

Pengaturan Cyberstalking Dalam Tinjauan Hukum Positif Indonesia Dan Hukum Pidana Islam

Putri Jannatul Husna

Universitas Islam Negeri Ar-Raniry, Aceh, Indonesia
Email Koresponden: 200104013@student.ar-raniry.ac.id

Abstrak

Cyberstalking merupakan bentuk penguntitan melalui media digital yang hingga saat ini belum dirumuskan sebagai tindak pidana tersendiri (*sui generis*) dalam sistem hukum Indonesia. Meskipun berbagai perbuatan yang memiliki karakteristik *cyberstalking* dapat dijerat melalui ketentuan Kitab Undang-Undang Hukum Pidana (KUHP), Undang-Undang Informasi dan Transaksi Elektronik (UU ITE), Undang-Undang Perlindungan Data Pribadi (UU PDP), dan Undang-Undang Tindak Pidana Kekerasan Seksual (UU TPKS), pengaturannya masih bersifat terfragmentasi karena masing-masing ketentuan menjangkau perbuatan konkret yang berbeda. Kondisi tersebut berpotensi menimbulkan perbedaan dalam konstruksi hukum dan penerapan ketentuan pidana serta memengaruhi kepastian hukum dan perlindungan korban. Penelitian ini bertujuan menganalisis pengaturan *cyberstalking* dalam hukum positif Indonesia, mengkaji implikasi belum adanya pengaturan khusus terhadap kepastian hukum, serta menganalisis *cyberstalking* dalam perspektif hukum pidana Islam. Penelitian ini menggunakan metode penelitian hukum normatif dengan pendekatan perundang-undangan, konseptual, dan komparatif, melalui studi kepustakaan terhadap peraturan perundang-undangan, putusan pengadilan, literatur ilmiah, serta sumber hukum Islam. Hasil penelitian menunjukkan bahwa *cyberstalking* belum memiliki rumusan delik mandiri dalam hukum positif Indonesia, sehingga penanganannya masih bergantung pada kualifikasi perbuatan konkret berdasarkan ketentuan pidana yang tersedia. Karakteristik berupa pengulangan, persistensi, sifat tidak dikehendaki, dan tingkat intrusi terhadap privasi dapat digunakan sebagai parameter analitis untuk mengidentifikasi pola *cyberstalking*, tetapi tidak dengan sendirinya merupakan unsur tindak pidana yang berdiri sendiri. Studi komparatif menunjukkan bahwa beberapa negara telah mengembangkan pengaturan yang lebih khusus terhadap *cyberstalking* dengan menekankan pola perilaku dan perlindungan korban. Dalam perspektif hukum pidana Islam, *cyberstalking* dapat dianalisis melalui konsep *jarimah ta'zir* karena bentuk perbuatannya dapat berkaitan dengan perlindungan kehormatan, privasi, ketenteraman, dan *kemaslahatan* korban. Penelitian ini merekomendasikan pengembangan pengaturan khusus *cyberstalking* yang mampu mengakomodasi karakteristik pola perilaku berulang sekaligus memberikan kepastian hukum dan perlindungan yang lebih *efektif* bagi korban.

Kata Kunci: Cyberstalking; Hukum Positif Indonesia; Hukum Pidana Islam; Kepastian Hukum; Jarimah Ta'Zir.

Pendahuluan

Perkembangan teknologi digital dalam satu dekade terakhir telah secara fundamental mengubah pola komunikasi, aktivitas ekonomi, serta



interaksi sosial masyarakat Indonesia. Transformasi tersebut menghadirkan berbagai kemudahan dalam kehidupan sehari-hari, namun pada saat yang sama juga memunculkan berbagai bentuk kejahatan siber (*cybercrime*) yang semakin kompleks (Efendi et al., 2026). Salah satu bentuk perilaku bermasalah dalam ruang siber yang berkembang seiring transformasi digital adalah *cyberstalking*, yaitu perilaku penguntitan yang dilakukan melalui media elektronik dengan memanfaatkan berbagai platform digital (Audrina et al., 2024). Berbeda dengan kejahatan siber lain yang telah memperoleh perhatian lebih luas dalam regulasi maupun penelitian, *cyberstalking* masih menghadapi berbagai persoalan konseptual dan yuridis dalam sistem hukum Indonesia, sehingga penanganannya belum sepenuhnya memberikan kepastian hukum maupun perlindungan yang optimal bagi korban (Habibi et al., 2020). Secara umum, *cyberstalking* dipahami sebagai serangkaian tindakan mengawasi, memantau, menghubungi, atau mengganggu seseorang secara berulang melalui media elektronik tanpa persetujuan korban sehingga menimbulkan rasa takut, tekanan *psikologis*, atau terganggunya rasa aman (Wahyuningsih, 2025). Karakter utama perilaku ini tidak terletak pada satu tindakan tunggal, melainkan pada adanya *pattern of conduct*, yaitu pola perilaku yang dilakukan secara berulang dan sistematis. Perkembangan teknologi digital turut memperbesar risiko terjadinya *cyberstalking* karena anonimitas di ruang siber memungkinkan pelaku mengumpulkan informasi pribadi, memantau aktivitas korban, mengirimkan pesan secara terus-menerus, hingga melakukan intimidasi tanpa mudah teridentifikasi (Komnas Perempuan, 2026). Dampak yang ditimbulkan tidak hanya berupa gangguan *psikologis* dan hilangnya rasa aman, tetapi dalam kondisi tertentu dapat berkembang menjadi bentuk kejahatan lain seperti *doxing*, *sextortion*, maupun penguntitan di dunia nyata. Fenomena tersebut tercermin dalam meningkatnya laporan Kekerasan Berbasis Gender Online (KBGO) yang diterima Komisi Nasional Anti Kekerasan terhadap Perempuan (Komnas Perempuan), di mana *cyberstalking* menjadi salah satu pola perilaku yang kerap dilaporkan (Komnas Perempuan, 2026). Kondisi tersebut menunjukkan bahwa *cyberstalking* tidak lagi dapat dipandang semata-mata sebagai persoalan etika bermedia digital, melainkan telah berkembang menjadi

persoalan hukum yang berkaitan erat dengan perlindungan privasi, keamanan, dan hak atas rasa aman setiap individu.

Persoalan mendasar dalam konteks hukum positif Indonesia adalah bahwa *cyberstalking* hingga saat ini belum dirumuskan sebagai tindak pidana tersendiri (*sui generis*). Berbagai perilaku yang memiliki karakteristik *cyberstalking* dapat dijerat berdasarkan ketentuan dalam Kitab Undang-Undang Hukum Pidana, Undang-Undang Informasi dan Transaksi Elektronik, Undang-Undang Perlindungan Data Pribadi, maupun peraturan perundang-undangan lainnya (Sinaga et al., 2021). Namun, pengaturan tersebut masih bersifat terfragmentasi karena masing-masing ketentuan hanya mengatur *fragmen* perilaku tertentu, seperti ancaman, penghinaan, akses ilegal, atau penyalahgunaan data pribadi, tanpa merumuskan *cyberstalking* sebagai satu kesatuan pola perilaku (Winarno et al., 2021). Akibatnya, penerapan hukum sangat bergantung pada karakteristik masing-masing perkara sehingga berpotensi menimbulkan perbedaan dalam konstruksi hukum, penerapan pasal, maupun tingkat perlindungan terhadap korban. Kondisi ini tidak hanya memunculkan persoalan kepastian hukum, tetapi juga menunjukkan perlunya evaluasi terhadap model pengaturan *cyberstalking* dalam sistem hukum Indonesia. Dalam konteks tersebut, perspektif hukum pidana Islam menjadi relevan untuk dikaji karena menawarkan nilai-nilai perlindungan terhadap kehormatan (*ḥifẓ al-'ird*), perlindungan terhadap jiwa (*ḥifẓ al-nafs*), dan *kemaslahatan* yang dapat memperkaya analisis mengenai perlindungan korban kejahatan digital.

