional menjadi faktor penentu dalam konteks kejahatan berbasis proxy asing. Ketiadaan Perjanjian *Mutual Legal Assistance* (MLA), Indonesia belum memiliki perjanjian bantuan hukum timbal balik dengan banyak negara yang menjadi lokasi server proxy yang sering digunakan pelaku (Yuwono et al., 2021). Proses permintaan bantuan hukum melalui jalur diplomatik memerlukan waktu yang sangat lama, sementara bukti digital dapat dengan mudah dihapus atau dimanipulasi. Perbedaan konsep hukum antara sistem *common law* dan *civil law*, serta perbedaan definisi delik antara negara, menimbulkan kesulitan dalam kerjasama penegakan hukum. Apa yang dianggap sebagai kejahatan di Indonesia belum tentu dikategorikan sebagai kejahatan di negara lain. Banyak negara menerapkan prinsip data *sovereignty* yang ketat, di mana data yang tersimpan di server mereka tidak dapat diakses oleh penegak hukum negara lain tanpa persetujuan otoritas setempat. Beberapa negara bahkan menolak memberikan data dengan alasan perlindungan privasi warga negaranya. Sehingga,

kerjasama internasional dalam penegakan hukum siber seringkali terkendala oleh pertimbangan politik dan kepentingan geopolitik.

Menurut sudut pandang hak asasi manusia, setiap kriminalisasi penyebaran hoaks harus diuji melalui *parameter legality, legitimate aim, necessity, dan proportionality*. Negara memang memiliki tujuan yang sah untuk melindungi ketertiban umum dan keamanan nasional. Namun, pembatasan terhadap kebebasan berekspresi harus dilakukan secara proporsional dan berbasis norma yang jelas. Jika rumusan delik terlalu luas dan tidak mensyaratkan adanya niat jahat yang nyata serta akibat konkret, maka pembatasan tersebut berpotensi melanggar prinsip proporsionalitas (Rizkia et al., 2025). Dengan demikian, perbaikan hukum tidak cukup dilakukan melalui peningkatan kapasitas teknis, tetapi juga melalui reformulasi norma delik yang lebih presisi dan terukur.

3. Fungsionalisasi Hukum Pidana yang Ideal dalam Penanggulangan Disinformasi melalui Proxy Asing

Fungsionalisasi hukum pidana terhadap penyebaran hoax dan disinformasi melalui jaringan proxy asing tidak cukup dipahami sebagai sekadar perluasan kriminalisasi. Permasalahan utamanya terletak pada kekosongan normatif, ketidakjelasan unsur delik, keterbatasan yurisdiksi, serta potensi benturan dengan perlindungan hak asasi manusia. Oleh karena itu, pembaruan hukum pidana harus dirumuskan secara sistematis dan konstitusional, dengan memastikan bahwa kriminalisasi benar-benar ditujukan untuk melindungi keamanan negara tanpa mengorbankan kebebasan berekspresi.

Secara normatif, pengaturan dalam Kitab Undang-Undang Hukum Pidana dan Undang-Undang Informasi dan Transaksi Elektronik (UU ITE) memang telah mengatur tindak pidana terkait informasi elektronik, namun belum secara spesifik mengantisipasi penggunaan teknologi penyamaran seperti proxy asing, VPN, atau jaringan anonimisasi. Ketentuan yang ada masih berorientasi pada delik konvensional dan belum membedakan secara tegas antara hoax, disinformasi terorganisir, kritik, satire, maupun ekspresi yang sah. Jika diuji melalui konstruksi

actus reus dan mens rea, tampak bahwa unsur akibat konkret terhadap keamanan negara serta pembuktian kesengajaan untuk menyesatkan belum dirumuskan secara eksplisit, sehingga berpotensi menimbulkan multitafsir dan *overcriminalization* (Alaini, 2026). Oleh sebab itu, diperlukan reformulasi ketentuan pidana yang secara spesifik mengkriminalisasi penyebaran hoax dan disinformasi melalui jaringan proxy asing yang mengancam keamanan negara.

Unsur-unsur delik harus dirumuskan secara jelas dan terukur untuk menghindari multitafsir, dengan kriteria:

- a. Definisi yang tegas tentang "hoax" dan "disinformasi" yang membedakannya dengan kritik, satire, atau ekspresi pendapat yang sah;
- b. Unsur kesengajaan (*mens rea*) yang jelas, yaitu pelaku mengetahui informasi tersebut palsu dan memiliki intensi untuk menyesatkan;
- c. Akibat yang ditimbulkan (*actus reus*) berupa ancaman nyata terhadap keamanan negara, bukan sekadar potensi abstrak;
- d. Penggunaan teknologi penyamaran (proxy, VPN, TOR) sebagai unsur yang memberatkan.

