

Cyberstalking sebagai Kejahatan Multidimensional

Ketut Ratri Wahyuningsih

Fakultas Hukum dan Ilmu Sosial, Universitas Pendidikan Ganesha Singaraja, Indonesia

Korespondensi penulis: ratri@student.undiksha.ac.id

Abstract. *The rapid development of information technology has brought various conveniences to human life, but it also brings new challenges in the form of cybercrime threats. One of these threats is cyberstalking, which is the act of stalking, harassment, or threats through digital media. Cyberstalking utilizes the anonymity of technology to violate the privacy, dignity, and psychological safety of the victim. In Indonesia, the regulation of cyberstalking is implicitly regulated through Law Number 11 of 2008 concerning Electronic Information and Transactions (ITE Law) or in its latest amendment, namely in Law Number 1 of 2024 concerning the Second Amendment to Law Number 1 of 2008 concerning Electronic Information and Transactions and the Criminal Code (KUHP). However, these regulations have not been able to cover the multidimensional dimensions of the crime, such as non-verbal harassment or emotional threats through digital media. This article analyzes cyberstalking in the perspective of Indonesian criminal law by highlighting the existing legal vacuum and the importance of regulatory reform based on the principles of legality, legal certainty, and protection of individual rights. Recommendations include revising the ITE Law, strengthening the capacity of law enforcers, and increasing public awareness to deal holistically with the threat of cyberstalking. With these steps, it is hoped that legal protection for victims can be improved in line with technological developments.*

Keywords: Criminal Law, Cyber Crime, Cyberstalking, ITE Law, Legal Protection.

Abstrak. Perkembangan teknologi informasi yang pesat telah menghadirkan berbagai kemudahan dalam kehidupan manusia, tetapi juga membawa tantangan baru berupa ancaman kejahatan siber. Salah satu bentuk ancaman tersebut adalah *cyberstalking* yaitu tindakan penguntitan, pelecehan, atau ancaman melalui media digital. *Cyberstalking* memanfaatkan anonimitas teknologi untuk melakukan pelanggaran terhadap privasi, martabat, dan keamanan psikologis korban. Di Indonesia pengaturan *cyberstalking* secara implisit diatur melalui Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik (UU ITE) atau dalam perubahan terakhirnya yaitu dalam Undang-Undang Nomor 1 Tahun 2024 Tentang Perubahan Kedua Atas Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik serta Kitab Undang-Undang Hukum Pidana (KUHP). Namun regulasi ini belum mampu mencakup dimensi kejahatan yang bersifat multidimensional, seperti pelecehan non-verbal atau ancaman emosional melalui media digital. Artikel ini menganalisis *cyberstalking* dalam perspektif hukum pidana Indonesia dengan menyoroti kekosongan hukum yang ada dan pentingnya pembaruan regulasi berbasis prinsip legalitas, kepastian hukum, dan perlindungan hak individu. Rekomendasi yang diajukan meliputi revisi UU ITE, penguatan kapasitas penegak hukum, dan peningkatan kesadaran masyarakat untuk menghadapi ancaman *cyberstalking* secara holistik. Dengan langkah-langkah tersebut diharapkan perlindungan hukum terhadap korban dapat ditingkatkan sejalan dengan perkembangan teknologi.

Kata Kunci: Hukum Pidana, Cyber Crime, Cyberstalking, UU ITE, Perlindungan Hukum.

1. PENDAHULUAN

Di era digital teknologi informasi telah menjadi bagian integral dari kehidupan manusia mengubah cara berkomunikasi, berinteraksi, dan menjalankan aktivitas sehari-hari. Internet dan media sosial membuka peluang besar untuk kemajuan di berbagai bidang tetapi di sisi lain juga menciptakan ruang baru bagi kejahatan salah satunya adalah *cyberstalking*. *Cyberstalking* merupakan tindakan penguntitan yang dilakukan melalui media digital dengan tujuan mengganggu, mengancam, atau melecehkan individu. Kejahatan ini memanfaatkan sifat

anonim dari teknologi digital sehingga pelaku dapat bertindak tanpa diketahui identitasnya secara langsung.

Cyberstalking membawa dampak serius bagi korban tidak hanya dalam bentuk pelanggaran privasi tetapi juga gangguan psikologis seperti kecemasan, stres, hingga trauma. Tindakan ini dapat, hingga trauma. Tindakan ini dapat merusak martabat korban, reputasi sosial, dan bahkan berdampak pada keamanan fisik jika ancaman yang dibuat berlanjut ke dunia nyata. Fenomena ini juga menimbulkan implikasi hukum yang kompleks mengingat kejahatan ini sering kali sulit diidentifikasi dan dibuktikan terutama dalam konteks bukti digital yang dapat dengan mudah dihapus atau dimanipulasi.