Kajian mengenai *cyberstalking* di Indonesia sesungguhnya telah mengalami perkembangan yang cukup signifikan. Sebagian besar penelitian terdahulu berfokus pada pertanggungjawaban pidana pelaku, identifikasi ketentuan hukum yang dapat digunakan untuk menjerat pelaku berdasarkan KUHP maupun UU ITE, serta perlindungan hukum bagi korban (Purnama et al., 2024; Pratama et al., 2024). Sejumlah penelitian lain juga telah mengaitkan *cyberstalking* dengan perspektif hukum pidana Islam melalui konsep *fiqh jināyah* dan *jarimah ta'zīr* (Wanantho et al., 2024), baik dalam kerangka *jināyah* secara umum (Inaya & Yazid, 2025) maupun dalam

pembahasan mengenai penguntitan di media sosial (Fauzan et al., 2025). Meskipun demikian, perhatian terhadap implikasi yuridis dari belum adanya pengaturan *cyberstalking* sebagai tindak pidana tersendiri terhadap kepastian hukum masih relatif terbatas. Demikian pula, kajian yang mengintegrasikan analisis hukum positif Indonesia dengan perspektif hukum pidana Islam dalam rangka mengevaluasi kebutuhan pembaruan pengaturan *cyberstalking* belum banyak dilakukan. Berangkat dari kondisi tersebut, penelitian ini menawarkan tiga kontribusi utama. Pertama, penelitian ini menganalisis implikasi pengaturan *cyberstalking* yang masih terfragmentasi terhadap kepastian hukum dalam sistem hukum pidana Indonesia. Kedua, penelitian ini mengintegrasikan analisis hukum positif dengan perspektif hukum pidana Islam, khususnya konsep *jarīmah ta'zīr*, untuk memberikan landasan konseptual dalam memahami *cyberstalking* sebagai bentuk kejahatan siber kontemporer. Ketiga, penelitian ini menawarkan kerangka analitis berupa *parameter normatif* untuk membedakan perilaku *cyberstalking* yang masih berada dalam ranah gangguan sosial dengan perilaku yang telah memenuhi karakteristik tindak pidana sebagai bahan pertimbangan dalam pengembangan pengaturan hukum di Indonesia.

Sejumlah negara telah mengembangkan model pengaturan yang secara lebih *eksplisit* mengakomodasi perilaku *stalking* melalui sarana elektronik, sementara negara lainnya masih mengandalkan kombinasi ketentuan pidana umum dan peraturan sektoral. Variasi tersebut menunjukkan bahwa kriminalisasi *cyberstalking* tidak hanya berkaitan dengan perumusan delik, tetapi juga dengan cara sistem hukum mengidentifikasi pola perilaku, melindungi korban, dan menjamin kepastian hukum. Dibandingkan dengan negara-negara tersebut, Indonesia masih mengandalkan pengaturan yang tersebar dalam berbagai peraturan perundang-undangan sehingga belum memiliki konstruksi hukum yang secara khusus mengakomodasi karakteristik *cyberstalking* sebagai suatu pola perilaku.

Berdasarkan latar belakang tersebut, penelitian ini difokuskan untuk menjawab tiga pertanyaan utama. Pertama, bagaimana pengaturan *cyberstalking* dalam hukum positif Indonesia? Kedua, apa implikasi yuridis

dari belum adanya pengaturan *cyberstalking* sebagai tindak pidana tersendiri terhadap kepastian hukum dalam penegakan hukum di Indonesia? Ketiga, bagaimana hukum pidana Islam memandang *cyberstalking* dan sejauh mana konsep *jarimah ta'zīr* dapat memberikan landasan normatif bagi pengembangan pengaturan *cyberstalking* di Indonesia? Untuk menjawab pertanyaan tersebut, penelitian ini bertujuan menganalisis pengaturan *cyberstalking* dalam hukum positif Indonesia, mengkaji implikasi *fragmentasi* pengaturannya terhadap kepastian hukum, serta menganalisis relevansi konsep *jarimah ta'zīr* sebagai landasan konseptual dalam pengembangan pengaturan *cyberstalking* di Indonesia. Penelitian ini diharapkan memberikan kontribusi baik secara teoritis maupun praktis. Dari sisi akademik, penelitian ini diharapkan memperkaya pengembangan kajian hukum pidana siber melalui analisis terhadap *fragmentasi* pengaturan *cyberstalking* yang dipadukan dengan perspektif hukum pidana Islam. Dari sisi praktis, hasil penelitian ini diharapkan menjadi bahan pertimbangan bagi aparat penegak hukum dalam memahami karakteristik *cyberstalking* serta memberikan masukan bagi pembentuk kebijakan dalam merumuskan pengaturan yang lebih komprehensif sehingga mampu mewujudkan kepastian hukum dan perlindungan yang lebih efektif bagi korban *cyberstalking* di Indonesia.

Metode Penelitian

Penelitian ini merupakan penelitian hukum normatif (*juridis normatif*), yaitu penelitian yang berfokus pada pengkajian norma, asas, doktrin, serta kaidah hukum yang terdapat dalam berbagai peraturan perundang-undangan dan sumber hukum lainnya untuk menjawab isu hukum yang diteliti (Marzuki, 2017). Penelitian ini diarahkan untuk menganalisis pengaturan *cyberstalking* dalam hukum positif Indonesia, mengkaji implikasi belum adanya pengaturan khusus mengenai *cyberstalking* sebagai tindak pidana tersendiri (*sui generis*) terhadap kepastian hukum, serta menelaah persoalan tersebut melalui perspektif hukum pidana Islam sebagai landasan konseptual bagi pengembangan pengaturan *cyberstalking* di Indonesia (Soekanto & Mamudji, 2001).

Penelitian menggunakan tiga pendekatan. Pertama, pendekatan perundang-undangan (*statute approach*) (Ali, 2010) untuk menelaah berbagai ketentuan hukum yang berkaitan dengan *cyberstalking* meliputi Kitab Undang-Undang Hukum Pidana, Undang-Undang Informasi dan Transaksi Elektronik beserta perubahannya, Undang-Undang Perlindungan Data Pribadi, Undang-Undang Tindak Pidana Kekerasan Seksual, serta peraturan perundang-undangan lain yang relevan. Kedua, pendekatan konseptual (*conceptual approach*) (Efendi & Ibrahim, 2018) yang digunakan untuk mengkaji konsep-konsep hukum mengenai *cyberstalking*, tindak pidana siber, delik khusus (*sui generis*), kepastian hukum, serta konsep *jarīmah ta'zīr* dalam hukum pidana Islam. Ketiga, pendekatan komparatif (*comparative approach*) (Ariawan, 2013) digunakan untuk membandingkan pengaturan *cyberstalking* dalam hukum positif Indonesia dengan beberapa yurisdiksi lain yang memiliki karakteristik pengaturan berbeda, sekaligus membandingkannya dengan konsep hukum pidana Islam. Pendekatan ini bertujuan mengidentifikasi persamaan, perbedaan, serta kemungkinan pengembangan pengaturan *cyberstalking* di Indonesia.

Bahan hukum yang digunakan terdiri atas bahan hukum primer, sekunder, dan tersier. Bahan hukum primer meliputi Undang-Undang Dasar Negara Republik Indonesia Tahun 1945, Kitab Undang-Undang Hukum Pidana, Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik beserta seluruh perubahannya hingga Undang-Undang Nomor 1 Tahun 2024, Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi, Undang-Undang Nomor 12 Tahun 2022 tentang Tindak Pidana Kekerasan Seksual, Kitab Undang-Undang Hukum Acara Pidana, putusan pengadilan yang relevan, serta Al-Qur'an dan Hadis sebagai sumber hukum pidana Islam. Putusan pengadilan digunakan untuk menganalisis bagaimana hakim mengonstruksikan perbuatan yang memiliki karakteristik *cyberstalking* ke dalam ketentuan pidana yang tersedia (Firmansyah et al., 2024). Adapun bahan hukum sekunder berupa buku, artikel ilmiah, hasil penelitian terdahulu, serta dokumen resmi lembaga negara, sedangkan bahan hukum tersier berupa kamus hukum dan ensiklopedia yang mendukung penafsiran terhadap bahan hukum primer dan

