

Kejahatan *Cyberstalking* Dalam Perspektif Undang-Undang Nomor 1 Tahun 2024 Tentang Informasi dan Transaksi Elektronik

Aswindari Harahap¹, Rahmayanti², Suci Ramadani³, Bambang Agus Pariyono⁴,
Bima Lumbanbatu⁵.

^{1,2,3,4,5} Program Studi Magister Hukum, Pascasarjana, Universitas Pembangunan Panca Budi.
E-mail: siarienmanja@gmail.com (CA)

Abstrak: Pesatnya perkembangan konektivitas digital di Indonesia telah diikuti dengan munculnya berbagai bentuk kejahatan yang memanfaatkan teknologi informasi, salah satunya adalah *cyberstalking*. Penelitian ini bertujuan untuk menganalisis pengaturan hukum *cyberstalking* dalam Undang-Undang Nomor 1 Tahun 2024 tentang Perubahan Kedua atas Undang-Undang Informasi dan Transaksi Elektronik, serta mengkaji pertanggungjawaban pidana terhadap pelaku *cyberstalking* dalam kerangka peraturan tersebut. Penelitian ini menggunakan metode yuridis normatif dengan pendekatan perundang-undangan, pendekatan konseptual, dan pendekatan kasus. Bahan hukum yang digunakan terdiri atas bahan hukum primer berupa peraturan perundang-undangan dan putusan pengadilan, serta bahan hukum sekunder yang diperoleh dari berbagai literatur ilmiah. Hasil penelitian menunjukkan bahwa hukum positif Indonesia belum mengatur *cyberstalking* sebagai tindak pidana yang berdiri sendiri, sehingga penegakan hukumnya masih didasarkan pada kombinasi beberapa ketentuan, terutama Pasal 27A, Pasal 27B, Pasal 29, dan Pasal 26 Undang-Undang ITE, serta ketentuan yang relevan dalam Kitab Undang-Undang Hukum Pidana yang baru. Pertanggungjawaban pidana ditentukan berdasarkan adanya kesengajaan, kemampuan bertanggung jawab pelaku, serta pembuktian yang didukung oleh alat bukti elektronik sebagai instrumen utama. Penelitian ini menyimpulkan bahwa meskipun pengaturan yang berlaku telah memberikan perlindungan yang lebih baik bagi korban dibandingkan pengaturan sebelumnya, masih terdapat kekosongan norma karena karakter *cyberstalking* yang bersifat berulang dan sistematis belum diatur secara eksplisit. Oleh karena itu, diperlukan penyempurnaan regulasi untuk memberikan kepastian hukum dan perlindungan yang lebih efektif bagi korban.

Kata Kunci: *Cybercrime*; *cyberstalking*; informasi elektronik; perlindungan korban; pertanggungjawaban pidana.

Sitasi: Harahap, A., Rahmayanti, R., Ramadani, S., Pariyono, B. A., & Lumbanbatu, B. (2026). Kejahatan *Cyberstalking* Dalam Perspektif Undang-Undang Nomor 1 Tahun 2024 Tentang Informasi dan Transaksi Elektronik. *Locus Journal of Academic Literature Review*, 5(6), 781–791.
<https://doi.org/10.56128/ljoalr.v5i6.1135>

1. Pendahuluan

Teknologi informasi telah mengubah cara masyarakat Indonesia berinteraksi secara fundamental. Mayoritas penduduk Indonesia kini terhubung dengan internet dan

menghabiskan sebagian besar waktunya pada media sosial serta aplikasi pesan instan (APJII, 2024). Transformasi digital ini tidak hanya melahirkan kemudahan, tetapi juga konsekuensi kriminologis yang serius. Holt, Bossler, dan Seigfried-Spellar (2022) menggambarkan bahwa internet telah mentransformasi kejahatan konvensional ke bentuk baru yang lebih sulit dilacak dan berdampak lebih luas. Perkembangan layanan digital, termasuk telemedicine dan rekam medis elektronik, turut memperluas ruang rentan terhadap penyalahgunaan teknologi yang berimplikasi hukum (Rahmayanti & Ramadani, 2024; Ramadani, 2025). Salah satu bentuk kejahatan siber yang kerap luput dari perhatian adalah cyberstalking, yaitu penguntitan yang dilakukan melalui sarana elektronik (Mudzalifah & Pujiyono, 2023).

Cyberstalking merupakan serangkaian perilaku berulang yang memanfaatkan teknologi informasi untuk mengganggu, mengintimidasi, atau menebar ketakutan pada orang lain (Wilson, Sheridan, & Garratt-Reed, 2022). Pelaku dapat memantau aktivitas korban di media sosial, mengirim pesan teror secara terus-menerus, membuat akun palsu, menyebarkan data pribadi korban atau doxing, hingga mengancam menyebarkan konten intim (Marcum & Higgins, 2021). Fenomena ini terbukti nyata di Indonesia Catatan Tahunan Komnas Perempuan secara konsisten menempatkan kekerasan berbasis gender siber, termasuk penguntitan daring, sebagai kejahatan yang laporannya terus meningkat (Komnas Perempuan, 2024). Manipulasi data elektronik sebagai bagian dari kejahatan siber juga telah dibuktikan di hadapan pengadilan, sebagaimana tercermin dalam putusan atas pelaku yang memanipulasi data transaksi digital (Rahmayanti, 2020). Dampaknya terhadap korban meliputi gangguan kecemasan, depresi, dan penurunan kepercayaan sosial (Stevens, Nurse, & Arief, 2021).

Hukum positif Indonesia tidak pernah menyebut istilah cyberstalking secara eksplisit. Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik sebagaimana diubah Undang-Undang Nomor 19 Tahun 2016 hanya menyediakan pasal-pasal umum, sehingga penjeratan pelaku dilakukan secara kasuistik yang kerap menimbulkan persoalan penafsiran karena karakter stalking yang berulang dan berpola tidak tertangkap oleh satu rumusan delik tunggal (Putri, Saputro, & Amanita, 2024; Wahyuningsih, 2025). Di samping itu, perlindungan hukum terhadap korban kejahatan siber yang menggunakan data pribadi, sebagaimana juga dijumpai dalam manipulasi data elektronik pada layanan digital, masih memerlukan penguatan regulasi yang lebih tegas (Rahmayanti, 2020).

Undang-Undang Nomor 1 Tahun 2024 tentang Perubahan Kedua atas UU ITE kemudian memisahkan delik penghinaan ke dalam Pasal 27A, merumuskan delik pengancaman dan pemerasan dalam Pasal 27B, serta menyesuaikan delik ancaman kekerasan dalam Pasal 29, selaras dengan Undang-Undang Nomor 1 Tahun 2023 tentang KUHP (Undang-Undang Nomor 1 Tahun 2024). Meski demikian, istilah

penguntitan tetap tidak muncul dalam batang tubuh undang-undang, sehingga timbul pertanyaan apakah konstruksi pasal-pasal tersebut sudah memadai menjangkau seluruh spektrum perbuatan *cyberstalking*, dan bagaimana pertanggungjawaban pidana pelaku dikonstruksikan mengingat kerumitan pembuktian kesengajaan dalam ruang siber (Putra, 2024)? Kajian ini mengemban urgensi ganda teoritis untuk mengisi kekosongan literatur hukum pidana siber pascaperubahan kedua UU ITE, dan praktis untuk memberi kepastian bagi penegak hukum serta perlindungan bagi korban.

Kondisi normatif tersebut menimbulkan persoalan hukum yang penting untuk dikaji, yaitu apakah konstruksi ketentuan dalam Undang-Undang Nomor 1 Tahun 2024 tentang Perubahan Kedua atas Undang-Undang Informasi dan Transaksi Elektronik telah memadai untuk menjangkau seluruh bentuk perbuatan *cyberstalking*, atau masih terdapat kekosongan norma yang menyebabkan sebagian perbuatan belum dapat dijerat secara efektif melalui hukum pidana. Selain itu, perlu dikaji bagaimana konstruksi pertanggungjawaban pidana terhadap pelaku *cyberstalking*, mengingat pembuktian unsur kesengajaan, pola perilaku yang berulang, dan penggunaan alat bukti elektronik dalam ruang siber memiliki karakteristik yang berbeda dengan tindak pidana konvensional (Putra, 2024). Kajian terhadap permasalahan ini memiliki urgensi teoretis dalam memperkaya literatur hukum pidana siber di Indonesia pasca berlakunya Undang-Undang Nomor 1 Tahun 2024, sekaligus urgensi praktis untuk memberikan kepastian hukum bagi aparat penegak hukum serta memperkuat perlindungan hukum bagi korban. Berdasarkan latar belakang tersebut, penelitian ini mengkaji dua permasalahan utama, yaitu: **(1)** bagaimana pengaturan dan konstruksi hukum terhadap perbuatan *cyberstalking* berdasarkan Undang-Undang Nomor 1 Tahun 2024 tentang Informasi dan Transaksi Elektronik; dan **(2)** bagaimana bentuk pertanggungjawaban pidana terhadap pelaku *cyberstalking* dalam perspektif Undang-Undang Nomor 1 Tahun 2024 tentang Informasi dan Transaksi Elektronik.

2. Metode

Penelitian ini merupakan penelitian hukum normatif (*doctrinal legal research*) yang bertujuan mengkaji konstruksi pengaturan dan pertanggungjawaban pidana terhadap *cyberstalking* berdasarkan sistem norma hukum yang berlaku. Penelitian menggunakan pendekatan perundang-undangan (*statute approach*), pendekatan konseptual (*conceptual approach*), dan pendekatan kasus (*case approach*). Pendekatan perundang-undangan dilakukan dengan menelaah berbagai regulasi yang relevan, khususnya Undang-Undang Nomor 1 Tahun 2024 tentang Perubahan Kedua atas Undang-Undang Informasi dan Transaksi Elektronik, Undang-Undang Nomor 1 Tahun 2023 tentang Kitab Undang-Undang Hukum Pidana, serta Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi. Pendekatan konseptual digunakan untuk mengkaji doktrin dan teori mengenai *cyberstalking* yang belum diatur secara

eksplisit dalam hukum positif Indonesia, sedangkan pendekatan kasus digunakan untuk menganalisis putusan pengadilan dan kasus-kasus *cyberstalking* yang telah dipublikasikan. Bahan hukum yang digunakan terdiri atas bahan hukum primer berupa peraturan perundang-undangan dan putusan pengadilan, serta bahan hukum sekunder yang meliputi buku, jurnal ilmiah, laporan lembaga resmi, dan hasil penelitian terdahulu. Pengumpulan bahan hukum dilakukan melalui studi kepustakaan, kemudian dianalisis secara preskriptif dengan menggunakan logika deduktif serta penafsiran gramatikal, sistematis, dan teleologis untuk mengidentifikasi kekuatan, kelemahan, dan kekosongan norma dalam pengaturan *cyberstalking*, sekaligus merumuskan konstruksi hukum dan pertanggungjawaban pidana yang lebih komprehensif.

3. Hasil & Pembahasan

3.1. Pengaturan dan Konstruksi Hukum *Cyberstalking* dalam Perspektif Undang-Undang Nomor 1 Tahun 2024 tentang Informasi dan Transaksi Elektronik

Titik tolak pembahasan pertama adalah kenyataan normatif bahwa hukum pidana Indonesia tidak mengenal *cyberstalking* sebagai nomenklatur delik. Tidak ada satu pasal pun, baik dalam UU ITE hasil perubahan kedua maupun dalam KUHP Nasional, yang merumuskan penguntitan sebagai tindak pidana yang berdiri sendiri dengan unsur pengulangan perbuatan sebagai intinya. Kedudukan *cyberstalking* dalam hukum pidana Indonesia dengan demikian bersifat derivatif, artinya perbuatan tersebut hanya dapat dijerat sepanjang salah satu episode perbuatannya memenuhi rumusan delik lain yang sudah ada, seperti penghinaan, pengancaman, atau pelanggaran atas data pribadi (Wahyuningsih, 2025). Konstruksi semacam ini lazim disebut penjeratan melalui pasal antara, dan di sinilah analisis terhadap pasal-pasal UU ITE hasil perubahan kedua menemukan relevansinya.

Pasal pertama yang dapat difungsikan adalah Pasal 27A Undang-Undang Nomor 1 Tahun 2024, yang melarang setiap orang dengan sengaja menyerang kehormatan atau nama baik orang lain dengan cara menuduhkan suatu hal melalui sistem elektronik. Rumusan ini memisahkan delik penghinaan dari rumusan lama Pasal 27 ayat (3) yang selama ini dikritik sebagai pasal karet, dan secara eksplisit menundukkannya pada ketentuan pencemaran dalam KUHP, termasuk sifat deliknya sebagai delik aduan absolut (Undang-Undang Nomor 1 Tahun 2024). Bagi korban *cyberstalking* yang diteror melalui unggahan yang merusak reputasinya, misalnya akun impersonasi yang menyebarkan tuduhan palsu, Pasal 27A menjadi pintu masuk yang lebih terukur dibanding rumusan lama karena unsur menuduhkan suatu hal mempersempit ruang kriminalisasi terhadap sekadar kritik atau penilaian.

Instrumen kedua adalah Pasal 27B yang melarang pengancaman pencemaran dan pemerasan melalui sistem elektronik, yakni perbuatan dengan maksud

menguntungkan diri sendiri atau orang lain secara melawan hukum dengan ancaman pencemaran atau ancaman membuka rahasia, memaksa orang memberikan sesuatu, membuat utang, menghapus piutang, atau melakukan sesuatu. Rumusan ini sangat relevan dengan salah satu modus cyberstalking yang paling merusak, yaitu ancaman penyebaran konten intim atau rahasia pribadi korban, yang dalam literatur dikenal sebagai sextortion dan kerap menjadi kelanjutan dari relasi yang berakhir buruk (Komnas Perempuan, 2024). Sebelum perubahan kedua, perbuatan semacam ini dijerat melalui Pasal 27 ayat (4) yang rumusannya sumir; kini unsur-unsurnya diuraikan lebih rinci sehingga memberi kepastian yang lebih baik, sekaligus diancam pidana yang lebih berat ketika ancaman itu menyasar pembukaan rahasia.

Instrumen ketiga, dan barangkali yang paling dekat dengan inti cyberstalking, adalah Pasal 29 juncto Pasal 45B. Pasal 29 melarang setiap orang dengan sengaja dan tanpa hak mengirimkan informasi elektronik yang berisi ancaman kekerasan atau menakut-nakuti yang ditujukan secara pribadi. Penjelasan Pasal 45B bahkan menyebut bahwa ketentuan ini termasuk menjangkau perundungan di ruang siber atau cyber bullying yang mengandung unsur ancaman kekerasan atau menakut-nakuti (Undang-Undang Nomor 19 Tahun 2016; Undang-Undang Nomor 1 Tahun 2024). Unsur menakut-nakuti itulah yang membuat pasal ini paling mendekati hakikat stalking, sebab tujuan akhir penguntit memang menciptakan rasa takut dan kehilangan rasa aman pada diri korban. Pesan-pesan teror yang dikirim berulang kali dari berbagai akun, sekalipun isinya tidak selalu berupa ancaman kekerasan eksplisit, dapat dikualifikasikan menakut-nakuti apabila dinilai dalam konteks keseluruhan polanya.

Di samping ketiga pasal tersebut, Pasal 26 UU ITE diperkuat Undang-Undang Nomor 27 Tahun 2022 mengkriminalisasi pengumpulan dan penyebaran data pribadi secara melawan hukum, sehingga modus doxing dapat dijerat melalui jalur ini (Anggen Suari & Sarjana, 2023). Penguntitan yang bereskalasi ke dunia fisik dapat dijangkau Pasal 256 dan Pasal 449 KUHP Nasional (Undang-Undang Nomor 1 Tahun 2023). Praktik peradilan membuktikan bahwa kombinasi pasal ini dapat bekerja pelaku peneror dijerat Pasal 29 juncto Pasal 45B, pelaku impersonasi dengan delik penghinaan, dan pelaku sextortion dengan delik pemerasan elektronik. Pola serupa tercatat dalam kasus kekerasan berbasis gender siber yang didampingi lembaga layanan (SAFE-net, 2023; Komnas Perempuan, 2024).

Meskipun demikian, konstruksi derivatif tersebut memiliki tiga kelemahan struktural. Pertama, seluruh pasal merumuskan delik sebagai perbuatan tunggal, padahal esensi stalking terletak pada rangkaian perbuatan berpola ratusan pesan berulang kepada seseorang yang telah menolak adalah teror, tetapi tidak ada unsur pengulangan dalam rumusan delik yang ada (Kaur, Dhir, Tandon, Alzeiby, & Abohassan, 2021). Kedua, pemantauan obsesif tanpa komunikasi misalnya mengawasi korban dengan akun

anonim nyaris tidak tersentuh pasal apapun. Ketiga, sifat delik aduan pada Pasal 27A membebaskan inisiatif penuntutan kepada korban yang justru sedang berada dalam ketakutan.

Kelemahan tersebut tampak semakin jelas apabila dibandingkan dengan pengaturan di negara lain. Singapura merumuskan unlawful stalking dalam *Protection from Harassment Act* 2014 dengan mendefinisikan course of conduct atau rangkaian perbuatan sebagai unsur inti, disertai daftar contoh perbuatan seperti mengikuti, mengomunikasikan, memantau penggunaan internet korban, dan mengintai, yang menimbulkan harassment, alarm, atau distress. Inggris melalui amendemen *Protection from Harassment Act* 1997 menambahkan delik stalking dengan pendekatan serupa, sementara Amerika Serikat dalam 18 U.S.C. § 2261A menjangkau penggunaan sarana elektronik yang menimbulkan ketakutan substansial atau tekanan emosional berat. Ketiganya sama-sama menjadikan pola perbuatan dan dampak psikis korban sebagai jantung rumusan delik, sesuatu yang absen dalam hukum Indonesia (Holt, Bossler, & Seigfried-Spellar, 2022; Weekes, Storey, & Pina, 2025). Di titik inilah dapat disimpulkan adanya kekosongan norma, bukan dalam arti tidak ada pasal yang dapat dipakai sama sekali, melainkan dalam arti tidak ada norma yang menangkap kejahatan ini sebagaimana wujudnya yang sebenarnya. Dengan demikian, konstruksi hukum cyberstalking pasca Undang-Undang Nomor 1 Tahun 2024 dapat dirumuskan sebagai konstruksi mozaik. Perubahan kedua UU ITE patut diapresiasi karena memperjelas unsur delik, menyelaraskan dengan KUHP Nasional, dan memperkuat orientasi perlindungan korban pada delik pengancaman; pada saat yang sama, pembentuk undang-undang belum beranjak dari paradigma delik tunggal menuju paradigma rangkaian perbuatan. Selama paradigma itu belum bergeser, penegakan hukum terhadap cyberstalking akan terus bergantung pada kecakapan aparat merangkai pasal dan pada keberanian korban melapor, dua hal yang dalam kenyataan tidak selalu tersedia (Putri et al., 2024; SAFEnet, 2023).

3.2. Pertanggungjawaban Pidana Pelaku *Cyberstalking* Berdasarkan Undang-Undang Nomor 1 Tahun 2024 tentang Informasi dan Transaksi Elektronik

Pembahasan kedua bertolak dari asas *geen straf zonder schuld* yang kini ditegaskan eksplisit dalam Pasal 36 KUHP Nasional setiap orang hanya dapat dimintai pertanggungjawaban atas tindak pidana yang dilakukan dengan kesengajaan atau kelalaian (Undang-Undang Nomor 1 Tahun 2023). Bagi perkara cyberstalking, penuntut umum harus membuktikan bahwa terdakwa mengendalikan akun yang digunakan, bahwa ia menghendaki atau setidaknya menyadari perbuatannya, dan bahwa ia mampu bertanggung jawab.

Unsur kesengajaan dalam delik-delik yang relevan menuntut pembuktian yang berlapis. Pada Pasal 29, kesengajaan harus meliputi pengetahuan bahwa informasi yang dikirim berisi ancaman kekerasan atau bersifat menakut-nakuti dan bahwa informasi itu ditujukan secara pribadi kepada korban. Pada Pasal 27A, kesengajaan bahkan dirangkai dengan unsur maksud agar tuduhan diketahui umum, yang dalam doktrin disebut kesengajaan dengan maksud atau opzet als oogmerk (Putra, 2024). Menariknya, karakter cyberstalking yang berulang justru mempermudah pembuktian sikap batin ini. Seseorang yang telah diblokir berkali-kali namun terus membuat akun baru untuk menghubungi korban sulit berdalih tidak menghendaki gangguan itu; pola perbuatan menjadi indikator objektif dari kehendak subjektif. Di sinilah teori kesengajaan bertemu dengan realitas digital jejak elektronik yang ditinggalkan pelaku merekam bukan hanya perbuatannya, tetapi juga arah kehendaknya (Weekes et al., 2025).

Alat bukti elektronik sebagaimana diakui Pasal 5 UU ITE merupakan instrumen pembuktian utama (Undang-Undang Nomor 11 Tahun 2008; Sedau, Masu, & Tungga, 2023). Dalam perkara cyberstalking, alat bukti dapat berupa tangkapan layar percakapan, log akses, metadata, data registrasi akun, hingga hasil forensik perangkat pelaku. Otentikasi melalui keterangan ahli forensik digital diperlukan karena tangkapan layar mudah dimanipulasi (Sedau et al., 2023). Pertanggungjawaban pidana kemudian dibangun dari rantai tiga mata *actus reus* (episode perbuatan memenuhi delik), *mens rea* (kesengajaan yang terbukti dari pola berulang sebagai indikator objektif kehendak subjektif), dan kemampuan bertanggung jawab. Pelaku yang telah diblokir berkali-kali namun terus berganti akun sulit berdalih tidak menghendaki gangguan; karakter berulang justru menjadi bukti kesengajaan (Weekes et al., 2025; Putra, 2024; Stevens, Nurse, & Arief, 2021).

Empat kendala empiris menghambat bekerjanya konstruksi pertanggungjawaban ini (1) anonimitas pelaku di balik akun palsu atau VPN menyulitkan identifikasi; (2) fragmentasi perbuatan membuat laporan korban sering ditolak karena belum memenuhi unsur delik, padahal akumulasi gangguan itulah inti penderitaannya (Stevens et al., 2021); (3) kapasitas forensik digital yang tidak merata; dan (4) sifat delik aduan pada sebagian pasal membebankan beban prosedural pada korban yang sedang mengalami tekanan psikis (Komnas Perempuan, 2024). Perubahan kedua UU ITE membawa perbaikan melalui penegasan delik aduan dan perlindungan khusus bagi anak dalam Pasal 16A, namun korban penguntitan nonseksual masih berada pada posisi perlindungan yang lebih lemah dibanding korban kekerasan seksual berbasis elektronik (Undang-Undang Nomor 1 Tahun 2024; Undang-Undang Nomor 12 Tahun 2022).

Penilaian terhadap efektivitas UU ITE hasil perubahan kedua dalam menangani *cyberstalking* dengan demikian harus diberikan secara berimbang. Sebagai instrumen represif terhadap episode-episode perbuatan yang paling merusak, yaitu ancaman kekerasan, pemerasan dengan ancaman pembukaan rahasia, dan pencemaran, undang-undang ini cukup memadai dan bahkan lebih baik daripada rezim sebelumnya karena rumusan deliknya lebih terang dan ancaman pidananya proporsional. Akan tetapi, sebagai instrumen yang menangkap kejahatan penguntitan dalam keutuhannya, undang-undang ini belum efektif karena bekerja secara fragmentaris dan reaktif hukum baru hadir setelah gangguan bereskalasi menjadi ancaman, bukan ketika pola teror mulai terbentuk. Pendapat penulis, kesenjangan inilah yang seharusnya menjadi agenda pembaruan berikutnya, baik melalui penambahan delik penguntitan dalam revisi KUHP maupun melalui undang-undang khusus tentang kekerasan berbasis elektronik yang menempatkan rangkaian perbuatan dan dampak psikis korban sebagai unsur delik (Kaur et al., 2021; Weekes et al., 2025).

4. Penutup

Berdasarkan hasil penelitian, pengaturan hukum terhadap perbuatan *cyberstalking* dalam Undang-Undang Nomor 1 Tahun 2024 tentang Perubahan Kedua atas Undang-Undang Informasi dan Transaksi Elektronik masih bersifat parsial karena belum mengatur *cyberstalking* sebagai tindak pidana yang berdiri sendiri. Penegakan hukum masih mengandalkan kombinasi beberapa ketentuan, seperti Pasal 27A, Pasal 27B, Pasal 29, Pasal 26 Undang-Undang ITE, Undang-Undang Pelindungan Data Pribadi, serta ketentuan dalam Kitab Undang-Undang Hukum Pidana. Meskipun konstruksi tersebut mampu menjangkau sebagian bentuk perbuatan *cyberstalking*, masih terdapat kekosongan norma karena karakter utama *cyberstalking* yang berupa tindakan berulang, sistematis, dan obsesif belum diakomodasi secara eksplisit dalam peraturan perundang-undangan.

Selanjutnya, pertanggungjawaban pidana terhadap pelaku *cyberstalking* didasarkan pada terpenuhinya unsur tindak pidana, adanya kesengajaan, serta kemampuan pelaku untuk bertanggung jawab secara hukum, dengan alat bukti elektronik sebagai instrumen pembuktian utama yang harus didukung melalui proses forensik digital. Namun, penerapan pertanggungjawaban pidana masih menghadapi berbagai kendala, antara lain anonimitas pelaku, fragmentasi perbuatan, keterbatasan kemampuan forensik digital, dan beban pembuktian yang masih berada pada korban. Oleh karena itu, diperlukan pembentukan pengaturan khusus mengenai delik *cyberstalking* yang mengakomodasi unsur pola perbuatan (*course of conduct*) serta dampak psikologis terhadap korban, disertai penguatan kapasitas aparat penegak hukum dalam penanganan barang bukti digital. Selain itu, penelitian empiris mengenai praktik

penegakan hukum terhadap perkara *cyberstalking* perlu dilakukan untuk melengkapi dan menguji temuan penelitian normatif ini.

Referensi

- Aldriano, M. A., & Priyambodo, M. A. (2022). Cyber crime dalam sudut pandang hukum pidana. *Jurnal Kewarganegaraan*, 6(1).
- Anggen Suari, K. R., & Sarjana, I. M. (2023). Menjaga privasi di era digital Perlindungan data pribadi di Indonesia. *Jurnal Analisis Hukum*, 6(1), 132–142. <https://doi.org/10.38043/jah.v6i1.4484>
- Asosiasi Penyelenggara Jasa Internet Indonesia. (2024). Survei penetrasi internet Indonesia 2024. Jakarta APJII.
- Council of Europe. (2001). Convention on cybercrime (European Treaty Series No. 185). Budapest Council of Europe.
- Firdaus, R. A. (2024). Perlindungan hukum dan pencegahan kejahatan siber di era digital dalam sistem hukum di Indonesia. *Staatsrecht Jurnal Hukum Kenegaraan dan Politik Islam*, 4(1).
- Holt, T. J., Bossler, A. M., & Seigfried-Spellar, K. C. (2022). Cybercrime and digital forensics An introduction (3rd ed.). New York Routledge.
- Kaur, P., Dhir, A., Tandon, A., Alzeiby, E. A., & Abohassan, A. A. (2021). A systematic literature review on cyberstalking An analysis of past achievements and future promises. *Technological Forecasting and Social Change*, 163, 120426. <https://doi.org/10.1016/j.techfore.2020.120426>
- Komnas Perempuan. (2024). Catatan tahunan kekerasan terhadap perempuan. Jakarta Komisi Nasional Anti Kekerasan terhadap Perempuan.
- Marcum, C. D., & Higgins, G. E. (2021). A systematic review of cyberstalking victimization and offending behaviors. *American Journal of Criminal Justice*, 46(6), 882–910. <https://doi.org/10.1007/s12103-021-09653-6>
- Mudzalifah, M., & Pujiyono. (2023). The politics of criminal law in cybercrime An effort to combat information technology crimes in Indonesia. *Jurnal Pembaharuan Hukum*, 10(1). <https://doi.org/10.26532/jph.v10i1.26707>
- Putra, I. M. W. (2024). Asas kesalahan terkait pertanggungjawaban pidana atas tindak pidana dalam pelaksanaan jabatan notaris. *Acta Diurnal Jurnal Ilmu Hukum Kenotariatan*, 8(1), 116–131. <https://doi.org/10.23920/acta.v8i1.1958>
- Putri, S. N. P., Saputro, H. D., & Amanita, A. (2024). Perlindungan hukum bagi korban pornografi cyberstalking menurut Undang-Undang Nomor 1 Tahun 2024 tentang Informasi dan Transaksi Elektronik. *Rechtswetenschap Jurnal Mahasiswa Hukum*, 2(1). <https://doi.org/10.36859/rechtswetenschap.v2i1.3264>
- Rahmayanti. (2020). Tinjauan yuridis terhadap driver Grabcar sebagai pelaku tindak pidana memanipulasi data elektronik (tinjauan putusan nomor 853/PID.SUS/2018/PNMKS). *Jurnal Mercatoria*, 13(2), 118–130.

- Rahmayanti, & Ramadani, S. (2024). Review of legal digitalization aspects from using telemedicine for health management in Indonesia. *Formosa Journal of Multidisciplinary Research*, 3(6).
- Ramadani, S. (2025). Legal responsibilities of third parties and hospitals regarding the implementation of electronic medical records. *International Journal of Social and Health Science*, 4(1).
- SAFE.net. (2023). Laporan situasi hak-hak digital Indonesia. Denpasar Southeast Asia Freedom of Expression Network.
- Sedau, K. S., Masu, R. R., & Tunga, I. A. (2023). Penggunaan dokumen elektronik sebagai alat bukti oleh hakim dalam pertimbangan putusan perkara pornografi. *Jurnal Indonesia Sosial Teknologi*, 4(6), 726–740. <https://doi.org/10.59141/jist.v4i6.631>
- Stevens, F., Nurse, J. R. C., & Arief, B. (2021). Cyber stalking, cyber harassment, and adult mental health A systematic review. *Cyberpsychology, Behavior, and Social Networking*, 24(6), 367–376. <https://doi.org/10.1089/cyber.2020.0253>
- Tan, D. (2021). Metode penelitian hukum Mengupas dan mengulas metodologi dalam menyelenggarakan penelitian hukum. *Nusantara Jurnal Ilmu Pengetahuan Sosial*, 8(8), 2463–2478.
- Undang-Undang Republik Indonesia Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (Lembaran Negara Republik Indonesia Tahun 2008 Nomor 58).
- Undang-Undang Republik Indonesia Nomor 19 Tahun 2016 tentang Perubahan atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (Lembaran Negara Republik Indonesia Tahun 2016 Nomor 251).
- Undang-Undang Republik Indonesia Nomor 12 Tahun 2022 tentang Tindak Pidana Kekerasan Seksual (Lembaran Negara Republik Indonesia Tahun 2022 Nomor 120).
- Undang-Undang Republik Indonesia Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi (Lembaran Negara Republik Indonesia Tahun 2022 Nomor 196).
- Undang-Undang Republik Indonesia Nomor 1 Tahun 2023 tentang Kitab Undang-Undang Hukum Pidana (Lembaran Negara Republik Indonesia Tahun 2023 Nomor 1).
- Undang-Undang Republik Indonesia Nomor 1 Tahun 2024 tentang Perubahan Kedua atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (Lembaran Negara Republik Indonesia Tahun 2024 Nomor 1).
- Wahyuningsih, K. R. (2025). Cyberstalking sebagai kejahatan multidimensional. *Jurnal Hukum, Administrasi Publik dan Negara*, 2(3), 129–136. <https://doi.org/10.62383/hukum.v2i3.273>

- Weekes, C. J., Storey, J. E., & Pina, A. (2025). Cyberstalking perpetrators and their methods A systematic literature review. *Trauma, Violence, & Abuse*. Advance online publication. <https://doi.org/10.1177/15248380251333411>
- Wilson, C., Sheridan, L., & Garratt-Reed, D. (2022). What is cyberstalking? A review of measurements. *Journal of Interpersonal Violence*, 37(11–12). <https://doi.org/10.1177/0886260520985489>