Cyberstalking di Indonesia diatur secara implisit dalam beberapa peraturan seperti UU No. 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik yang telah diperbarui dengan UU No. 19 Tahun 2016 dan perubahan yang terakhir yaitu UU No. 1 Tahun 2024 serta KUHP. Pasal 27B dan pasal 29 UU ITE misalnya, mengatur tentang ancaman dan pelecehan melalui media elektronik. Namun, regulasi ini belum mencakup seluruh dimensi *cyberstalking* seperti pelecehan non-verbal yang tidak disertai ancaman eksplisit. Kekosongan hukum ini menimbulkan tantangan besar bagi aparat penegak hukum untuk memberikan perlindungan yang memadai bagi korban.

Prinsip legalitas dalam hukum pidana menuntut adanya pengaturan yang jelas untuk menjamin keadilan dan kepastian hukum. Selain itu asas perlindungan hukum menempatkan korban sebagai subjek yang harus mendapatkan jaminan keamanan dan keadilan dari negara. Artikel ini bertujuan untuk menganalisis pengaturan *cyberstalking* dalam sistem hukum pidana Indonesia, mengidentifikasi kekosongan regulasi, serta memberikan rekomendasi langkah-langkah hukum yang relevan untuk menangani kejahatan ini di era digital.

2. METODE PENELITIAN

Metode penelitian yang digunakan dalam artikel ini adalah hukum normatif dengan pendekatan peraturan perundang-undangan (*statute approach*) dan pendekatan konsep (*conceptual approach*). Pendekatan perundang-undangan dilakukan dengan mengkaji regulasi terkait seperti UU ITE Nomor 11 Tahun 2008 beserta perubahannya dalam UU Nomor 1 Tahun 2024 serta Kitab Undang-Undang Hukum Pidana (KUHP). Analisis ini bertujuan untuk mengidentifikasi pengaturan hukum *cyberstalking* dan mengevaluasi kesesuaiannya dengan asas legalitas dan kepastian hukum. Pendekatan konsep digunakan untuk memahami fenomena *cyberstalking* sebagai bentuk kejahatan multidimensional dalam sistem hukum pidana Indonesia. Melalui pendekatan ini penelitian menggali prinsip-prinsip hukum pidana yang relevan seperti perlindungan hak individu, keadilan, dan keseimbangan antara

kepentingan negara dan masyarakat. Kombinasi kedua pendekatan ini bertujuan untuk memberikan solusi hukum yang efektif dalam menghadapi ancaman *cyberstalking* di era digital.

3. PEMBAHASAN

Pengaturan Tindak Pidana Cyberstalking dalam UU ITE dan KUHP

Cyberstalking merupakan salah satu bentuk kejahatan siber yang terus meningkat seiring dengan perkembangan teknologi digital. Di Indonesia pengaturan hukum terhadap kejahatan ini menggunakan pendekatan regulasi melalui Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE) yang telah mengalami perubahan dengan Undang-Undang Nomor 1 Tahun 2024, serta melalui Kitab Undang-Undang Hukum Pidana (KUHP). Namun meskipun terdapat regulasi tersebut efektivitas pengaturan ini sering kali dipertanyakan karena adanya tantangan dalam aspek legalitas dan kepastian hukum terutama dalam konteks kejahatan multidimensional seperti *cyberstalking*.

UU ITE menjadi landasan utama dalam menjerat pelaku *cyberstalking* di Indonesia.

Pasal 27B ayat (1) Undang-Undang Nomor 1 Tahun 2024 mengatur bahwa “Setiap orang dengan sengaja dan tanpa hak mendistribusikan dan/atau mentransmisikan Informasi Elektronik dan/atau Dokumen Elektronik, dengan maksud untuk menguntungkan diri sendiri atau orang lain secara melawan hukum, memaksa orang dengan ancaman kekerasan untuk:

- a. memberikan suatu barang, yang sebagian atau seluruhnya milik orang tersebut atau milik orang lain; atau
- b. memberi utang, membuat pengakuan utang, atau menghapuskan piutang.”