sekunder. Pengumpulan bahan hukum dilakukan melalui studi kepustakaan (*library research*) dengan cara mengidentifikasi, menginventarisasi, mengklasifikasikan, dan menelaah berbagai bahan hukum yang relevan dengan objek penelitian (Djarawula et al., 2023). Seluruh bahan hukum yang diperoleh kemudian dianalisis secara kualitatif melalui analisis deskriptif, interpretatif, dan komparatif (Disemadi, 2022). Analisis deskriptif digunakan untuk menguraikan pengaturan *cyberstalking* dalam hukum positif Indonesia, sedangkan analisis interpretatif digunakan untuk menafsirkan ketentuan hukum serta konsep-konsep yang berkaitan dengan *cyberstalking*, kepastian hukum, dan *jarīmah ta'zīr* (Arianto & Prasetyo, 2025). Selanjutnya, analisis komparatif dilakukan untuk membandingkan model pengaturan *cyberstalking* di Indonesia dengan beberapa negara yang dipilih secara purposive berdasarkan variasi pendekatan regulasinya, yaitu negara yang telah memiliki pengaturan khusus mengenai *cyberstalking* (Inggris dan Singapura), negara yang masih mengandalkan ketentuan pidana umum (Sri Lanka), serta negara yang sedang menghadapi tantangan harmonisasi antara perkembangan teknologi dan hukum (Australia, Pakistan, dan India). Hasil analisis tersebut digunakan untuk mengidentifikasi kelebihan dan keterbatasan pengaturan yang berlaku serta merumuskan argumentasi mengenai arah pengembangan pengaturan *cyberstalking* dalam hukum positif Indonesia dengan mempertimbangkan nilai-nilai hukum pidana Islam.

Pembahasan

A. Analisis Pengaturan Cyberstalking dalam Hukum Positif Indonesia

Dalam penelitian ini, *cyberstalking* dipahami sebagai pola perilaku berulang melalui media elektronik yang dilakukan tanpa persetujuan korban dengan tujuan mengawasi, mengendalikan, mengintimidasi, atau menimbulkan rasa takut sehingga mengganggu rasa aman dan privasi korban. Sampai saat ini, hukum positif Indonesia belum merumuskan *cyberstalking* sebagai tindak pidana yang berdiri sendiri (*sui generis*). Namun, kondisi tersebut tidak berarti bahwa hukum Indonesia sama sekali tidak memiliki ketentuan yang dapat menjangkau perbuatan penguntitan. Undang-Undang Nomor 1 Tahun 2023 tentang Kitab Undang-Undang Hukum Pidana

(KUHP) yang mulai berlaku pada 2 Januari 2026, misalnya, telah mengatur perbuatan mengikuti orang lain secara mengganggu dalam Pasal 317. Ketentuan tersebut menunjukkan bahwa perilaku *stalking* telah memperoleh pengakuan dalam hukum pidana nasional, tetapi belum secara khusus mengakomodasi karakter *cyberstalking* yang dilakukan melalui sistem elektronik dan melibatkan pola perilaku lintas platform (Zaki, 2022). Dengan demikian, persoalan hukum *cyberstalking* di Indonesia lebih tepat dipahami sebagai *fragmentasi pengaturan*, bukan sebagai kekosongan norma secara mutlak. Berbagai ketentuan pidana memang tersedia untuk menjerat bagian tertentu dari perilaku *cyberstalking*, tetapi hingga kini belum dirumuskan secara khusus sebagai tindak pidana tersendiri, sehingga penggunaannya masih bergantung pada berbagai ketentuan pidana yang tersebar (Budianto Pansariadi & Soekorini, 2023). Perumusan *cyberstalking* sebagai tindak pidana tersendiri menjadi penting karena perbuatan ini bersifat multidimensional, mencakup aspek pelecehan *nonverbal*, ancaman emosional, dan pelanggaran data pribadi yang tidak sepenuhnya terakomodasi dalam delik umum seperti penghinaan atau pengancaman tradisional (Purnama et al., 2024). Penempatan *cyberstalking* dalam kategori delik khusus, baik melalui pembentukan pengaturan khusus maupun melalui pembaruan hukum pidana nasional, diharapkan dapat memberikan kepastian hukum dan perlindungan yang lebih komprehensif bagi korban (Rumlus et al., 2023).

Selain KUHP, beberapa instrumen hukum sektoral dapat menjangkau unsur tertentu dari *cyberstalking*. Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi, misalnya, melarang setiap orang secara melawan hukum memperoleh atau mengumpulkan Data Pribadi yang bukan miliknya dengan maksud tertentu yang dapat mengakibatkan kerugian bagi subjek data, serta melarang pengungkapan atau penggunaan Data Pribadi secara melawan hukum. Ketentuan tersebut relevan ketika perilaku *cyberstalking* disertai pengumpulan, pengungkapan, atau penyalahgunaan data pribadi korban (Undang-Undang Nomor 12 Tahun 2022). Sementara itu, Undang-Undang Nomor 1 Tahun 2024 tentang Perubahan Kedua atas Undang-Undang Informasi dan Transaksi Elektronik tetap menyediakan

ketentuan yang dapat digunakan terhadap perilaku digital tertentu, termasuk ancaman kekerasan atau tindakan menakut-nakuti melalui sistem elektronik. Ketentuan tersebut dapat menjangkau *cyberstalking* apabila perilaku penguntitan disertai unsur ancaman atau intimidasi yang memenuhi unsur delik. Dengan demikian, UU ITE tidak mengatur *cyberstalking* sebagai delik tersendiri, melainkan menjangkau aspek tertentu dari perilaku tersebut (Putusan Pengadilan Negeri Surabaya Nomor 1842/Pid.Sus/2024/PN Sby, 2024). UU Nomor 12 Tahun 2022 tentang Tindak Pidana Kekerasan Seksual juga memiliki relevansi terbatas. Pasal 14 mengatur kekerasan seksual berbasis elektronik, termasuk penguntitan dan/atau pelacakan menggunakan sistem elektronik terhadap orang yang menjadi objek dalam informasi atau dokumen elektronik untuk tujuan seksual. Oleh karena itu, ketentuan tersebut dapat diterapkan terhadap *cyberstalking* apabila perbuatan penguntitan atau pelacakan memenuhi unsur tujuan seksual sebagaimana ditentukan oleh undang-undang. Berdasarkan keseluruhan pengaturan tersebut, terlihat bahwa hukum positif Indonesia telah memiliki sejumlah norma yang dapat menjangkau *fragmen* perilaku *cyberstalking*, tetapi belum mengatur *cyberstalking* sebagai satu kesatuan pola perilaku. Fragmentasi tersebut menimbulkan kekaburan mengenai batas konseptual dan yuridis *cyberstalking*, khususnya ketika suatu perkara mengandung rangkaian tindakan berulang yang tidak seluruhnya memenuhi unsur salah satu delik secara tersendiri. Di sisi lain, Mahkamah Konstitusi dalam putusan pengujian ketentuan pencemaran nama baik pada UU ITE telah menegaskan pentingnya kejelasan rumusan norma pidana demi kepastian hukum (Putusan Mahkamah Konstitusi Nomor 50/PUU-VI/2008, 2008), sebuah prinsip yang relevan ditarik ke persoalan *cyberstalking* mengingat rumusan yang tersebar dan tidak spesifik berpotensi menimbulkan persoalan serupa dalam praktik peradilan sebagaimana tampak pula pada putusan kasasi Mahkamah Agung yang menerapkan ketentuan UU ITE terhadap perbuatan yang berkarakter penguntitan dan intimidasi elektronik (Putusan Mahkamah Agung Nomor 3635 K/Pid.Sus/2022, 2022). Meskipun berbagai ketentuan tersebut dapat digunakan untuk menjerat pelaku *cyberstalking*, pendekatan hukum positif Indonesia masih bersifat *parsial* karena setiap pasal hanya

mengakomodasi sebagian unsur perbuatan tersebut. UU ITE lebih menitikberatkan pada adanya ancaman atau pencemaran nama baik, sedangkan UU PDP berfokus pada penyalahgunaan data pribadi dan UU TPKS terbatas pada kasus yang bermuatan seksual. Akibatnya, karakter utama *cyberstalking* sebagai pola perilaku yang dilakukan secara berulang (*pattern of conduct*) belum memperoleh pengakuan normatif yang utuh. Kondisi ini menyebabkan perlindungan hukum terhadap korban bergantung pada kemampuan aparat untuk mengonstruksikan perbuatan pelaku ke dalam delik lain yang sebenarnya tidak dirancang secara khusus untuk mengatur *cyberstalking*.