Selanjutnya, perlu ditambahkan delik khusus dalam revisi KUHP atau amandemen UU ITE yang mengatur:

- a. Tindak pidana *organized disinformation campaign* yang dilakukan secara sistematis dan terorganisir;
- b. Pengoperasian *bot farm* atau *sock puppet account* untuk amplifikasi hoax dan disinformasi;
- c. Penyediaan infrastruktur atau jasa yang secara khusus digunakan untuk memfasilitasi penyebaran hoax (seperti layanan proxy yang tidak kooperatif dengan penegak hukum)
- d. *Foreign information interference*, yaitu operasi informasi yang disponsori oleh aktor asing untuk mengintervensi kedaulatan negara.

Selain itu, hukum pidana harus disesuaikan dengan tingkat bahaya dan dampak yang ditimbulkan. Untuk hoax dan disinformasi yang mengancam

keamanan negara, ancaman pidana harus lebih berat dibandingkan dengan hoax biasa. Perlu dipertimbangkan:

- a. Pidana penjara minimal dan maksimal yang proporsional;
- b. Pidana denda yang disesuaikan dengan kemampuan ekonomi pelaku dan kerugian yang ditimbulkan;
- c. Pidana tambahan berupa pencabutan hak tertentu (misalnya hak untuk mengoperasikan platform digital);
- d. Pertanggungjawaban pidana korporasi bagi platform digital yang tidak kooperatif dalam mencegah penyebaran hoax.

Selain reformulasi delik, persoalan yurisdiksi ekstrateritorial juga menjadi isu krusial. Penyebaran disinformasi melalui proxy asing pada hakikatnya merupakan kejahatan lintas batas yang melampaui prinsip teritorialitas klasik. Oleh karena itu, hukum pidana Indonesia perlu mengoperasionalkan prinsip *effects doctrine* dan *protective principle* secara lebih tegas, sehingga yurisdiksi dapat didasarkan pada dampak nyata yang ditimbulkan di wilayah Indonesia, meskipun perbuatan dilakukan dari luar negeri. Namun penguatan yurisdiksi tidak akan efektif tanpa dukungan mekanisme kerja sama internasional. Ketidakterlibatan Indonesia secara penuh dalam rezim internasional seperti *Budapest Convention on Cybercrime* menyebabkan proses mutual legal assistance berjalan lambat dan tidak seragam (Wicaksana, 2022). Dalam konteks ini, penguatan instrumen perjanjian bilateral maupun multilateral menjadi bagian integral dari fungsionalisasi hukum pidana.

Lebih jauh, pendekatan represif harus diimbangi dengan pembangunan kapasitas kelembagaan. Penegakan hukum terhadap disinformasi berbasis teknologi penyamaran memerlukan kemampuan digital forensik yang memadai, infrastruktur laboratorium siber yang terstandar, serta integrasi data lintas lembaga. Tanpa modernisasi tersebut, perluasan norma pidana hanya akan menghasilkan hukum yang normatif di atas kertas tetapi lemah dalam implementasi. Oleh karena itu, pembentukan unit khusus yang bersifat multidisipliner menggabungkan keahlian hukum, teknologi informasi, dan intelijen

merupakan kebutuhan struktural, bukan sekadar pilihan kebijakan. Namun demikian, setiap upaya kriminalisasi dalam ruang digital harus tunduk pada pembatasan hak asasi manusia.

Pendekatan represif hukum pidana harus diimbangi dengan pendekatan preventif melalui: (MASTEL, 2021)

- a. Program literasi digital nasional untuk meningkatkan kemampuan masyarakat dalam mengidentifikasi hoax dan disinformasi;
- b. Kampanye publik tentang bahaya hoax dan cara memverifikasi informasi;
- c. Integrasi pendidikan literasi media dan digital dalam kurikulum pendidikan;
- d. Pemberdayaan komunitas *fact-checker* dan *citizen journalist*.

Kemudian, untuk mencegah penyalahgunaan kewenangan dan melindungi kebebasan berekspresi, maka diperlukan: (Nations, 1948)

- a. Penerapan *strict scrutiny test* dalam kriminalisasi konten online;
- b. Pembatasan penerapan ketentuan pidana hanya untuk kasus-kasus yang benar-benar mengancam keamanan negara, bukan sekadar kritik atau satire politik;
- c. Transparansi dalam proses penegakan hukum dengan publikasi statistik penanganan kasus;
- d. Mekanisme *judicial review* yang efektif terhadap tindakan penegak hukum.

Dengan demikian, fungsionalisasi hukum pidana yang ideal dalam konteks disinformasi melalui proxy asing bukan sekadar memperberat ancaman pidana, melainkan membangun desain normatif yang presisi, terukur, dan berimbang antara keamanan negara dan kebebasan berekspresi. Kebaruan penelitian ini terletak pada perumusan model delik yang mengintegrasikan unsur *actus reus-mens rea* secara eksplisit, penerapan prinsip *effects doctrine* dalam konteks teknologi penyamaran, serta pengujian pembatasan HAM menggunakan parameter *legality*, *necessity*, dan *proportionality*. Pendekatan ini menempatkan hukum pidana tidak hanya sebagai instrumen represif, tetapi sebagai mekanisme perlindungan konstitusional yang tetap menghormati prinsip negara hukum dan demokrasi digital.

D. KESIMPULAN

Berdasarkan hasil penelitian dan pembahasan, dapat disimpulkan bahwa pengaturan hukum pidana Indonesia terhadap penyebaran hoax dan disinformasi melalui jaringan proxy asing masih belum memadai. Ketentuan dalam Kitab Undang-Undang Hukum Pidana masih bersifat konvensional dan belum mengantisipasi perkembangan teknologi informasi yang memungkinkan penggunaan proxy, VPN, atau jaringan anonimisasi untuk menyamarkan identitas pelaku. Sementara itu, Undang-Undang Informasi dan Transaksi Elektronik (UU ITE) memang telah mengatur kejahatan siber, namun belum secara spesifik mengatur penggunaan teknologi penyamaran maupun fenomena *organized disinformation campaign, foreign information interference*, serta pertanggungjawaban pidana platform digital yang memfasilitasi penyebaran hoax. Dalam praktiknya, penegakan hukum juga menghadapi kendala yuridis berupa keterbatasan yurisdiksi ekstrateritorial dan ketidakjelasan unsur delik, kendala teknis terkait kapasitas digital forensik dan kompleksitas enkripsi, kendala kelembagaan akibat fragmentasi kewenangan, serta hambatan kerja sama internasional karena keterbatasan perjanjian bantuan hukum timbal balik dan perbedaan sistem hukum antarnegara.

Oleh karena itu, fungsionalisasi hukum pidana yang ideal memerlukan pendekatan yang komprehensif dan terintegrasi. Reformulasi ketentuan pidana perlu dilakukan dengan memperjelas unsur delik, menambahkan delik khusus terkait disinformasi terorganisir, serta menyesuaikan ancaman pidana secara proporsional. Penguatan yurisdiksi ekstrateritorial melalui penerapan prinsip *effects doctrine* dan *protective principle* menjadi penting untuk menjangkau kejahatan lintas batas. Di samping itu, diperlukan peningkatan kapasitas penegak hukum melalui penguatan kompetensi sumber daya manusia dan modernisasi infrastruktur, harmonisasi regulasi dan kelembagaan untuk mengurangi tumpang tindih kewenangan, serta penguatan kerja sama internasional melalui perjanjian bilateral dan multilateral. Pendekatan represif tersebut harus diimbangi dengan

upaya preventif melalui literasi digital dan pembangunan ekosistem informasi yang sehat, serta tetap menjamin perlindungan hak asasi manusia melalui penerapan *safeguards, due process*, dan mekanisme pengawasan yang efektif.

Adapun saran dalam penelitian ini yaitu kepada pembentuk undang-undang, perlu segera melakukan pembaruan regulasi dengan mempercepat revisi Kitab Undang-Undang Hukum Pidana dan amandemen Undang-Undang Informasi dan Transaksi Elektronik agar memuat ketentuan khusus mengenai kejahatan informasi terhadap keamanan negara yang menggunakan teknologi penyamaran digital. Kemudian, penguatan posisi Indonesia dalam kerja sama internasional juga menjadi penting, baik melalui ratifikasi *Budapest Convention on Cybercrime* maupun pembentukan konvensi regional terkait kejahatan siber. Seluruh langkah tersebut harus didukung dengan alokasi anggaran yang memadai guna memperkuat kapasitas penegakan hukum siber secara berkelanjutan.

Di sisi lain, aparat penegak hukum perlu meningkatkan kompetensi personel melalui pelatihan dan sertifikasi digital forensik secara berkesinambungan serta membangun kerja sama operasional dengan otoritas negara lain untuk pertukaran informasi dan pelaksanaan *joint investigation*. Penyusunan *standard operating procedure* yang jelas dalam penanganan perkara hoax dan disinformasi juga diperlukan agar tetap mempertimbangkan aspek kebebasan berekspresi dan prinsip *due process*.

E. DAFTAR PUSTAKA

- Abbas, N. A. (2026). *KUHAP Baru: Adaptasi Pembuktian di Era Digital*. MARI News.
- Alaini. (2026). Analisis Yuridis Tindak Pidana Penyebaran Hoaks Dalam Perspektif Hukum Pidana Indonesia Pasca Pembaharuan KUHP. *IJBL: Indonesia of Journal Business Law*, 5(1), 19–40. <https://doi.org/10.47709/ijbl.v5i1.7535>
- Arianto, D., Rindiani, A., & Yuliana, S. (2026). Analisis Penegakan Hukum Pidana dalam Menangani Ujaran Kebencian Berbasis Sara di Platform Media Sosial. *Legal Standing, Jurnal Ilmu Hukum*, 10(1), 1–17. <https://doi.org/10.24269/lv.v9i5.12589>
- Arief, B. N. (2016). *Bunga Rampai Kebijakan Hukum Pidana Perkembangan Penyusunan Konsep KUHP Baru*. Prenadamedia.
- Auli, R. C. (2024). *Pasal 390 KUHP tentang Berita Bohong*. HukumOnline.Com.
- Aziz, Z. A. (2025). Peran Literasi Media dalam Menangkal Penyebaran Hoaks di Era Digital. *Iqtida: Journal of Da'wah and Communication*, 5(2), 248–264.
-
-

- <https://doi.org/10.28918/iqtida.v5i02.11593>
- Brennen, J. S., Simon, F., Howard, P. N., & Nielsen, R. K. (2020). Types, Sources, and Claims of COVID-19 Misinformation. In *Reuters Institute for the Study of Journalism*, Oxford University.
<https://doi.org/https://dx.doi.org/10.60625/risj-awvq-sr55>
- BSSN. (2020). *Laporan Tahunan BSSN*.
- Candra, M., & Dinata, M. R. K. (2025). Penegakan Hukum terhadap Tindak Pidana Penyebaran Berita Hoaks melalui Media Sosial. *Arus Jurnal Sosial Dan Humaniora (AJSH)*, 5(2), 1577–1586.
<http://jurnal.ardenjaya.com/index.php/ajsh>
<http://jurnal.ardenjaya.com/index.php/ajsh>
- Edmon, M. (2013). *Tanggung Jawab Hukum Penyelenggara Sistem Elektronik*. RajaGrafindo Persada.
- Firganefi, & Diska Nabila, A. (2024). Penegakan Hukum Terhadap Tindak Pidana Penyebaran Berita Bohong (Hoax) Mengenai Politik Melalui Media Sosial. *Lex Lata: Jurnal Ilmiah Ilmu Hukum*, 6(1), 85–95.
<https://doi.org/10.28946/lexl.v6i1.2624>
- Indarta, Y. (2025). *Cyber Law: Dimensi Hukum dalam Era Digital*. Pustaka Galeri Mandiri.
- Irwansyah. (2021). *Penelitian Hukum Pilihan Metode & Praktik Penulisan Artikel* (A. Yunus (ed.); Revisi). Mirra Buana Media.
- MASTEL. (2021). *Survei Literasi Digital Indonesia 2021*. Masyarakat Telematika Indonesia.
- Nations, U. (1948). *Universal Declaration of Human Rights*. 217A.
- Nations, U. (1966). *International Covenant on Civil and Political Rights*. 999.
- Nurdin, S. W., & Nugraha, I. F. (2025). Ancaman Deepfake Dan Disinformasi Berbasis Ai: Implikasi Terhadap Keamanan Siber Dan Stabilitas Nasional Indonesia. *JIMR: Journal Of International Multidisciplinary Research*, 4(1), 73–92.
<http://azramedia-indonesia.azramediaindonesia.com/index.php/JIMR/indexDOI:https://doi.org/10.62668/jimr.v4i01.1551>
- Oktabiantoro, D., & Wulan, E. R. (2024). Ketidakjelasan Makna “Mentransmisikan” Pasal 28 Ayat 2 Undang-Undang Informasi dan Transaksi Elektronik Revisi Kedua. *Iblam Law Review*, 4(1), 461–467.
<https://doi.org/https://doi.org/10.52249/ilr.v4i1.307>
- Persily, N. (2017). The 2016 U.S. Election: Can Democracy Survive the Internet? *Journal of Democracy*, 28(2), 63–76.
<https://doi.org/https://doi.org/10.1353/jod.2017.0025>
- Purnomo, H., & M, A. Y. (2021). Inkonsistensi Penegakan Hukum Tindak Pidana Hoaks Di Indonesia Pasca Reformasi. *Jurnal Ius Constituendum*, 6(2), 235–251.
<https://doi.org/https://doi.org/10.26623/jic.v6i1.3176>
- Putra, A. V., & Wisnubroto, A. (2013). Eksistensi Pasal 27 ayat (3) Undang-Undang Nomor 11 Tahun 2008 dalam Perkara Pencemaran Nama Baik. *Journal Universitas Atma Jaya Yogyakarta*, 3, 1–17.
<https://repository.uajy.ac.id/id/eprint/4921/1/AtvenVemanda> NPM
-
-

090510007.JURNAL.pdf

- Rahmad, N., & Anggita, S. O. (2025). Korelasi Antara Dukungan Infrastruktur dan Optimalisasi Hukum Di Indonesia. *Jurnal SUTASOMA: Science Teknologi Sosial Humaniora*, 4(1), 13–18. <https://doi.org/https://doi.org/10.58878/sutasoma.v4i1.408>
- Rizkia, S. N., Ramadhan, M. R., Akmal, S. A., & Hosnah, A. U. (2025). Penerapan Asas Proposionalitas Oleh Mahkamah Konstitusi Dalam Pengujian Undang-Undang. *Indonesian Journal of Islamic Jurisprudence, Economic and Legal Theory*, 3(4), 3315–3319. <https://mail.shariajournal.com/index.php/IJIEL/article/view/1481>
- Shao, C., Ciampaglia, G. L., Varol, O., Yang, K.-C., Flammini, A., & Menczer, F. (2018). The Spread of Low-Credibility Content by Social Bots. *Nature Communications*, 9(1), 1–9. <https://www.nature.com/articles/s41467-018-06930-7>
- Sukmareni, S., Fernando, Z. J., Yunus, A., Flora, H. S., Amelia, H., Satrul, H. S., & Ukas. (2026). *Kriminologi 5.0: Memahami Kejahatan di Era Siber*. CV. Edu Akademi.
- Suriadi Hari. (2025). Krisis Kepercayaan Masyarakat terhadap Lembaga Publik di Era Disinformasi Digital. *Journal of Social, Educational and Religious Studies*, 1(1), 38–52. <https://jurnal.suriaacademicpress.com/index.php/JSERS/article/view/10>
- Vosoughi, S. (2018). The Spread of True and False News Online. *Science*, 359(6380), 1146–1151. <https://doi.org/https://doi.org/10.1126/science.aap9559>
- Wadjo, H. Z., Hasibuan, M. N. P., Sueni, A. S., Z, Y. F., Naidah, S., Kamaluddin, M., Amrullah, R., Hattu, J., Ramadhan, R. A. K., Apriyani, R., Hehanussa, D. J. A., Darlisma, D., & Muhariza, I. Y. (2025). *Delik-Delik dalam KUHP: klasifikasi, Unsur dan Analisis Yuridis*. CV. Gita Lentera.
- Wardle, C., & Derakhshan, H. (2017). *Information Disorder: Toward an Interdisciplinary Framework for Research and Policy Making*. Council of Europe Report. <https://www.firstdraftnews.org/wp-content/uploads/2017/11/PREMS-162317-GBR-2018-Report-désinformation-1.pdf>
- Wicaksana, P. (2022). *Pakar Hukum Siber UNAIR: Indonesia Harus Meratifikasi Budapest Convention*. UNAIR NEWS. <https://unair.ac.id/pakar-hukum-siber-unair-indonesia-harus-meratifikasi-budapest-convention/>
- Wildanah, H., & Rivai, A. (2025). Harmonisasi Lex Specialis UU ITE dan KUHP dalam Penegakan Cybercrime serta Validitas Transaksi Elektronik di Indonesia general provisions in the Criminal Code and specific provisions in the Electronic Information and Transaction Law (EIT Law), in additi. *Sawerigading Law Journal*, 4(2), 106–127. <https://doi.org/https://doi.org/10.62084/slj.v4i2.454>
- Yuwono, T., Kusniati, R., & Ardianto, B. (2021). Bantuan Hukum Timbal Balik dalam Penanganan Kejahatan Transnasional: Studi. *Uti Possidetis: Journal of International Law*, 2(3), 268–287. <https://doi.org/https://doi.org/10.22437/up.v2i3.13042>
-
-