Hukuman pidana sebagaimana diatur dalam pasal ini adalah pidana penjara maksimal enam tahun dan/atau pidana denda paling banyak sebesar Rp 1.000.000.000,00 (satu miliar rupiah). Elemen penting yang menjadi fokus dalam pasal ini adalah adanya ancaman kekerasan yang dilakukan melalui informasi elektronik yang berpotensi menimbulkan rasa takut, cemas, atau khawatir pada korban. Selain itu pada pasal 29 jo. pasal 45B UU ITE juga memberikan dasar hukum yang lebih spesifik untuk menindak pelaku *cyberstalking*. Pasal 29 jika dijelaskan secara lebih rinci menyatakan bahwa siapa pun yang dengan sengaja dan tanpa hak menyampaikan Informasi Elektronik atau Dokumen Elektronik yang mengandung ancaman kekerasan atau menakut-nakuti secara langsung kepada orang lain akan dikenai ketentuan hukum. Pelanggaran terhadap pasal ini diancam dengan pidana penjara paling lama empat (4) tahun dan/atau denda paling banyak Rp 750.000.000,00 (tujuh ratus lima puluh juta rupiah). Ketentuan ini mencakup pengiriman informasi elektronik yang berisi intimidasi langsung kepada korban baik secara eksplisit maupun implisit yang bertujuan untuk menakut-nakuti atau

menciptakan tekanan psikologis. Namun pengaturan dalam UU ITE ini memiliki keterbatasan dalam mencakup dimensi pelecehan non-verbal atau ancaman emosional yang sering kali menjadi bagian dari kejahatan *cyberstalking* (Purnama, 2024). Regulasi saat ini lebih berfokus pada ancaman eksplisit yang dapat dibuktikan secara langsung sementara intimidasi yang bersifat psikologis atau emosional belum mendapatkan perhatian yang memadai. Tantangan ini semakin diperumit dengan sifat bukti digital yang efemeris dan mudah dimanipulasi yang membuat proses pembuktian dalam kasus *cyberstalking* menjadi lebih sulit.

Selain UU ITE, KUHP juga memberikan landasan hukum untuk menjerat pelaku *cyberstalking*. Dalam KUHP yang berlaku saat ini pasal 368 mengatur pemerasan dengan kekerasan atau ancaman kekerasan dengan ancaman pidana penjara paling lama sembilan (9) tahun. Pasal ini menjelaskan bahwa siapa pun yang dengan sengaja bermaksud menguntungkan diri sendiri atau orang lain secara melawan hukum, memaksa orang lain menggunakan kekerasan atau ancaman kekerasan untuk menyerahkan barang miliknya atau milik orang lain, memberikan pinjaman, atau menghapuskan utang, dapat dikenai hukuman. Meskipun pasal ini tidak secara spesifik menyebutkan kejahatan berbasis digital unsur ancaman kekerasan yang diatur di dalamnya dapat diterapkan pada kasus *cyberstalking* yang melibatkan ancaman eksplisit kepada korban (Juharwati, 2024). Pada KUHP yang baru yang diatur dalam Undang-Undang Nomor 1 Tahun 2023, pasal 448 memberikan pengaturan yang lebih relevan dengan konteks kejahatan digital. Bunyi pasal 448 adalah “Dipidana dengan pidana penjara paling lama satu (1) tahun atau pidana denda paling banyak Rp10.000.000,00 (sepuluh juta rupiah) setiap orang yang:

- (a) secara melawan hukum memaksa orang lain supaya melakukan, tidak melakukan, atau membiarkan sesuatu, dengan kekerasan atau ancaman kekerasan, baik terhadap orang itu sendiri maupun orang lain; atau
- (b) memaksa orang lain supaya melakukan, tidak melakukan, atau membiarkan sesuatu dengan ancaman pencemaran atau pencemaran tertulis.”

Ketentuan ini mencerminkan upaya untuk memperluas cakupan hukum terhadap kejahatan berbasis digital meskipun implementasinya masih memerlukan waktu hingga efektif berlaku pada tahun 2026.

Cyberstalking disebut sebagai kejahatan multidimensional karena mencakup berbagai aspek yang saling berkaitan yaitu aspek psikologis, sosial, dan hukum. Dari sisi psikologis korban *cyberstalking* sering kali mengalami kecemasan, stres, dan trauma akibat ancaman atau pelecehan yang dilakukan secara terus-menerus melalui media digital. Ancaman yang tidak hanya bersifat fisik tetapi juga emosional ini dapat merusak keseimbangan mental korban dan

berdampak pada kualitas hidup mereka. Dari sisi sosial, *cyberstalking* memiliki potensi untuk merusak reputasi korban di lingkungan sosial. Pelaku dapat menggunakan media sosial untuk menyebarkan informasi palsu, mengintimidasi korban, atau bahkan mengisolasi korban dari jaringan sosialnya. Dari sisi hukum tantangan utama dalam menangani kasus *cyberstalking* adalah anonimitas pelaku dan sifat lintas batas dari kejahatan ini. Pelaku sering kali menggunakan akun anonim untuk melakukan ancaman atau pelecehan sehingga sulit diidentifikasi oleh aparat penegak hukum. Selain itu regulasi yang ada belum sepenuhnya mencakup dimensi pelecehan non-verbal atau intimidasi psikologis yang sering kali menjadi bagian penting dari kejahatan ini.