Tabel 1. Unsur-unsur Cyberstalking dalam Hukum Positif Indonesia

Unsur Cyberstalking	Instrumen Hukum
Pengiriman pesan berulang	UU ITE Pasal 29 jo. 45B (terbatas jika ada ancaman)
Pemantauan aktivitas daring	Belum diatur eksplisit
Pengumpulan data pribadi tanpa izin	UU PDP
Penyebaran informasi memalukan	UU ITE Pasal 27A
Penguntitan bermuatan seksual	UU TPKS Pasal 14

Sumber: hasil analisis penulis berdasarkan KUHP, UU ITE, UU PDP, dan UU TPKS.

Untuk melihat bagaimana *cyberstalking* dikonstruksikan dalam praktik, perlu ditinjau beberapa putusan pengadilan yang memuat karakteristik perbuatan tersebut. Meskipun belum terdapat delik *cyberstalking* secara *eksplisit*, aparat penegak hukum tetap berupaya menjangkau perilaku tersebut melalui berbagai ketentuan pidana yang telah

Putusan	Fakta Singkat	Pasal yang Digunakan	Temuan Penulis
PN Surabaya No. 1842/Pid.Sus/2024/PN Sby	Penguntitan dan komunikasi elektronik berulang	UU TPKS	Unsur <i>cyberstalking</i> dipandang sebagai bagian

			dari KSBE, bukan delik mandiri
MA No. 3635 K/Pid.Sus/2022	Intimidasi melalui media elektronik	UU ITE	Penjeratan bergantung pada adanya ancaman <i>eksplisit</i> , bukan pola penguntitan

Tabel 2. Ilustrasi Konstruksi Delik dalam Praktik Peradilan

Kedua putusan tersebut menunjukkan bahwa aparat penegak hukum belum memiliki dasar normatif yang secara khusus mengatur *cyberstalking*, sehingga konstruksi dakwaan harus diarahkan pada delik lain yang dianggap paling mendekati karakter perbuatan pelaku. Kondisi ini menunjukkan adanya *fragmentasi norma* yang berpotensi menimbulkan ketidakpastian hukum. Dari hasil analisis terhadap karakteristik *cyberstalking* dan pengaturan hukum yang berlaku, terdapat beberapa faktor yang menyebabkan belum dirumuskannya *cyberstalking* sebagai tindak pidana tersendiri: Pertama, hingga kini belum terdapat perumusan unsur-unsur *cyberstalking* yang seragam sebagai dasar pembentukan delik, baik mengenai intensitas perbuatan, bentuk perilaku, maupun akibat yang ditimbulkan terhadap korban (Zaki, 2022). Kedua, *cyberstalking* memiliki karakter multidimensional karena merupakan rangkaian perilaku yang dapat mencakup pengawasan, intimidasi, pelecehan, pelanggaran privasi, maupun penyalahgunaan data pribadi, sehingga sulit direduksi ke dalam satu bentuk perbuatan pidana tunggal (Liawi et al., 2023). Ketiga, praktik penegakan hukum selama ini masih mengandalkan ketentuan pidana yang telah tersedia dalam KUHP, UU ITE, maupun peraturan perundang-undangan lainnya, sehingga pembentukan delik khusus mengenai *cyberstalking* belum menjadi prioritas legislasi (Andespitrikasih et al., 2024). Keempat, karakter *cyberstalking* yang dilakukan secara berulang, secara anonim, serta memanfaatkan berbagai platform digital menimbulkan tantangan tersendiri dalam pembuktian, terutama untuk membuktikan adanya pola perilaku (*pattern of conduct*) sebagai satu kesatuan tindak pidana (Hutasoit & Kurniawan, 2024).

B. Perbandingan Model Pengaturan Cyberstalking di Beberapa Negara

Pendekatan hukum terhadap *cyberstalking* di berbagai negara menunjukkan bahwa belum ada satu model pengaturan yang seragam. Perbedaan tersebut terutama terlihat pada cara masing-masing negara mendefinisikan *cyberstalking*, menentukan unsur tindak pidana, serta membangun mekanisme perlindungan bagi korban. Oleh karena itu, studi komparatif dilakukan untuk mengidentifikasi karakteristik pengaturan yang dapat menjadi bahan evaluasi terhadap sistem hukum Indonesia (Pratama et al., 2024). Inggris dan Singapura, misalnya, telah merumuskan ketentuan *eksplisit* mengenai *stalking* dan *cyberstalking* yang mencantumkan daftar contoh perbuatan (*non-exhaustive list*) sebagai pedoman penafsiran, sementara Sri Lanka masih bertumpu pada ketentuan pelecehan yang bersifat umum (Harasgama & Munasinghe, 2021). Studi perbandingan antara Australia dan Pakistan menunjukkan bahwa baik negara maju maupun berkembang sama-sama membutuhkan kesadaran publik, kebijakan yang tegas, dan penegakan hukum yang konsisten, disertai kolaborasi erat antara lembaga legislatif, aparat penegak hukum, dan penyedia layanan internet. Kajian mengenai kerangka hukum India juga menyoroti pentingnya pengembangan regulasi *cyberstalking* yang lebih adaptif terhadap perkembangan teknologi, disertai instrumen pencegahan seperti perintah perlindungan digital (*digital protection order*) dan mekanisme penghapusan konten yang cepat, serta menyoroti pentingnya definisi hukum yang adaptif terhadap perkembangan modus operasi kejahatan siber (Gopinath, 2026).

Kelompok	Negara	Fungsi Dalam Analisis
Model delik khusus yang matang	Inggris, Singapura	Menunjukkan bagaimana <i>cyberstalking</i> dirumuskan sebagai delik tersendiri dan unsur apa yang digunakan.
Model transisi atau campuran	Australia, India	Menunjukkan variasi pendekatan dan tantangan pengaturan dalam sistem hukum yang berkembang.
Model yang masih mengandalkan ketentuan umum	Sri Lanka	Menjadi pembanding yang lebih dekat dengan kondisi Indonesia karena belum memiliki pengaturan yang sepenuhnya komprehensif.

Tabel 3. Pola pengaturan pada sejumlah negara yang dibandingkan.

Perbandingan tersebut memperlihatkan bahwa negara-negara yang telah mengatur *cyberstalking* sebagai delik tersendiri memiliki tiga karakteristik utama. Hal tersebut memperlihatkan bahwa negara-negara yang telah mengatur *cyberstalking* sebagai delik tersendiri cenderung menempatkan pola perilaku (*pattern of conduct*) sebagai unsur utama, sedangkan Indonesia masih mengandalkan delik-delik yang mengatur *fragmen* perilaku tertentu. Jika dilihat dari tabel di atas, Indonesia sendiri lebih dekat dengan kelompok ketiga, yaitu Sri Lanka, yang masih menggunakan ketentuan umum dan belum memiliki pengaturan yang sepenuhnya komprehensif.

C. Implikasi Belum Adanya Pengaturan Khusus Terhadap Kepastian Hukum Dan Penegakan Hukum.

Belum adanya pengaturan khusus mengenai *cyberstalking* sebagai tindak pidana tersendiri menimbulkan sejumlah implikasi yuridis dalam sistem hukum pidana Indonesia. Implikasi pertama berkaitan dengan kepastian hukum. Meskipun berbagai bentuk perbuatan yang memiliki karakteristik *cyberstalking* dapat dijerat melalui ketentuan dalam KUHP, UU ITE, maupun peraturan perundang-undangan lainnya, tidak seluruh pola perilaku *cyberstalking* dapat secara langsung dikualifikasikan ke dalam unsur delik yang tersedia (Hartanto et al., 2024). Akibatnya, penanganan perkara sangat bergantung pada karakteristik perbuatan dalam setiap kasus serta kemampuan aparat penegak hukum untuk mengonstruksikannya ke dalam ketentuan pidana yang berlaku. Kondisi tersebut berpotensi menimbulkan variasi penerapan hukum terhadap perkara-perkara yang memiliki karakteristik serupa sehingga mengurangi konsistensi dan kepastian hukum. Selain itu, belum adanya delik khusus mengenai *cyberstalking* juga berdampak terhadap arah pengembangan hukum pidana nasional. Perkembangan teknologi informasi telah melahirkan bentuk-bentuk kejahatan yang memiliki karakteristik berbeda dengan kejahatan konvensional, terutama karena dilakukan melalui media digital, bersifat lintas platform, dan sering kali melibatkan pelanggaran privasi sebagai bentuk utama *viktimisasi* (Anisah & Nurisman, 2022). Oleh karena itu,

kebutuhan untuk merumuskan pengaturan khusus mengenai *cyberstalking* tidak semata-mata dimaksudkan untuk menambah jenis tindak pidana baru, melainkan sebagai upaya untuk membangun kepastian hukum, memberikan perlindungan hukum yang lebih komprehensif kepada korban, serta menyesuaikan hukum pidana Indonesia dengan perkembangan kejahatan siber dan kebutuhan masyarakat digital. Implikasi berikutnya berkaitan dengan perlindungan hukum terhadap korban. Ketidadaan pengaturan khusus menyebabkan perlindungan hukum terhadap korban *cyberstalking* belum diberikan secara utuh berdasarkan karakteristik perbuatannya, melainkan bergantung pada delik lain yang dianggap paling sesuai untuk diterapkan (Andespitrikasih et al., 2024). Akibatnya, perlindungan yang diberikan sering kali hanya mencakup aspek tertentu, seperti ancaman, penghinaan, akses ilegal, atau pelanggaran data pribadi, sementara keseluruhan pola penguntitan digital yang dilakukan secara berulang belum dipandang sebagai satu kesatuan perbuatan pidana. Padahal, karakter utama *cyberstalking* justru terletak pada rangkaian perilaku yang dilakukan secara terus-menerus (*pattern of conduct*), sehingga dampak yang ditimbulkan tidak selalu dapat dinilai dari satu tindakan secara terpisah (Kartono et al., 2026).

D. Batasan Konseptual dan Parameter Analitis Kualifikasi Perilaku Cyberstalking sebagai Gangguan dan Tindak Pidana

Dalam hukum positif Indonesia, belum terdapat rumusan delik yang secara khusus menetapkan *cyberstalking* sebagai tindak pidana tersendiri. Oleh karena itu, tidak tepat menetapkan satu rangkaian unsur sebagai “*unsur pidana cyberstalking*” yang berlaku secara mandiri. *Cyberstalking* lebih tepat dipahami sebagai pola perilaku yang dapat terdiri atas berbagai perbuatan konkret, seperti komunikasi yang dilakukan secara persisten, pengawasan terhadap aktivitas digital, akses terhadap akun atau perangkat tanpa hak, penggunaan data pribadi, maupun ancaman. Masing-masing perbuatan tersebut harus diklasifikasikan berdasarkan ketentuan pidana yang relevan dan hanya dapat dipertanggungjawabkan secara pidana apabila seluruh unsur delik yang menjadi dasar penjeratan terpenuhi.

Dengan demikian, karakteristik berupa pengulangan, persistensi, sifat tidak dikehendaki, serta dampak terhadap rasa aman korban berfungsi terutama sebagai *parameter konseptual* untuk mengidentifikasi suatu pola perilaku sebagai *cyberstalking*, bukan sebagai unsur delik pidana yang berdiri sendiri dalam hukum positif Indonesia. Pembedaan ini penting agar analisis *cyberstalking* tidak mencampurkan karakteristik suatu fenomena kriminal dengan unsur tindak pidana yang secara normatif harus dibuktikan berdasarkan ketentuan peraturan perundang-undangan.

Aspek	Aktivitas Digital	Cyberstalking
Kehendak	Dikehendaki/Diizinkan	Tidak dikehendaki dan tetap dilakukan
Tujuan	Dukungan/interaksi	Pengawasan/intimidasi/gangguan
Pola	Interaksi wajar	Berulang dan persisten
Batasan	Menghormati batasan	Mengabaikan batasan
Privasi	Berada pada ruang publik	Dapat mengintrusi ruang pribadi
Dampak	Tidak mengganggu rasa aman	Dapat mengganggu privasi dan rasa aman
Hukum	Umumnya bukan tindak pidana	Dapat memenuhi delik tertentu jika unsur terpenuhi

Tabel 4. Perbedaan Aktivitas Digital dan Cyberstalking

Tidak setiap bentuk pengamatan atau interaksi terhadap aktivitas seseorang di ruang digital dapat dikategorikan sebagai *cyberstalking*. Aktivitas seperti melihat *story*, memberikan *like*, mengikuti akun, berlangganan (*subscribe*) suatu *channel*, atau memberikan komentar terhadap konten yang tersedia untuk publik pada dasarnya merupakan bentuk interaksi digital yang berada dalam ranah sosial yang wajar. Penentuan suatu perilaku sebagai *cyberstalking* tidak semata-mata didasarkan pada *frekuensi* interaksi, tetapi harus memperhatikan pola perilaku, sifat tidak dikehendaki, tingkat intrusi terhadap privasi, cara memperoleh informasi, respons terhadap batasan yang diberikan korban, serta tujuan dan konteks perbuatan. Dengan demikian, pembedaan antara aktivitas penggemar dan *cyberstalking* diperlukan agar konsep *cyberstalking* tidak diterapkan secara berlebihan terhadap aktivitas digital yang pada dasarnya merupakan bentuk interaksi sosial yang sah.

Dalam konteks penentuan batas antara perilaku yang sekadar mengganggu dan perilaku yang memiliki relevansi pidana, penelitian ini menggunakan beberapa *parameter analitis*, antara lain *persistensi* (pengulangan perilaku), tingkat intrusi terhadap privasi, tujuan atau kecenderungan perilaku untuk mengawasi, mengendalikan, mengintimidasi, atau menimbulkan rasa takut, serta dampak yang ditimbulkan terhadap rasa aman dan kehidupan pribadi korban. Parameter tersebut tidak dimaksudkan sebagai unsur delik *cyberstalking* yang telah ditetapkan dalam hukum positif Indonesia, melainkan sebagai kerangka analitis untuk mengidentifikasi karakteristik dan tingkat keseriusan perilaku *cyberstalking*. Adapun suatu perbuatan dapat dikualifikasikan sebagai tindak pidana tetap bergantung pada terpenuhinya unsur-unsur delik tertentu yang telah diatur dalam peraturan perundang-undangan yang berlaku. Dengan demikian, keberadaan pola perilaku yang berulang dan dampak yang serius terhadap korban tidak dengan sendirinya menjadikan suatu perbuatan sebagai tindak pidana *cyberstalking*, tetapi dapat menjadi indikator untuk menilai karakteristik perbuatan serta menilai ketentuan pidana yang relevan untuk diterapkan berdasarkan fakta konkret suatu perkara. Penulis menyusun kerangka analitis tingkat keparahan *cyberstalking* sebagai alat bantu untuk membedakan perilaku yang masih berada pada ranah gangguan dengan perilaku yang telah memenuhi karakteristik tindak pidana. Kerangka ini disusun melalui sintesis terhadap karakteristik perbuatan yang relevan dalam hukum positif Indonesia, literatur mengenai *cyberstalking*, hasil perbandingan dengan beberapa negara, serta prinsip perlindungan korban dalam hukum pidana Islam. Oleh karena itu, klasifikasi ini bukan merupakan *klasifikasi normatif* yang telah diatur dalam peraturan perundang-undangan, melainkan model analitis yang digunakan untuk mendukung pembahasan.

Tingkat	Karakteristik Perilaku	Intensitas	Dampak	Relevansi Yuridis
I	Interaksi publik	Rendah	Tidak Nyaman	Belum Pidana
II	Gangguan berulang	Sedang	Tekanan <i>psikologis</i> ringan	Dapat terkait ketentuan tertentu

III	Pengawasan dan intimidasi	Tinggi	Ketakutan nyata	Dapat memenuhi unsur delik tertentu
IV	Ancaman, <i>doxing</i> , <i>sextortion</i>	Sangat Tinggi	Ancaman serius terhadap keamanan	Berpotensi kuat memenuhi unsur tindak pidana

Tabel 5. Parameter Analitis Tingkat Keparahan Cyberstalking

Parameter tersebut merupakan *konstruksi analitis* penelitian untuk mengidentifikasi tingkat keseriusan perilaku *cyberstalking* dan bukan merupakan klasifikasi tindak pidana yang telah ditetapkan oleh peraturan perundang-undangan. Hal ini untuk membantu menunjukkan kapan suatu perilaku masih berada pada tingkat gangguan dan kapan perilaku tersebut semakin menunjukkan karakteristik yang berpotensi bersinggungan dengan tindak pidana tertentu. Kualifikasi pidana tetap ditentukan berdasarkan terpenuhinya unsur delik yang relevan dalam hukum positif Indonesia.

A. Tingkat I – Interaksi Digital Biasa

Deskripsi: Melibatkan pencarian informasi publik mengenai seseorang secara pasif atau pengiriman pesan yang jarang dilakukan dan tidak menunjukkan pola intimidatif. Persistensi rendah; intrusi minimal; tidak menimbulkan rasa takut. Pada umumnya, belum menunjukkan relevansi pidana apabila tidak terdapat perbuatan lain yang memenuhi unsur delik tertentu dan masih berada dalam ranah interaksi digital biasa. Pelanggaran privasi: minimal, karena hanya menggunakan data yang tersedia untuk publik.

B. Tingkat II – Perilaku Mengganggu

Deskripsi: Pengiriman pesan yang mengganggu (*annoying*) secara berulang, komentar yang tidak pantas, atau mengikuti akun secara *obsesif* meskipun telah diminta untuk berhenti. Persistensi mulai meningkat; intrusi terhadap ruang pribadi; belum terdapat ancaman yang jelas. Dapat memiliki relevansi hukum tertentu apabila memenuhi unsur delik yang tersedia, tetapi tidak otomatis merupakan tindak pidana (R. Syailendra et al., 2023). Implikasi Etis: Pengabaian terhadap batasan pribadi individu. Pelanggaran privasi: menengah, mulai memasuki ruang pribadi komunikasi korban.

C. Tingkat III – Perilaku Berisiko

Deskripsi: Pemantauan sistematis, ancaman tersirat, atau pola perilaku yang secara objektif menunjukkan peningkatan intrusi dan intimidasi terhadap korban. Melibatkan ancaman emosional, pelecehan *nonverbal*, atau pola perilaku yang menimbulkan intimidasi nyata. Persistensi tinggi; intrusi signifikan; tujuan mengawasi atau mengintimidasi; dampak *psikologis* mulai nyata (Aulia Ansar, 2022). Memiliki relevansi pidana yang lebih kuat apabila fakta konkret memenuhi unsur delik tertentu, seperti ancaman, akses ilegal, atau pelanggaran terhadap ketentuan lain yang relevan. Dampak berupa rasa takut atau terganggunya rasa aman dapat menjadi fakta pendukung dalam menilai tingkat keseriusan perilaku, tetapi tidak dengan sendirinya menentukan adanya tindak pidana. Implikasi Etis: Pelanggaran berat terhadap martabat dan keamanan *psikologis*. Pelanggaran privasi: tinggi, melibatkan pengawasan terhadap rutinitas dan kehidupan pribadi korban.

D. Tingkat IV – Perilaku Berisiko Tinggi

Deskripsi: Perilaku pada tingkat ini menunjukkan keterlibatan perbuatan konkret yang secara lebih kuat dapat bersinggungan dengan ketentuan pidana tertentu, seperti pengancaman, pemerasan, akses ilegal, atau pelanggaran ketentuan mengenai data pribadi, sepanjang unsur delik yang bersangkutan terpenuhi. Persistensi sangat tinggi; intrusi berat; intimidasi atau ancaman serius; dampak terhadap keamanan korban. Berpotensi kuat memenuhi satu atau lebih delik yang telah diatur dalam hukum positif, tetapi kualifikasi pidana tetap bergantung pada terpenuhinya unsur delik yang relevan (Afrida et al., 2023). Implikasi Etis: Pelanggaran etis yang sangat berat terhadap keamanan fisik dan *psikologis* korban. Pelanggaran privasi: sangat berat, mencakup pelanggaran kedaulatan individu atas data dan ruang hidupnya.

E. Analisis perspektif hukum pidana Islam terhadap perilaku cyberstalking.

Hukum pidana Islam (*fiqh jinayah*) mengklasifikasikan tindak pidana (*jarimah*) ke dalam tiga kategori, yaitu *jarimah hudud*, *jarimah qisas-diyat*, dan

jarimah ta'zir, yang perbedaannya terletak pada sumber dan kepastian jenis sanksi (Muslich, 2005). *Jarimah hudud* dan *qisas-diyat* memiliki dasar serta kadar hukuman yang telah ditentukan secara pasti oleh *nash syariat*, sedangkan *jarimah ta'zir* mencakup seluruh bentuk maksiat yang kadar sanksinya tidak ditentukan oleh *nash*, sehingga penentuan bentuk dan berat sanksi diserahkan kepada *ulil amri* (penguasa atau hakim) melalui *ijtihad*, dengan tujuan menegakkan keadilan, mendidik pelaku (*tadrib*), sekaligus mewujudkan *kemaslahatan* masyarakat (Zulfadli et al., 2024). Dalam perspektif hukum pidana Islam, *cyberstalking* dapat dikualifikasikan sebagai *jarimah ta'zir* sepanjang perbuatannya memenuhi karakteristik *kemudaratan* yang tidak termasuk dalam *jarimah* yang telah ditentukan secara khusus oleh *nash*. Sejumlah unsur perbuatan *cyberstalking* dapat dikaitkan dengan nilai-nilai yang secara tegas dilindungi dalam *maqashid syariah*, khususnya *hifz al-nafs* (pemeliharaan jiwa) (Rustamovich et al., 2025) dan *hifz al-'ird* (pemeliharaan kehormatan) (Munifah & Mulyo, 2025). Prinsip *hurmah* kesucian atau ketidakbolehan mengganggu yang melekat pada diri, tempat, dan waktu tertentu dalam tradisi hukum Islam turut memperkuat argumen bahwa privasi dan ketenteraman seseorang merupakan objek hukum yang wajib dilindungi negara (Sherwani, 2018).

Prinsip Syariah	Relevansi
Larangan <i>tajassus</i>	Melarang memata-matai dan mengumpulkan informasi pribadi tanpa hak
<i>Hifz al-nafs</i>	Melindungi keamanan dan ketenteraman psikologis korban
<i>Hifz al-'ird</i>	Melindungi kehormatan dan reputasi korban
<i>Jarimah ta'zir</i>	Memberikan fleksibilitas penjatuhan sanksi terhadap bentuk kejahatan baru

Tabel 6. Relevansi Prinsip Hukum Pidana Islam terhadap Cyberstalking

Konsep *ta'zir* menawarkan *fleksibilitas normatif* yang justru dapat menjadi jawaban metodologis atas permasalahan yang dihadapi hukum positif (Sulistiyawati et al., 2025): karena sanksinya tidak dipatok secara kaku oleh *nash*, hakim atau penguasa dapat menyesuaikan bentuk dan berat sanksi dengan karakteristik perbuatan *cyberstalking* yang terus berkembang

mengikuti modus teknologi, selama tujuannya tetap berorientasi pada *kemaslahatan* dan perlindungan korban (Darsi & Husairi, 2019).

Fleksibilitas konsep *jarimah ta'zir* menunjukkan bahwa hukum pidana Islam tidak mensyaratkan bentuk perbuatan tertentu agar dapat dijatuhi sanksi. Selama suatu perbuatan terbukti menimbulkan *kemudharatan*, mengganggu ketenteraman, atau mengancam kehormatan seseorang, negara memiliki kewenangan untuk menentukan bentuk pidana yang proporsional (Muslich, 2005). Pendekatan ini memberikan inspirasi bahwa pembaruan hukum nasional juga perlu memberikan ruang bagi pengaturan *cyberstalking* yang adaptif terhadap perkembangan teknologi tanpa harus menunggu munculnya modus baru. Dengan demikian, hukum pidana Islam tidak menawarkan definisi teknis yang siap pakai untuk *cyberstalking*, melainkan kerangka *aksiologis* perlindungan jiwa, kehormatan, dan privasi yang dapat memperkaya pertimbangan pembentuk undang-undang dalam merumuskan batas antara gangguan biasa dan tindak pidana.

Kesimpulan

Sintesis atas ketiga temuan di atas memperlihatkan bahwa persoalan pokok pengaturan *cyberstalking* di Indonesia tidak terletak pada ketiadaan ketentuan pidana yang dapat digunakan sama sekali, melainkan pada belum adanya rumusan delik yang secara khusus mengakomodasi *cyberstalking* sebagai satu kesatuan pola perilaku, sehingga penanganannya masih bergantung pada berbagai ketentuan pidana yang bersifat *parsial*. Perbandingan dengan negara lain menegaskan bahwa solusi yang lazim ditempuh adalah perumusan definisi *eksplisit* berbasis pola perbuatan berulang, disertai mekanisme perlindungan *preventif* seperti perintah perlindungan digital. Perspektif hukum pidana Islam, melalui konsep *jarimah ta'zir*, menyumbangkan landasan *aksiologis* bahwa perlindungan kehormatan dan ketenteraman *psikologis* korban merupakan kepentingan hukum yang sah untuk dilindungi meskipun tidak selalu disertai ancaman kekerasan yang *eksplisit*, sebuah prinsip yang dapat memperkuat argumen kebijakan bagi perluasan cakupan norma dalam pembaruan UU ITE maupun dalam

peraturan pelaksana UU TPKS. Temuan penelitian menunjukkan bahwa persoalan utama bukanlah ketiadaan norma, melainkan ketidaksesuaian konstruksi delik yang ada dengan karakter *cyberstalking* sebagai pola perilaku berulang. Oleh sebab itu, pembaruan hukum tidak cukup dilakukan melalui penambahan ancaman pidana, tetapi juga melalui perubahan *paradigma* pengaturan yang mengakui *pattern of conduct* sebagai unsur utama *cyberstalking*.

Atas dasar sintesis tersebut, penelitian ini merekomendasikan tiga langkah kebijakan. Pertama, merumuskan definisi *cyberstalking* yang *eksplisit* dan berbasis pola perbuatan berulang dalam agenda pembaruan peraturan perundang-undangan, baik melalui revisi UU ITE maupun peraturan pelaksana UU TPKS. Kedua, mengintegrasikan nilai *kemaslahatan* dan perlindungan kehormatan dari hukum pidana Islam sebagai bahan pertimbangan *aksiologis* dalam perumusan kebijakan, tanpa mengurangi karakter hukum positif yang berlaku secara nasional. Ketiga, memperkuat kapasitas aparat penegak hukum serta mekanisme pelaporan dan perlindungan korban, termasuk mempertimbangkan instrumen perlindungan *preventif* sebagaimana dipraktikkan di sejumlah negara lain.

Daftar Pustaka

- Afrida, D. T., Ismansyah, & Elda, E. (2023, Juni). Sekstorsi Sebagai Tindak Pidana Kekerasan Seksual Berbasis Elektronik dalam Sistem Hukum di Indonesia. *Jurnal Hukum Pidana dan Kriminologi : DELICTI*, 1(1), 11-26. <https://doi.org/10.25077/delicti.v.1.i.1.p.11-26.2023>
- Ali, Z. (2010). *Metode Penelitian Hukum* (1st ed.). Jakarta: Sinar Grafika.
- Andespitrikasih, L., Waluyo, B., & Harefa, B. (2024, Juni). Legal Protection for Victims of Cyberstalking According to Indonesia's Law. *International Journal of Social Science and Human Research*, 7(6), 3732-3736. <https://doi.org/10.47191/ijsshr/v7-i06-23>
- Anisah, A. P., & Nurisman, E. (2022, April). Cyberstalking: Kejahatan Terhadap Perlindungan Data Pribadi Sebagai Pemicu Tindak Pidana. *Krtha Bhayangkara*, 16(1), 163-176. <https://doi.org/10.31599/krtha.v16i1.1203>

- Arianto, R. F., & Prasetyo, B. (2025). Keadilan Restoratif sebagai Solusi Alternatif Penanganan Tindak Pidana di Era Digital. *Legalite : Jurnal Perundang-Undangan Dan Hukum Pidana Islam*, 10(1), 167. <https://doi.org/10.32505/legalite.v10i1.11381>
- Ariawan, I. G. K. (2013, Desember). Metode Penelitian Hukum Normatif. *Jurnal Ilmu Hukum*, 1(1), 27-29. <https://doi.org/10.37637/kw.v1i1.419>
- Audrina, Washington, V., Harianto, S. K., Manjali, R., & Nadia, A. (2024). *Refleksi Satu Dekade 2014–2024: Menuju Transformasi Digital yang Bermakna* (1st ed.). Kemkominfo.
- Aulia Ansar, A. N. (2022, Mei). Pengaruh Aplikasi Pelacak Lokasi Terhadap Keamanan Privasi Pengguna Media Sosial. *Nomos : Jurnal Penelitian Ilmu Hukum*, 2(3), 112-120. <https://doi.org/10.56393/nomos.v1i5.599>
- Budianto Pansariadi, R. S., & Soekorini, N. (2023, Desember). Tindak Pidana Cybercrime dan Penegakan Hukumnya. *Binamulia Hukum*, 12(2), 288-296. <https://doi.org/10.37893/jbh.v12i2.605>
- Darsi, D., & Husairi, H. (2019, Januari). Ta'zir dalam Perspektif Fiqh Jinayat. *Al-Qisthu: Jurnal Kajian Ilmu-ilmu Hukum*, 16(2), 60-64. <https://doi.org/10.32694/010500>
- Disemadi, H. S. (2022, Desember). Lensa Penelitian Hukum: Esai Deskriptif tentang Metodologi Penelitian Hukum. *Journal of Judicial Review*, 24(2), 298-300. <https://doi.org/10.37253/jjr.v24i2.7280>
- Djarawula, M., Alfiani, N., & Mayasari, H. (2023, Juni). Tinjauan Yuridis Tindak Pidana Kejahatan Teknologi Informasi (Cybercrime) di Indonesia Ditinjau dari Perspektif Undang-Undang No. 11. Thn. 2008 Tentang Informasi dan Transaksi Elektronik. *Jurnal Cakrawala Ilmiah*, 2(10), 3801. <https://doi.org/10.53625/jcijurnalcakrawalailmiah.v2i10.5842>
- Efendi, J., & Ibrahim, J. (2018). *Metode Penelitian Hukum Normatif dan Empiris* (1st ed.). Depok: Prenada Media Group.
- Fauzan, A. M., Mudjrimin, J., & Sulfikar, S. (2025, Juni). Kejahatan Dunia Maya (Cybercrime) dalam Perspektif Hukum Islam dan Hukum Positif Masyarakat di Indonesia. *Bayt Al Hikmah: Jurnal Pendidikan Dan Pengembangan Masyarakat Islam*, 1(1), 143-153. <https://doi.org/10.54065/BaytAl-Hikmah.414>

- Firmansyah, A., Setiawan, D., Pratama, F., Marwan, T., Almanda, A., Oktarianda, S., Zulkarnen, Satrio, I., Saputra, I., Juna, A. M., & Rohman. (2024, Juni). Putusan Pengadilan Sebagai Sumber Hukum Yurisprudensi. *Wathan: Jurnal Ilmu Sosial Dan Humaniora*, 1(2), 137-140. <https://doi.org/10.71153/wathan.v1i2.79>
- Gopinath, M. (2026, Maret). Reconceptualising cyberstalking regulation in India: From a disjointed legal framework to proactive digital safety governance. *International Journal of Law*, 12(1), 383-392. <https://www.lawjournals.org/assets/archives/2026/vol12issue1/12074.pdf>
- Habibi, Rokhman, M., & Liviani, I. (2020, Desember). Kejahatan Teknologi Informasi (Cyber Crime) dan Penanggulangannya dalam Sistem Hukum Indonesia. *Al-Qanun: Jurnal Pemikiran dan Pembaharuan Hukum Islam*, 23(2), 401-407. <https://doi.org/10.15642/alqanun.2020.23.2.400-426>
- Harasgama, K., & Munasinghe, P. (2021, Agustus). A Comparative Analysis of Cyberstalking Legislations in the UK, Singapore and Sri Lanka. *SSRN Electronic Journal*, 2-10. <https://doi.org/10.2139/ssrn.3903800>
- Hartanto, Hakimi, A. C., & Munawar, S. (2024, April). Perbandingan Sanksi Pidana Pasal Tertentu Undang-Undang Informasi dan Transaksi Elektronik (UU Iti No.11 Tahun 2008 Dengan No 19 Tahun 2016): Comparison Of Criminal Sanctions For Certain Article Of The Information And Electronic Transactions Law (UU Iti No. *Journal of Presumption of Law*, 6(1), 33-48. <https://doi.org/10.31949/jpl.v6i1.4613>
- Hutasoit, R. R., & Kurniawan, R. (2024, Juli). Tinjauan Yuridis Perlindungan Korban Terhadap Kejahatan Cyber Bullying Dalam Sistem Hukum Pidana Indonesia. *Jurnal Yuridis Unaja*, 7(1), 40-48. <https://doi.org/10.35141/jyu.v7i1.1089>
- Inaya, A. N., & Yazid, I. (2025, Desember). Cyberstalking Crime in The Perspective of Islamic Criminal Law. *Journal Mercatoria*, 18(2), 122-132. <https://doi.org/10.31289/mercatoria.v18i2.16652>
- Kartono, Lagustiani, S. H., Koesoemo, S., Santoso PN, S., & Sosiawan, U. M. (2026, Juni). The Criminalization of Stalking in Indonesia: Assessing the Urgency and Formulation of a New Criminal Offense Under the National Criminal Code and a Comparative Analysis with Common Law Countries. *Tec Empresarial Journal*, 21(2), 14-36. https://revistas.tec-ac.cr/index.php/tec_empresarial/article

Kitab Undang-Undang Hukum Pidana.

Komisi Nasional Anti Kekerasan terhadap Perempuan (Komnas Perempuan). Catatan Tahunan (CATAHU) 2025: Kekerasan Berbasis Gender terhadap Perempuan. Jakarta: Komnas Perempuan, 2026.

Komnas Perempuan. "Siaran Pers Komnas Perempuan tentang Penyelesaian Dugaan Pelecehan Seksual Berbasis Online di Lingkungan Kampus." 2026.

Liawi, A. A., Sofyan, A. M., & Mirzana, H. A. (2023, Agustus). Kebijakan Hukum Pidana Terhadap Kejahatan Penguntitan Berbasis Elektronik Untuk Tujuan Seksual. *Alauddin Law Development Journal*, 5(2), 246-257. <https://doi.org/10.24252/aldev.v5i2.35504>

Marzuki, P. M. (2017). *Penelitian Hukum: Edisi Revisi* (13th ed.). Jakarta: Kencana.

Zulfadli, Efendi, S., Akbar, K., Syaf, M. N., Hasibuan, K., Gozali, M., Mas'odi, Naitboho, Y. R., Naisabur, N., & HS, D. E. R. (2024). *Fiqih Jinayah*. Pena Cendekia Pustaka.

Efendi, S., Majida, A. Z., Soraya, J., Abdurrachman, H., Halim, S. L., Subarkah, A. D., Tjahjadi, D. P., Purwati, A., Rahman, M. A., Juita, S. R., & Hermanto, B. (2026). *Hukum Cyber: Tantangan dan Solusi di Era Digital*. Adikara Cipta Aksa.

Munifah, & Mulyo, M. T. (2025, April). Personal Data Hacking: A Critical Analysis of Islamic Criminal Law and Islamic Jurisprudence. *Ulul Albab: Jurnal Studi dan Penelitian Hukum Islam*, 8(2), 180-194. <https://doi.org/10.30659/jua.v8i2.44585>

Muslich, A. W. (2005). *Hukum pidana Islam* (1st ed.). Jakarta: Sinar Grafika.

Pratama, A. Y., Dzaky N. Br, H. A., Rosyid, A. N., Astinda, & Adhipradana, Y. A. (2024, Desember). Penegakan Tindak Pidana Cyberstalking Dalam Hukum Positif Indonesia. *Legal Standing: Jurnal Ilmu Hukum*, 8(3), 698-708. <https://doi.org/10.24269/ls.v8i3.10320>

Purnama, Y. F., Herman, & Haris, O. K. (2024, April). Cyberstalking sebagai Perbuatan Melawan Hukum dalam Hukum Pidana Indonesia. *Halu Oleo Legal Research*, 6(1), 103-121. <https://doi.org/10.33772/holresch.v6i1.813>

Putusan Mahkamah Agung Nomor 3635 K/Pid.Sus/2022.

Putusan Mahkamah Konstitusi Nomor 50/PUU-VI/2008.

Putusan Pengadilan Negeri Surabaya Nomor 1842/Pid.Sus/2024/PN Sby.

R. Syailendra, M., Fitzgerald, S. E., & Santoso, M. (2023, Februari). Sosialisasi Perlindungan Data Pribadi Bagi Masyarakat Kabupaten Indramayu. *Jurnal Serina Abdimas*, 1(1), 157-165.
<https://doi.org/10.24912/jsa.v1i1.23845>

Rumlus, M. H., Kusmiadi, M. E., Rajab, A. M., & Pamungkas, A. C. (2023, Juli). Kebijakan penanggulangan tindak pidana cyberstalking pada media elektronik. *Equality Before The Law*, 3(2), 102-113.
<https://doi.org/10.36232/equalitybeforethelaw.v3i2.461>

Rustamovich, B. I., Khoshim ugli, M. F., & Al-Fatih, S. (2025, Juni). Right to Privacy in the Development of Digital Technologies. *International Journal of Law and Society*, 4(1), 131-140.
<https://doi.org/10.59683/ijls.v4i1.171>

Sherwani, M. (2018, Juni). The Right to Privacy under International Law and Islamic Law. *Kardan Journal of Social Sciences and Humanities*, 1(1), 30-48. 10.31841/KJSSH.2021.14

Sinaga, A. B., Usman, & Wahyudhi, D. (2021, Oktober). Perbuatan Menguntit (Stalking) dalam Perspektif Kebijakan Hukum Pidana Indonesia. *PAMPAS: Journal of Criminal Law*, 2(2), 16-21.
<https://doi.org/10.22437/pampas.v2i2.13715>

Soekanto, S., & Mamudji, S. (2001). *Penelitian Hukum Normatif* (1st ed.). Jakarta: Raja Grafindo Persada.

Sulistiyawati, E., Rahmah, S., & Lahmudinur. (2025, November). Jarimah Ta'zir Menurut Perspektif Hukum Pidana Islam. *Ahsan: Jurnal Ilmiah Keislaman Dan Kemasyarakatan*, 2(2), 191-201.
<https://doi.org/10.67802/ahsan.vi.63>

Undang-Undang Dasar Negara Republik Indonesia Tahun 1945.

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

Undang-Undang Nomor 1 Tahun 2024 tentang Perubahan Kedua atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik.

Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik.

Undang-Undang Nomor 12 Tahun 2022 tentang Tindak Pidana Kekerasan Seksual.

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

Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi.

Undang-Undang Nomor 8 Tahun 1981 tentang Hukum Acara Pidana.

Wahyuningsih, K. R. (2025, Mei). Cyberstalking sebagai Kejahatan Multidimensional. *Jurnal Hukum, Administrasi Publik Dan Negara*, 2(3), 129-130. <https://doi.org/10.62383/hukum.v2i3.273>

Wanantho, R., Irawan, D., & Burlian, P. (2024, Desember). Tindak Pidana Cyberstalking di Media Sosial Menurut Perspektif Hukum Pidana Islam. *Journal of Sharia and Legal Science*, 2(3), 439-451. <https://doi.org/10.61994/jsls.v2i3.866>

Winarno, A., Sugiri, B., & Cholil, Y. (2021, Oktober 341-372). Kekaburan Norma dalam Pasal 55 Undang-Undang Nomor 24 Tahun 2011 tentang Badan Penyelenggaraan Jaminan Sosial. *Media Iuris*, 4(3). <https://doi.org/10.20473/mi.v4i3.29023>

Zaki, M. M. (2022, Mei). Aspek Pidana Cyberstalking Sebagai Salah Satu Bentuk Cybercrime. *Jurist-Diction*, 5(3), 974-987. <https://doi.org/10.20473/jd.v5i3.35790>