Bentuk Perlindungan Hukum yang Ideal bagi Korban Cyberstalking Sesuai Dengan Prinsip Keadilan, Perlindungan Hak Individu, dan Penegakan Hukum yang Responsif

Cyberstalking sebagai kejahatan berbasis digital telah menimbulkan permasalahan yang signifikan dalam sistem hukum di Indonesia. Dalam konteks perlindungan hukum pendekatan yang ideal harus berlandaskan pada prinsip keadilan, penghormatan terhadap hak individu, serta penegakan hukum yang efektif dan responsif. Landasan ini harus diwujudkan melalui penguatan regulasi, penegakan hukum yang profesional, dan pengintegrasian layanan pendukung bagi korban. Perlindungan hukum yang ideal harus berlandaskan pada prinsip keadilan seperti yang diatur pada UUD 1945 pasal 28D ayat (1), yang menjelaskan bahwa setiap individu memiliki hak untuk diakui, dijamin, dilindungi, dan mendapatkan kepastian hukum yang adil serta diperlakukan setara di hadapan hukum. Korban *cyberstalking* harus diposisikan sebagai subjek hukum yang berhak atas perlindungan penuh termasuk akses terhadap mekanisme hukum yang ramah korban. Hal ini mencakup penyediaan layanan bantuan hukum yang mudah diakses, mekanisme pelaporan yang sederhana, serta penguatan peran lembaga perlindungan saksi dan korban sebagaimana diatur dalam Undang-Undang Nomor 13 Tahun 2006 tentang Perlindungan Saksi dan Korban. Selain itu hak individu untuk mendapatkan rasa aman sebagaimana dijamin dalam pasal 28G ayat (1) UUD 1945 harus diwujudkan melalui pengaturan perlindungan privasi dan data pribadi korban. Dalam hal ini UU No. 27 Tahun 2022 tentang Perlindungan Data Pribadi menjadi elemen penting yang harus diintegrasikan dengan UU ITE untuk memberikan perlindungan lebih komprehensif terhadap penyalahgunaan data pribadi korban. Hal ini dianggap penting karena sasaran utama dari kasus kejahatan ini atau *cybercrime* adalah menyerang data pribadi para korban (Azhari, 2019).

Penegakan hukum yang ideal memerlukan kapasitas aparat hukum yang mampu menghadapi tantangan kejahatan digital. Kemampuan untuk mengidentifikasi pelaku yang sering kali menggunakan anonimitas dalam dunia maya menjadi faktor utama. Oleh karena itu penegak hukum perlu dilatih dalam forensik digital termasuk pengelolaan bukti elektronik sesuai dengan ketentuan pasal 184 KUHP tentang alat bukti sah. Kemudian implementasi pasal 43 UU ITE yang mengatur peran pemerintah dalam penegakan hukum siber harus diperkuat. pasal ini menyatakan bahwa “Pemerintah bertanggung jawab untuk memfasilitasi penegakan hukum di bidang informasi dan transaksi elektronik sesuai dengan peraturan perundang-undangan.” Namun hingga saat ini pelaksanaan pasal tersebut masih menghadapi kendala dalam hal ketersediaan sumber daya, teknologi, dan koordinasi lintas lembaga. Oleh karena itu penguatan peran Badan Siber dan Sandi Negara (BSSN) serta kerja sama internasional dalam menangani kejahatan lintas batas menjadi langkah strategis yang harus diprioritaskan.

Perlindungan hukum juga harus mencakup dimensi pemulihan bagi korban. Pemulihan ini mencakup kompensasi finansial, rehabilitasi psikologis, dan pemulihan reputasi korban. Restitusi kepada korban dapat diatur melalui penerapan pasal 98 KUHP yang memungkinkan penggabungan perkara pidana dengan gugatan perdata untuk memberikan ganti rugi kepada korban. Selain itu korban *cyberstalking* sering kali mengalami trauma psikologis yang memerlukan intervensi profesional. Negara harus menyediakan layanan konseling gratis melalui lembaga profesional seperti Pusat Pelayanan Terpadu Perlindungan Perempuan dan Anak (P2TP2A) yang dapat diperluas cakupannya untuk menangani korban kejahatan berbasis digital. Aspek preventif juga menjadi bagian penting dari perlindungan hukum yang ideal. Pemerintah harus meningkatkan literasi digital masyarakat untuk memahami risiko *cyberstalking* dan cara melindungi diri di dunia maya. Edukasi ini dapat dilakukan melalui program-program di bawah Kementerian Komunikasi dan Informatika (KOMINFO) yang didukung oleh kampanye publik dan pelatihan di tingkat komunitas. Selain itu pengaturan yang lebih ketat terhadap platform digital sebagaimana diatur dalam pasal 5 UU ITE yang mewajibkan setiap penyelenggara sistem elektronik untuk memastikan keamanan data dan privasi pengguna, harus diawasi secara ketat. Platform digital harus memiliki mekanisme pelaporan yang cepat dan transparan untuk menangani tindakan *cyberstalking* termasuk penghapusan konten yang bersifat ancaman.

4. KESIMPULAN DAN REKOMENDASI

Kesimpulan

Cyberstalking merupakan salah satu bentuk kejahatan multidimensional yang berkembang seiring dengan kemajuan teknologi informasi. Di Indonesia pengaturan hukum terhadap kejahatan ini masih berada pada tahap awal dengan mengandalkan UU ITE dan KUHP sebagai kerangka hukum utama. Namun regulasi yang ada belum sepenuhnya mampu menjawab kompleksitas dimensi kejahatan ini terutama terkait pelecehan non-verbal dan intimidasi emosional yang sering kali terjadi.

Perlindungan hukum terhadap korban *cyberstalking* membutuhkan pendekatan yang holistik berdasarkan prinsip keadilan, perlindungan hak individu, dan responsivitas hukum. Prinsip keadilan menuntut perlakuan yang setara bagi korban dengan memberikan akses terhadap mekanisme hukum yang ramah dan transparan. Perlindungan hak individu menuntut jaminan terhadap privasi, keamanan, dan pemulihan bagi korban, termasuk perlindungan data pribadi. Selain itu penegakan hukum yang responsif memerlukan peningkatan kapasitas aparat penegak hukum untuk menangani bukti digital serta koordinasi yang lebih baik antar lembaga penegak hukum.

Rekomendasi

Berdasarkan penelitian ini disarankan adanya revisi regulasi yang mencakup dimensi non-verbal dan intimidasi emosional dalam UU ITE serta percepatan implementasi KUHP baru khususnya pasal 448 untuk memberikan perlindungan yang lebih luas terhadap kejahatan berbasis digital. Penegakan hukum juga harus ditingkatkan dengan memberikan pelatihan forensik digital kepada aparat hukum dan memperkuat koordinasi melalui Badan Siber dan Sandi Negara (BSSN). Selain itu literasi digital perlu ditingkatkan melalui kampanye publik untuk meningkatkan kesadaran masyarakat tentang risiko *cyberstalking* dan cara melindungi diri didukung oleh kewajiban platform digital menyediakan mekanisme pelaporan yang efektif. Untuk mendukung pemulihan korban perlu disediakan layanan konseling psikologis gratis dan program rehabilitasi sosial sehingga tercipta sistem hukum yang adaptif, ramah korban, dan responsif terhadap tantangan kejahatan berbasis teknologi informasi.

DAFTAR PUSTAKA

Jurnal dan Publikasi Ilmiah

- Azhari, M. R. (2019). Aspek pidana mayantara (cyberstalking). *Badamai Law Journal*, 4(1), 150.
- Juharwati, R. (2024). Cyberstalking sebagai kejahatan multidimensional: Analisis kekosongan hukum dan tantangan penegakan hukum. Dalam *Prosiding Konferensi Nasional Hukum Siber*.
- Purnama, Y. F. (2024). Tindak pidana cyberstalking dalam perspektif hukum Indonesia: Pendekatan UU ITE dan KUHP. *Jurnal Hukum dan Teknologi*, 5(2).

Peraturan Perundang-Undangan

- Undang-Undang Dasar Negara Republik Indonesia Tahun 1945.
- Undang-Undang Nomor 1 Tahun 2023 tentang Kitab Undang-Undang Hukum Pidana.
- Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik.
- Undang-Undang Nomor 13 Tahun 2006 tentang Perlindungan Saksi dan Korban.
- Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi.
- Undang-Undang Nomor 1 Tahun 2024 tentang Perubahan Kedua atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik.