URGENSI PENGATURAN TINDAK PIDANA *CYBERSTALKING* DI INDONESIA DAN PERBANDINGAN DENGAN INGGRIS

Brillian Prita Nyala[1] , H. B. Hasan Basri[2]
[1] *Fakultas Hukum, Universitas Islam Makassar, brillianprita@gmail.com*
[2] *Fakultas Hukum, Universitas Islam Makassar, hbhasanbasri.dty@uim makassar.ac.id*

Abstrak: Fenomena *Cyberstalking* merupakan bentuk penguntitan atau pelecehan berulang melalui media digital yang menimbulkan ancaman serius terhadap keamanan dan privasi individu. Penelitian ini bertujuan menganalisis pengaturan hukum terkait tindak pidana *Cyberstalking* di Indonesia serta membandingkannya dengan sistem hukum Inggris, menggunakan pendekatan yuridis normatif dan analisis perbandingan hukum. Di Indonesia, regulasi mengenai *Cyberstalking* masih bersifat parsial dan tersebar dalam beberapa ketentuan, seperti Undang-Undang Nomor 11 Tahun 2008 jo. Undang-Undang Nomor 1 Tahun 2024 tentang Informasi dan Transaksi Elektronik serta Kitab Undang-Undang Hukum Pidana (KUHP). Ketentuan tersebut belum secara eksplisit mengkriminalisasi *Cyberstalking*, sehingga menimbulkan kekosongan hukum, terutama dalam aspek pembuktian bukti digital, pelacakan pelaku anonim, dan perlindungan korban secara menyeluruh. Sebaliknya, Inggris telah memiliki kerangka hukum yang komprehensif melalui *Protection from Harassment Act* 1997, *Protection of Freedoms Act* 2012, serta *Communications Act* 2003, yang secara tegas mendefinisikan *stalking* dan *Cyberstalking* sebagai tindak pidana dengan unsur *course of conduct,* disertai mekanisme perlindungan korban seperti *Stalking Protection Orders.* Perbandingan ini menunjukkan perlunya Indonesia mengadopsi pendekatan hukum yang lebih spesifik dan progresif agar selaras dengan perkembangan teknologi serta nilai-nilai moral Islam, sebagaimana prinsip *hifz al-nafs* (perlindungan jiwa) dan *hifz al-'ird* (perlindungan kehormatan) yang tercermin dalam Al-Qur'an. Dengan demikian, pembaruan hukum nasional menjadi langkah strategis dalam memastikan perlindungan yang efektif bagi korban *Cyberstalking* di era digital.

Kata Kunci: *Cyberstalking*, Hukum ITE, Perlindungan Hukum, Inggris, Hukum Islam

1. Pendahuluan

Cyberstalking adalah bentuk penguntitan atau pelecehan berulang yang dilakukan melalui media digital, seperti email, media sosial, atau platform daring lainnya.[1] Pelaku *Cyberstalking* umumnya terus menerus mengirim pesan ancaman, menyebarkan informasi palsu, atau memantau aktivitas korban secara *online* tanpa izin.[2] Tindakan ini sering kali dilakukan dengan tujuan menakut-nakuti, mengganggu, atau bahkan memeras korban. Karena dilakukan di dunia maya, *Cyberstalking* dapat berlangsung secara anonim, yang membuat pelaku lebih sulit dilacak dan korban merasa lebih terancam. Fenomena ini berkembang pesat seiring dengan meningkatnya penggunaan internet dan media sosial, di mana pelaku bisa dengan mudah mengakses informasi pribadi korban dan terus mengganggu kehidupan mereka. Bahaya *Cyberstalking* tidak hanya terbatas pada gangguan digital, tetapi juga bisa menyebabkan dampak psikologis yang serius pada korban. Korban sering mengalami rasa takut, cemas, dan stres berkepanjangan akibat pelecehan yang mereka alami. Dampak lain yang signifikan adalah gangguan mental seperti depresi,

[1] Oktavany, L. (2021). Terbentuknya Cyberstalking Pada Media Sosial Instagram (Doctoral dissertation, Universitas Islam Riau).
[2] Pandie, M. M., & Weismann, I. T. J. (2021). Pengaruh Cyberbullying di Media Sosial terhadap perilaku reaktif sebagai pelaku maupun sebagai korban cyberbullying pada siswa kristen SMP Nasional Makassar. *Jurnal Jaffray*, *14*(1), 43-62.

gangguan tidur, dan ketakutan untuk berinteraksi di ruang publik atau *online*.[3] Dalam beberapa kasus, *Cyberstalking* dapat meningkat menjadi ancaman fisik jika pelaku mengetahui lokasi korban. Selain itu, korban *Cyberstalking* sering merasa terisolasi karena kurangnya perlindungan hukum yang memadai atau sulitnya menindak pelaku secara efektif, terutama di negara-negara yang belum memiliki regulasi yang jelas terkait tindak pidana ini.

Pasal 27B UU Nomor 1 Tahun 2024 tentang Informasi dan Transaksi Elektronik (ITE) mencakup ketentuan yang mengatur tentang pemerasan dan ancaman di dunia maya[4], namun belum secara spesifik mendefinisikan atau mengatur tindak pidana *Cyberstalking* . Meskipun ketentuan ini memberikan perlindungan terhadap tindakan-tindakan yang mengandung unsur pemaksaan dan ancaman melalui media elektronik, tidak adanya aturan yang jelas mengenai *Cyberstalking* meninggalkan kesenjangan dalam penegakan hukum. *Cyberstalking* adalah kejahatan yang bersifat berulang dan menargetkan korban secara sistematis[5], namun tanpa pengaturan yang lebih spesifik, tindakan ini hanya dapat dihukum jika memenuhi unsur-unsur tindak pidana lainnya seperti ancaman atau penghinaan. Ketiadaan aturan yang spesifik mengenai *Cyberstalking* dalam Pasal 27B UU Nomor 1 Tahun 2024 Tentang Informasi dan Transaksi Elektronik (UU ITE) menciptakan tantangan serius dalam penegakan hukum. Fenomena *Cyberstalking* yang semakin berkembang di era digital tidak sepenuhnya tertangani oleh regulasi saat ini, sehingga korban sering kali tidak mendapatkan perlindungan hukum yang memadai. Selain itu, para pelaku *Cyberstalking* dapat memanfaatkan celah ini untuk melancarkan aksi mereka tanpa harus khawatir terjerat oleh undang-undang yang ada. Oleh karena itu, penting bagi pemerintah untuk mengembangkan kerangka hukum yang lebih komprehensif yang tidak hanya mencakup pemerasan dan ancaman, tetapi juga mengatur *Cyberstalking* secara spesifik guna melindungi hak privasi dan keamanan individu di ranah digital.

Berbanding terbalik dengan Indonesia, Inggris telah mengatur secara spesifik tindak pidana *Cyberstalking* melalui *Protection from Harassment Act* 1997 dan *Malicious Communications Act* 1988.[6] Regulasi ini secara tegas mengakui bahwa tindakan *Cyberstalking* adalah bentuk kejahatan yang serius, terutama ketika dilakukan secara berulang dan menimbulkan ketakutan atau distress bagi korban. *Protection from Harassment Act,* mengklasifikasikan tindakan penguntitan baik di dunia nyata maupun digital sebagai kejahatan yang dapat dihukum.[7] Sementara itu, *Malicious Communications Act* memberikan dasar hukum bagi korban untuk menuntut pelaku yang mengirimkan pesan atau komunikasi bernada ancaman, melecehkan, atau mengintimidasi melalui sarana elektronik.[8] Regulasi-regulasi ini memberikan perlindungan yang lebih jelas bagi korban *Cyberstalking* di Inggris, sekaligus memberi dasar hukum yang kuat bagi penegak hukum untuk menindak pelaku. Indonesia dapat memanfaatkan pendekatan Inggris ini sebagai rujukan dalam merancang undang-undang yang lebih komprehensif. Dengan mengambil pelajaran dari Inggris, Indonesia dapat mengembangkan regulasi yang mengakomodasi fenomena *Cyberstalking* yang semakin meningkat, memberikan perlindungan bagi korban, serta memastikan bahwa pelaku dapat dikenakan hukuman yang setimpal. Hal ini akan membantu mengisi kesenjangan hukum yang saat

---

[3] Pratama, F. H., Purnomo, F., Zannethi, M. B., & Supriyadi, T. (2024). Analisa Dampak Psikologis Cyberbulling Tehadap Korban. *Liberosis: Jurnal Psikologi dan Bimbingan Konseling*, *3*(3), 11-20.

[4] Idris, J. I., & Supandi, A. (2024). Evaluasi Kebijakan Undang-Undang Informasi dan Transaksi Elektronik di Indonesia; Potret Bibliometric Analysis. *Transparansi: Jurnal Ilmiah Ilmu Administrasi*, *7*(1), 149-162.

[5] Azahra, A. P., Simanjuntak, A. C. A., Tarigan, E. S., & Hosnah, A. U. (2024). Analisa kepada Para Oknum yang Tidak Bijak dalam Menggunakan Media Sosial atau Cyberspace. *Civilia: Jurnal Kajian Hukum Dan Pendidikan Kewarganegaraan*, *3*(1), 34-47.

[6] El Asam, A., & Samara, M. (2021). Cyberbullying and the law: A review of psychological and legal challenges. *Computers in Human Behavior*, *65*, 127-141.

[7] Callender Smith, R. (2022). Protection of Harassment Act 1997: From Anti-Stalking Crimes to Celebrity Privacy Remedies. *Queen Mary Law*, *5*, 23-37.

[8] Benito, I. G. (2023). Online harassment and cyberstalking: a case study. *Sortuz: Oñati Journal of Emergent Socio-Legal Studies*, *13*(2), 242-257.

ini ada di Indonesia, sekaligus memastikan bahwa undang-undang diadaptasi dengan perkembangan teknologi.

Melihat perbedaan signifikan dalam regulasi *Cyberstalking* antara Indonesia dan Inggris, studi perbandingan hukum sangat diperlukan untuk menemukan elemen-elemen yang dapat diadopsi oleh Indonesia. Di Inggris, regulasi tentang *Cyberstalking* telah dirancang secara spesifik dalam *Protection from Harassment Act* 1997 dan *Malicious Communications Act* 1988, yang memberikan perlindungan hukum yang jelas bagi korban serta menjerat pelaku dengan ancaman hukuman yang tegas. Sementara itu, di Indonesia, peraturan terkait *Cyberstalking* masih belum konkret, karena hanya mencakup aspek pemerasan dan ancaman secara umum dalam Pasal 27B UU Nomor 1 Tahun 2024 Tentang Informasi dan Transaksi Elektronik (UU ITE). Hal ini menimbulkan kesenjangan dalam penanganan kasus *Cyberstalking*, yang semakin meningkat seiring dengan perkembangan teknologi dan media sosial. Studi perbandingan ini penting untuk memberikan panduan dalam mendesain aturan yang lebih spesifik dan sesuai dengan kondisi di Indonesia. Dengan mempelajari praktik terbaik dari Inggris dan negara lain yang memiliki regulasi komprehensif, Indonesia dapat merancang aturan yang lebih efektif dalam menangani *Cyberstalking*. Selain itu, konteks hukum dan sosial di Indonesia juga harus diperhatikan, agar aturan yang dibuat dapat diimplementasikan secara realistis dan tidak bertentangan dengan budaya serta sistem hukum yang ada. Studi perbandingan ini akan membantu mengidentifikasi celah-celah hukum di Indonesia dan menawarkan solusi berdasarkan pengalaman internasional, sehingga penegakan hukum terkait *Cyberstalking* bisa lebih optimal.

Ketiadaan pengaturan yang spesifik dan efektif mengenai *Cyberstalking* di Indonesia menyebabkan banyak pelaku tindak pidana ini sering kali hanya dikenai sanksi berdasarkan regulasi yang kurang memadai. Saat ini, kasus *Cyberstalking* di Indonesia umumnya ditangani melalui undang-undang yang mencakup pemerasan, ancaman, atau pelecehan umum, seperti dalam Pasal 27B UU Nomor 1 Tahun 2024 Tentang Informasi dan Transaksi Elektronik (UU ITE), yang belum secara eksplisit mendefinisikan *Cyberstalking* sebagai kejahatan terpisah. Akibatnya, banyak kasus yang tidak mendapatkan perhatian yang semestinya, sehingga korban seringkali dibiarkan tanpa perlindungan hukum yang memadai dan pelaku dapat terus melakukan tindakannya tanpa ada sanksi yang tegas. Dengan merujuk pada pengalaman negara-negara lain, seperti Inggris, yang memiliki *Protection from Harassment Act* 1997 dan *Malicious Communications Act* 1988, Indonesia dapat memperbaiki regulasi hukum pidananya terkait *Cyberstalking*. Regulasi tersebut memberikan definisi yang jelas tentang tindakan berulang yang menimbulkan ketakutan atau distress pada korban, serta menyediakan kerangka hukum yang kuat untuk menjerat pelaku. Indonesia bisa mengadopsi pendekatan ini untuk memberikan perlindungan yang lebih baik bagi korban *Cyberstalking* di era digital, sekaligus memastikan bahwa penegakan hukum terhadap pelaku dapat dilakukan dengan efektif dan tegas. Sehingga hal ini akan menutup celah hukum yang selama ini menghambat penanganan *Cyberstalking* di Indonesia.

2. Metode Penelitian

Penelitian ini menggunakan metode normatif dengan fokus pada kajian peraturan perundang-undangan terkait tindak pidana *Cyberstalking* di Indonesia dan Inggris, bertujuan untuk menganalisis ketentuan hukum yang berlaku serta efektivitas penerapannya. Objek penelitian mencakup regulasi utama di kedua negara: di Indonesia, diteliti Undang-Undang Informasi dan Transaksi Elektronik (UU ITE) No. 19 Tahun 2016, khususnya Pasal 27 hingga Pasal 29 yang mengatur tindak pidana seperti pencemaran nama baik, penghinaan, dan ancaman melalui media elektronik; sementara di Inggris, regulasi yang dianalisis adalah *Protection from Harassment Act* 1997 dan *Malicious Communications Act* 1988. Pendekatan normatif dipilih karena sesuai dengan tujuan penelitian yang bersifat analitis terhadap hukum positif, bukan pengujian empiris terhadap perilaku pelaku atau korban.

Instrumen penelitian berupa analisis dokumen hukum yang mencakup sumber hukum primer seperti undang-undang dan putusan pengadilan serta sumber sekunder seperti jurnal dan buku akademik. Pengumpulan data dilakukan melalui studi kepustakaan yang sistematis, dengan teknik analisis data menggunakan pendekatan deskriptif kualitatif dan komparatif. Metode ini memungkinkan peneliti untuk menggambarkan secara mendalam ketentuan hukum masing-masing negara sekaligus membandingkan kekuatan, kelemahan, dan efektivitas regulasi *Cyberstalking* dalam konteks hukum nasionalnya. Dengan demikian, penelitian ini tidak hanya mengidentifikasi perbedaan hukum, tetapi juga memberikan dasar untuk mengevaluasi sejauh mana kerangka hukum di kedua negara mampu merespons tantangan kejahatan siber secara memadai.

3. Hasil dan Pembahasan

1. Pengaturan Hukum Terkait Tindak Pidana *Cyberstalking* Dalam Hukum Indonesia

a. Konsep *Cyberstalking* dalam Hukum Indonesia

Dalam hukum Indonesia, cyberstalking dipahami sebagai tindakan penguntitan, pelecehan, atau intimidasi melalui media elektronik dan internet yang dilakukan berulang kali untuk mengganggu, mengancam, atau menimbulkan ketakutan pada korban. Ciri utamanya adalah penggunaan teknologi yang memungkinkan pelaku bertindak anonim dan sulit dilacak. Saat ini, belum ada ketentuan khusus yang secara eksplisit mengatur "pengawasan atau pemantauan daring secara berulang" sebagaimana dimaksud dalam Pasal 27B UU No. 1 Tahun 2024 tentang perubahan atas UU ITE. Pasal tersebut baru menjadi dasar awal urgensi pengaturan khusus mengenai *cyberstalking* di Indonesia.[9]

Unsur-unsur yang terkandung dalam *Cyberstalking* menurut hukum pidana meliputi adanya ancaman, pelecehan, gangguan, dan intimidasi secara daring. Perbuatan ini berbeda dengan komunikasi biasa di dunia maya, karena sifatnya yang berulang dan menimbulkan tekanan psikologis bagi korban. Dalam sistem hukum Indonesia, perbuatan *Cyberstalking* seringkali masuk dalam kategori kejahatan siber (*cybercrime*) yang melanggar hak-hak dasar individu, khususnya hak atas rasa aman dan perlindungan privasi.[10]

Perbedaan utama antara *stalking* konvensional dan *cyberstalking* terletak pada sarana serta cara pelaku beraksi. Stalking konvensional melibatkan kontak fisik seperti mengikuti atau mengintai korban, sedangkan *cyberstalking* dilakukan melalui media digital tanpa kehadiran fisik, membuatnya sulit diantisipasi karena dapat terjadi kapan saja dan di mana saja, bahkan di ruang privat korban. Dari sisi hukum Indonesia, stalking konvensional umumnya dijerat dengan ketentuan KUHP, sementara *cyberstalking* lebih sering menggunakan Undang-Undang ITE meski belum diatur secara spesifik. Hal ini menunjukkan perlunya pendekatan hukum yang lebih modern dan komprehensif terhadap *cyberstalking* karena sifatnya yang berbasis teknologi dan beroperasi di ruang siber.

b. Peraturan Perundang-undangan yang mengatur

Pengaturan tindak pidana *cyberstalking* di Indonesia pada dasarnya berlandaskan pada Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE) yang telah diubah, terakhir melalui UU No. 1 Tahun

[9] Listiawati, Nora. 2023. "Apa Itu Cybertalking?" *Kepolisian Daerah Kepulauan Riau (Polda Kepri) Batam*. https://pid.kepri.polri.go.id/apa-itu-cybertalking/?utm_source.

[10] Nurdayati dkk. 2021. "Eksistensi Keamanan Siber Terhadap Tindakan Cyberstalking Dalam Sistem Pertanggungjawaban Pidana Cybercrime." *Syntax Literate: Jurnal Ilmiah Indonesia* 6(4): 1554–72.

2024. Dalam UU ITE, *cyberstalking* dikategorikan sebagai perbuatan yang mengandung unsur ancaman, pelecehan, atau gangguan melalui media elektronik. Pasal-pasal yang sering digunakan antara lain Pasal 27 ayat (3) tentang pencemaran nama baik, Pasal 27B tentang pemerasan dan pengancaman, serta Pasal 29 mengenai ancaman kekerasan atau menakut-nakuti lewat sistem elektronik. Perubahan dalam UU No. 1 Tahun 2024 memperjelas perlindungan hukum dengan menambahkan ketentuan lebih spesifik terkait tindak pidana berbasis elektronik, termasuk pelecehan dan intimidasi daring. Meskipun istilah *cyberstalking* belum disebut secara eksplisit, Pasal 27B memberi dasar yuridis untuk menafsirkan penguntitan digital sebagai bentuk kejahatan siber. Selain itu, KUHP juga dapat digunakan melalui pendekatan analogi, misalnya Pasal 335 tentang perbuatan tidak menyenangkan dan Pasal 368 tentang pemerasan dan ancaman, yang dapat diterapkan pada tindakan penguntitan daring sebagai perluasan dari tindak pidana konvensional[11]

Meskipun telah diatur dalam UU ITE dan KUHP, para ahli hukum menilai bahwa pengaturan terkait *cyberstalking* masih belum komprehensif. Kejahatan ini memiliki karakteristik berbeda dari stalking konvensional karena memanfaatkan teknologi digital yang lintas batas, sulit dilacak, dan berlangsung terus-menerus, sehingga menimbulkan kendala dalam pembuktian dan pertanggungjawaban pidana. UU ITE masih berfungsi sebagai payung hukum umum yang memerlukan regulasi turunan agar mampu menyesuaikan diri dengan dinamika kejahatan siber. Perubahan melalui UU No. 1 Tahun 2024 memang menjadi langkah maju dalam memperkuat perlindungan terhadap ancaman digital, namun para akademisi seperti Rumangkang, Mohede, dan Sumilat (2025) menekankan perlunya penegasan definisi serta batasan hukum *cyberstalking* agar penegakan hukumnya efektif dan tidak menimbulkan multitafsir, sekaligus menjamin keadilan substantif bagi korban.

c. Kekosongan dan Keterbatasan Regulasi

Kekosongan regulasi mengenai *cyberstalking* di Indonesia masih menjadi persoalan penting karena belum ada aturan khusus yang mengatur penguntitan daring secara komprehensif. Ketentuan yang ada hanya mencakup aspek terbatas seperti penghinaan, pencemaran nama baik, atau ancaman, sementara bentuk-bentuk *cyberstalking* yang lebih kompleks seperti pelecehan berulang, intimidasi psikologis, dan gangguan terus-menerus di media digital belum diatur secara tegas. Kondisi ini menimbulkan risiko inkonsistensi hukum dan membuka peluang impunitas bagi pelaku. Dari sisi penegakan hukum, tantangan juga muncul akibat keterbatasan kemampuan aparat, infrastruktur, serta kerangka hukum yang masih terfragmentasi. UU ITE dan KUHP hanya memberikan dasar umum tanpa kategori khusus bagi *cyberstalking*, sehingga aparat kerap harus menafsirkan pasal-pasal yang kurang relevan, menyebabkan banyak laporan korban tidak dapat diproses secara optimal karena tidak memenuhi unsur pidana yang ada.[12]

Dalam praktik pembuktian, keterbatasan juga terjadi. Bukti digital sering menimbulkan masalah keabsahan dan rantai bukti (*chain of custody*). Kasus-kasus *Cyberstalking* sering mengandalkan pesan elektronik, rekaman, atau data digital lain yang mudah dihapus atau dimanipulasi. Ketidakjelasan standar pembuktian menimbulkan kesulitan bagi hakim dan penyidik dalam memastikan validitas barang

[11] Rumlus, Muhamad Hasan, Moh Ery Kusmiadi, Adirandi M Rajab, and Agfajrina Cindra Pamungkas. 2023. "Kebijakan Penangguangan Tindak Pidana Cyberstalking Pada Media Elektronik." *Equality Before The Law* 3(2): 101–16. doi:10.36232/equalitybeforethelaw.v3i2.461.

[12] Sitanggang, Andri Sahata, Fernanda Darmawan, and Dony Saputra. 2024. "Hukum Siber Dan Penegakan Hukum Di Indonesia: Tantangan Dan Solusi Memerangi Kejahatan Siber." *Jurnal Pendidikan dan Teknologi Indonesia* 4(3): 79–83. doi:10.52436/1.jpti.409.

bukti, sehingga banyak kasus tidak dapat dilanjutkan ke tahap penuntutan.[13] Pembuktian dalam hukum pidana Indonesia terhadap *cybercrime* memiliki kendala besar karena sistem hukum pidana Indonesia masih didominasi paradigma pembuktian tradisional yang menekankan bukti fisik dan saksi langsung. *Cyberstalking* yang berbasis daring membuat korban sering tidak memiliki bukti "fisik" berupa saksi mata atau dokumen cetak, melainkan bukti elektronik. Tanpa adaptasi regulasi, sistem hukum kesulitan menampung perkembangan modus operandi kejahatan digital.[14]

Kejahatan siber, termasuk *Cyberstalking*, sulit diberantas karena karakteristiknya lintas batas negara dan pelaku kerap bersembunyi di balik anonimitas. Hal ini menimbulkan *problem* yurisdiksi dan koordinasi antarnegara. UU ITE maupun KUHP tidak secara memadai memberikan dasar untuk mengejar pelaku yang berada di luar negeri, sehingga banyak kasus berhenti di tahap penyelidikan.[15]

Masalah lain adalah rendahnya kesadaran korban dan aparat dalam mengenali *Cyberstalking* sebagai tindak pidana. Masih banyak korban yang ragu untuk melapor karena belum memahami bahwa *Cyberstalking* merupakan bentuk kejahatan yang bisa dipidana. Aparat penegak hukum juga kerap menganggapnya sekadar persoalan pribadi atau perdata, bukan tindak pidana, sehingga respons hukum tidak optimal.[16]

Keterbatasan dalam aspek substansi hukum tampak dari ketiadaan definisi jelas mengenai *cyberstalking*, yang memunculkan multiinterpretasi misalnya, apakah pengiriman pesan berulang tanpa ancaman langsung dapat dikategorikan sebagai tindak pidana. Tanpa kepastian norma, aparat penegak hukum kesulitan menentukan batasan, sementara pelaku dapat beralasan bahwa tindakannya bukan kejahatan. Kekosongan regulasi ini mencakup tiga aspek utama: substansi (tidak ada aturan khusus dan tegas), struktur (kompetensi aparat yang terbatas), dan budaya hukum (rendahnya kesadaran masyarakat dan aparat terhadap bahaya *cyberstalking*). Selama hukum hanya bertumpu pada pasal umum dalam UU ITE dan KUHP, kejahatan ini akan sulit dijerat secara efektif. Karena itu, dibutuhkan pembaruan hukum yang spesifik, peningkatan kapasitas aparat, serta penguatan regulasi melalui perumusan pasal baru yang meniru pendekatan negara seperti Inggris, dengan mengintegrasikan Pasal 27B UU ITE sebagai dasar pembentukan norma khusus mengenai *cyberstalking*.

d. Upaya Penegakan Hukum, Praktik dan Perlindungan Korban

Di. Kasus *Cyberstalking* di Indonesia umumnya dilaporkan oleh korban langsung ke kepolisian dengan membawa bukti digital seperti tangkapan layar, rekaman percakapan, atau tautan konten. Proses penindakan biasanya menggunakan dasar hukum dalam UU No. 1 Tahun 2024 tentang Informasi dan Transaksi Elektronik, khususnya pasal yang terkait dengan ancaman, pelecehan, penyebaran konten bermuatan melawan hukum, serta pasal-pasal umum dalam KUHP yang mengatur penghinaan, ancaman, atau perbuatan tidak menyenangkan. Laporan korban *Cyberstalking*, termasuk yang

[13] Saragih, Alexandra Exelsia, Noel Christian, and Pujia Khoirunisa. 2024. "Media Hukum Indonesia (MHI) Analisis Penggunaan Barang Bukti Digital Di Dalam Sistem Hukum Di Indonesia (Studi Kasus Putusan Nomor 3 K/PID.SUS/2019)." *Media Hukum Indonesia* 2(2): 504. https://doi.org/10.5281/zenodo.12082755.

[14] Yustia, M. 2010. "Pembuktian Dalam Hukum Pidana Indonesia Terhadap Cyber Crime." *Pranata Hukum* 5(2): 26724.

[15] Habibi, Miftakhur Rokhman, and Isnatul Liviani. 2020. "Kejahatan Teknologi Informasi (Cyber Crime) Dan Penanggulangannya Dalam Sistem Hukum Indonesia." *Al-Qanun: Jurnal Pemikiran dan Pembaharuan Hukum Islam* 23(2): 400–426. doi:10.15642/alqanun.2020.23.2.400-426.

[16] Juharwati. 2024. "Jerat Hukum Pelaku Ctberstalking Dalam UNDANG-UNDANG ITE 2024 Dan KUHP (KUHP Saat Ini Dan Masa Mendatang/UNDANG-UNDANG/1/2023." *Hoc*: 1. https://www.hukumonline.com/klinik/a/jerat-hukum-pelaku-plagiat-skripsi-cl2503/.

bermuatan pornografi, lebih banyak diarahkan melalui jalur UU ITE karena KUHP belum secara spesifik mengatur perbuatan penguntitan daring.[17]

Hambatan penegakan muncul terutama pada tahap pembuktian. Bukti digital memiliki sifat rapuh karena mudah dihapus, dipalsukan, atau dimodifikasi. Selain itu, tantangan muncul dalam otentikasi data dan memastikan rantai bukti *(chain of custody)* agar dapat diterima di pengadilan. Pelacakan identitas pelaku juga sulit karena mereka sering menggunakan akun anonim, server luar negeri, atau teknologi penyamaran. Kerja sama dengan penyedia platform digital menjadi penting, namun sering terkendala oleh regulasi privasi internasional, serta rumitnya prosedur *mutual legal assistance* jika pelaku berada di luar negeri.[18]

Hak korban dalam kasus *Cyberstalking* tidak hanya terkait dengan keadilan hukum, tetapi juga perlindungan psikologis, legal, dan privasi. Korban memiliki posisi hukum yang perlu dijamin oleh negara, termasuk perlindungan identitas dalam proses peradilan serta layanan konseling untuk mencegah trauma berkepanjangan. Perlindungan ini mencakup hak korban untuk tidak dipublikasikan datanya tanpa izin, mengingat banyak kasus *Cyberstalking* justru memperparah penderitaan korban karena data pribadi mereka beredar luas di ruang digital.[19]

Dari perspektif perlindungan hukum, korban *Cyberstalking* berhak atas perlindungan khusus terhadap privasi dan kebebasan pribadi mereka, khususnya ketika serangan berbentuk pornografi atau pelecehan seksual daring². Negara memiliki kewajiban memberikan mekanisme perlindungan hukum, termasuk pendampingan advokat atau lembaga perlindungan saksi dan korban, agar korban tidak semakin tertekan dalam proses peradilan. Hal ini menunjukkan bahwa perlindungan hukum tidak hanya sebatas represif (penindakan), tetapi juga preventif melalui pengamanan hak-hak korban.

Mekanisme restitusi atau ganti rugi dalam kasus *Cyberstalking* masih terbatas. Hingga kini, tidak ada ketentuan spesifik yang mengatur kompensasi finansial bagi korban, meskipun korban dapat mengajukan gugatan perdata berdasarkan kerugian material dan immaterial yang dialami. Beberapa putusan pengadilan hanya menekankan pada pidana penjara atau denda bagi pelaku, belum pada pemulihan korban. Listiawati (2023) menyoroti perlunya adanya perintah pengadilan *(restraining order)* yang dapat menghentikan tindakan pelecehan berulang secara daring, sebagaimana diterapkan di negara lain. Dengan demikian, sistem hukum Indonesia masih perlu pembaruan agar dapat memberikan pemulihan yang lebih komprehensif bagi korban *Cyberstalking*. Oleh karena itu, urgensi pembentukan peraturan khusus tentang *Cyberstalking* menjadi semakin nyata, agar perlindungan korban tidak hanya bersifat umum, tetapi juga komprehensif terhadap seluruh bentuk intimidasi digital lintas platform.

e. Urgensi dan Rekomendasi Regulasi

Urgensi pembentukan regulasi khusus tentang *Cyberstalking* di Indonesia menjadi kebutuhan mendesak. Meskipun telah ada pengaturan dalam Undang-Undang ITE dan KUHP, ketiadaan pasal yang secara eksplisit mengatur tindak penguntitan digital menyebabkan penegakan hukum berjalan tidak efektif. Oleh karena itu, Indonesia perlu mempertimbangkan pembentukan undang-undang tersendiri yang

[17] Listiawati, Nora. 2023. "Apa Itu Cybertalking?" *Kepolisian Daerah Kepulauan Riau (Polda Kepri) Batam*. https://pid.kepri.polri.go.id/apa-itu-cybertalking/?utm_source.

[18] Nurdayati dkk. 2021. "Eksistensi Keamanan Siber Terhadap Tindakan Cyberstalking Dalam Sistem Pertanggungjawaban Pidana Cybercrime." *Syntax Literate: Jurnal Ilmiah Indonesia* 6(4): 1554–72.

[19] Pratama, Akbar Yudha, Hafidz Amrullah Dzaky Nugroho Br, Afifudin Nur Rosyid Astinda, and Yurista Ardien Adhipradana. 2024. "Legal Standing." *LEGAL STANDING JURNAL ILMU HUKUM* 8(3): 242–55. https://news.detik.com/berita/d-3567290/polling-58-masyarakat-puas-kinerja-kpk,.

meniru ketegasan *Protection from Harassment Act 1997* di Inggris, namun tetap disesuaikan dengan konteks sosial dan hukum nasional. Dalam UNDANG-UNDANG ITE, tindak *Cyberstalking* dapat dikategorikan sebagai bentuk perbuatan yang mengandung ancaman, pelecehan, atau gangguan melalui media elektronik. Pasal-pasal yang sering digunakan dalam menjerat pelaku antara lain Pasal 27 ayat (3) tentang penghinaan/pencemaran nama baik, Pasal 27B tentang pemerasan dan pengancaman, serta Pasal 29 yang mengatur mengenai ancaman kekerasan atau menakut-nakuti melalui sistem elektronik. Perubahan melalui UNDANG-UNDANG No. 1 Tahun 2024 mempertegas perlindungan hukum dengan menambahkan klausul-klausul yang lebih spesifik mengenai tindak pidana berbasis elektronik, termasuk yang berhubungan dengan pelecehan dan intimidasi secara daring.

f. Perspektif Al-Qur'an tentang *Cyberstalking*

Fenomena *Cyberstalking* yang berupa pelecehan, pengawasan, pengancaman, dan penyalahgunaan ruang digital terhadap korban bertentangan dengan nilai-nilai Islam yang menekankan penghormatan terhadap kehormatan, privasi, dan ketenangan jiwa manusia. Al-Qur'an menegaskan larangan untuk mencari-cari kesalahan orang lain dan melakukan intrusi terhadap kehidupan pribadi. Dalam QS. Al-Hujurat [49]:12 disebutkan:

وَلَا تَجَسَّسُوا وَلَا يَغْتَب بَّعْضُكُم بَعْضًا ۚ أَيُحِبُّ أَحَدُكُمْ أَن يَأْكُلَ لَحْمَ أَخِيهِ مَيْتًا فَكَرِهْتُمُوهُ ۚ وَاتَّقُوا اللَّهَ إِنَّ اللَّهَ تَوَّابٌ رَّحِيم

Wa lā tajassasū wa lā yaghtab ba'ḍukum ba'ḍā, a-yuḥibbu aḥadukum a-yakula laḥma akhīhi maytan fa karih'tumūhu, wattaqullāh, innallāha tawwābun raḥīm[20]

"Dan janganlah kamu mencari-cari kesalahan orang lain, dan janganlah ada di antara kamu yang menggunjing sebagian yang lain. Sukakah salah seorang di antara kamu memakan daging saudaranya yang sudah mati? Maka tentulah kamu merasa jijik kepadanya. Bertakwalah kepada Allah, sesungguhnya Allah Maha Penerima taubat lagi Maha Penyayang."

Ayat ini menegaskan larangan *tajassus* (mengintai/mengintip) yang sangat relevan dengan praktik *Cyberstalking*. Tindakan memantau aktivitas digital orang lain tanpa izin, mengganggu, bahkan menyebarkan privasi korban, merupakan bentuk pelanggaran terhadap larangan Al-Qur'an tersebut.

Selain itu, *Cyberstalking* kerap kali bermuatan pelecehan dan ancaman yang menyebabkan ketakutan atau penderitaan psikologis. Hal ini ditegaskan dalam QS. An-Nur [24]:19:

إِنَّ ٱلَّذِينَ يُحِبُّونَ أَن تَشِيعَ ٱلْفَـٰحِشَةُ فِى ٱلَّذِينَ ءَامَنُوا۟ لَهُمْ عَذَابٌ أَلِيمٌ فِى ٱلدُّنْيَا وَٱلْـَٔاخِرَةِ ۚ وَٱللَّهُ يَعْلَمُ وَأَنتُمْ لَا تَعْلَمُون

Inna alladzīna yuḥibbūna an tasyī'al-fāḥisyatu fī alladzīna āmanū lahum 'adzābun alīmun fī ad-dunyā wa al-ākhirah, wallāhu ya'lamu wa antum lā ta'lamūn[21]

"Sesungguhnya orang-orang yang suka terjadinya perbuatan keji itu tersebar di kalangan orang-orang beriman, bagi mereka azab yang pedih di dunia dan di akhirat. Dan Allah mengetahui, sedang kamu tidak mengetahui."

Ayat ini menunjukkan bahwa siapa pun yang suka menyebarkan hal-hal buruk, menimbulkan keresahan, dan merusak kehormatan orang lain, termasuk melalui dunia digital, akan mendapat ancaman keras. *Cyberstalking* yang menyebarkan ketakutan, pelecehan, atau konten merendahkan martabat korban, jelas bertentangan dengan pesan moral Al-Qur'an.

[20] Al-Quran dan Terjemahan Universitas Islam Makassar,2021.
[21] Al-Quran dan Terjemahan Universitas Islam Makassar,2021.

Dari sisi perlindungan korban, Al-Qur'an menekankan pentingnya menjaga ucapan dan interaksi agar tidak menimbulkan mudarat bagi orang lain. QS. Al-Isra [17]:53 menyatakan:

وَقُل لِّعِبَادِى يَقُولُوا۟ ٱلَّتِى هِىَ أَحْسَنُ ۚ إِنَّ ٱلشَّيْطَٰنَ يَنزَغُ بَيْنَهُمْ ۚ إِنَّ ٱلشَّيْطَٰنَ كَانَ لِلْإِنسَٰنِ عَدُوًّا مُّبِينًا

Wa qul li'ibādī yaqūlū allatī hiya aḥsan, inna asy-syayṭāna yanzaghu bainahum, inna asy-syayṭāna kāna lil-insāni 'aduwwan mubīnā

"Dan katakanlah kepada hamba-hamba-Ku: 'Hendaklah mereka mengucapkan perkataan yang lebih baik (benar).' Sesungguhnya setan menimbulkan perselisihan di antara mereka. Sesungguhnya setan adalah musuh yang nyata bagi manusia."

Ayat ini menekankan prinsip komunikasi yang baik, sopan, dan menenangkan. Sebaliknya, *Cyberstalking* menghadirkan kata-kata kasar, intimidasi, dan gangguan yang menimbulkan konflik batin maupun sosial. Dengan demikian, regulasi hukum positif yang masih terbatas harus memperhatikan landasan etik dan spiritual dari Al-Qur'an agar mampu melindungi korban secara utuh.

2. Perbandingan Pengaturan Tindak Pidana *Cyberstalking* di Indonesia Dengan Inggris

a. Konsep dan Legislasi *Cyberstalking* di Inggris

Kerangka hukum Inggris menempatkan stalking dan harassment sebagai tindak pidana yang diatur secara khusus dalam *Protection from Harassment Act* 1997 (PHA 1997). Pada dasarnya PHA 1997 melarang "*a course of conduct*" yang mengakibatkan pelecehan terhadap orang lain; sejak 2012 undang-undang ini diperjelas untuk memasukkan bentuk-bentuk stalking, termasuk tindakan yang terjadi secara *online (monitoring online, contacting, sending messages,* dll.). Penuntutan dan panduan penerapan pasal-pasal ini dikeluarkan oleh *Crown Prosecution Service* (CPS) sehingga praktik penegakan berlandaskan baik teks hukum maupun pedoman penuntutan profesional.[22]

Definisi stalking menurut PHA 1997 (sejak disisipkannya pasal 2A oleh *Protection of Freedoms Act* 2012) menekankan "*course of conduct*", yaitu perilaku berulang pada lebih dari satu kesempatan yang jumlah dan jenis tindakannya dapat berbeda (mis. mengikuti, menghubungi, memantau *online*, mengintai, mengganggu properti, menyebarkan informasi pribadi). Pasal 2A secara khusus menciptakan *delik offence of stalking* yang bersifat ringkas (*summary*) dan memuat contoh-contoh tindakan yang termasuk dalam unsur stalking; Penjelasan legislatif (*explanatory notes*) menjabarkan bahwa pengertian ini sengaja meliputi kegiatan daring sehingga tidak perlu ada kehadiran fisik pelaku untuk terpenuhi unsur.

Untuk perilaku yang lebih serius, pasal 4A (juga dimasukkan oleh *Protection of Freedoms Act* 2012) menetapkan *delik stalking involving fear of violence or serious alarm or distress*. Kriteria objektifnya: perilaku berulang yang (a) menyebabkan korban takut akan kekerasan pada sedikitnya dua kesempatan, atau (b) menyebabkan "*serious alarm or distress*" yang secara substansial mengganggu kegiatan hari-hari korban. Pelanggaran pasal 4A bersifat *either-way* (dapat diadili di *magistrates' court* atau *crown court*) dan diprogramkan memiliki sanksi berat, hakim dapat menjatuhkan hukuman yang signifikan; sejak beberapa perubahan kebijakan/pengetatan hukuman, ancaman hukuman untuk pelanggaran berat telah dinaikkan dalam praktik penjatuhan sanksi. Panduan *sentencing* dan CPS membantu memilih pasal paling tepat (2/2A/4/4A) sesuai bukti dan tingkat bahaya.

[22] Fullbrook, S. 1998. "The Protection From Harassment Act." *The British journal of theatre nursing : NATNews : the official journal of the National Association of Theatre Nurses* 7(11): 18–20.

Untuk aspek komunikasi *online* yang ofensif, legislasi lain melengkapi PHA 1997. *Section 127 Communications Act* 2003 membuatnya tindak pidana untuk mengirim lewat jaringan komunikasi elektronik pesan yang *"grossly offensive, indecent, obscene or menacing",* sehingga sering dipakai untuk kasus-kasus ancaman dan pelecehan *online*. Selain itu, *Malicious Communications Act* 1988 (s.1) menangani pengiriman materi dengan maksud menyebabkan tekanan atau kecemasan, dan keduanya kerap dipakai bersama PHA saat perilaku daring memenuhi unsur komunikasi bermuatan kriminal. CPS menyediakan *guidance* khusus untuk *offence-offence* komunikasi ini agar penyidik dan jaksa memilih kerangka hukum yang paling sesuai.[23]

Mekanisme perlindungan non-pidana dan penegakan preventif juga tersedia: *Stalking Protection Orders* (SPOs) diperkenalkan melalui *Stalking Protection Act* 2019 memungkinkan otoritas (*police/courts*) mengeluarkan perintah pencegahan terhadap individu yang menunjukkan perilaku *stalking*, termasuk kewajiban untuk menghentikan kontak *online* atau menyerahkan perangkat tertentu. Selain itu ada protokol investigasi dan praktek terbaik (*College of Policing, CPS protocols*) yang memberi panduan tentang pengumpulan bukti elektronik, penilaian risiko, dan rujukan layanan korban. Meskipun kerangka hukum Inggris lebih komprehensif dibanding banyak yurisdiksi lain karena mengkombinasikan pasal *stalking* khusus, peraturan komunikasi, dan mekanisme perlindungan praktiknya tetap menghadapi tantangan pembuktian bukti digital, pengklasifikasian tindak (*harassment vs stalking*), dan pelacakan pelaku lintas batas.

b. Unsur dan Tingkat Keseriusan

Dalam hukum Inggris, inti dari *stalking* adalah adanya *course of conduct,* yaitu pola perilaku berulang yang terjadi minimal dua kali. "Perilaku" ini tidak dibatasi hanya pada interaksi fisik (mengikuti, mendekati), tetapi juga mencakup perilaku melalui media elektronik seperti mengirim pesan berulang kali, memantau akun media sosial, atau melacak aktivitas *online* korban. Dengan demikian, satu tindakan tunggal biasanya tidak cukup untuk memenuhi unsur *stalking*, tetapi bila ada pengulangan dan kontinuitas, unsur ini terpenuhi. Hal ini ditegaskan dalam Section 2A PHA 1997 yang dimasukkan melalui *Protection of Freedoms Act* 2012.

Untuk kategori yang lebih serius, hukum Inggris menambahkan unsur bahwa korban harus mengalami "*fear of violence"* (rasa takut akan kekerasan). Dalam *Section* 4A PHA 1997, dinyatakan bahwa jika *course of conduc*t pelaku menyebabkan korban, pada sedikitnya dua kesempatan, takut akan tindak kekerasan, maka kejahatan ini termasuk bentuk yang lebih berat. Unsur ini dimaksudkan untuk memberikan perlindungan terhadap korban yang berada dalam kondisi ancaman serius, baik secara fisik maupun psikologis.[24]

Selain rasa takut akan kekerasan, hukum juga mencakup korban yang mengalami *"serious alarm or distress"* akibat tindakan *stalking*. Unsur ini meliputi keadaan di mana korban menderita keresahan yang mendalam, kehilangan rasa aman, atau gangguan signifikan terhadap kehidupan sehari-harinya. Dengan kata lain, meskipun pelaku tidak secara eksplisit mengancam kekerasan, tindakannya yang konsisten dapat menyebabkan trauma serius yang masuk kategori pidana berat. Contoh: korban berhenti bekerja, mengubah rutinitas, atau mengalami gangguan kesehatan mental akibat tekanan.

---

[23] CPS. 2018. "Stalking or Harassment." *cps.gov.uk*. https://www.cps.gov.uk/legal-guidance/stalking-or-harassment?utm_source.

[24] Fullbrook, S. 1998. "The Protection From Harassment Act." *The British journal of theatre nursing : NATNews : the official journal of the National Association of Theatre Nurses* 7(11): 18–20.

Perbedaan antara tindak ringan dan berat terlihat pada tingkat keseriusan unsur yang terpenuhi. *Stalking* biasa (s.2A) merupakan tindak *summary offence* dengan hukuman lebih ringan (umumnya denda atau kurungan singkat). Sedangkan *stalking* yang memenuhi unsur *fear of violence* atau *serious alarm/distress* (s.4A) merupakan *either-way offence,* sehingga dapat dibawa ke pengadilan tinggi dengan ancaman hukuman yang lebih berat, termasuk penjara hingga 5 tahun. Tingkatan ini menunjukkan bahwa hukum Inggris membedakan bobot kejahatan berdasarkan dampak terhadap korban, sehingga penegakan hukum lebih proporsional.[25]

c. Praktik Penegakan Hukum, Keterbatasan Serta Tantangan

Penegakan hukum terhadap *Cyberstalking* di Inggris dimulai dari tahap pelaporan oleh korban kepada kepolisian. Polisi berperan sebagai pintu masuk utama untuk menerima laporan, melakukan penyelidikan, dan mengumpulkan bukti elektronik maupun fisik. Dalam kasus *Cyberstalking*, polisi memiliki kewajiban untuk menilai risiko langsung terhadap korban, termasuk ancaman kekerasan atau distress yang serius. Selanjutnya, berkas perkara diserahkan ke *Crown Prosecution Service* (CPS) yang bertugas memutuskan apakah bukti yang ada cukup untuk melanjutkan ke penuntutan berdasarkan *Code for Crown Prosecutors.* CPS mempertimbangkan aspek kepentingan publik dan kemungkinan keberhasilan penuntutan sebelum membawa kasus ke pengadilan.[26]

Selain penegakan pidana, sistem hukum Inggris menyediakan opsi perintah perlindungan untuk melindungi korban. *Restraining Orders* dapat diberikan oleh pengadilan setelah putusan pidana maupun tanpa putusan *(post-conviction atau stand-alone orders),* dengan tujuan mencegah pelaku melakukan tindakan serupa di masa depan. Sejak diberlakukannya *Stalking Protection Orders* (SPOs) pada tahun 2020 melalui *Stalking Protection Act* 2019, korban juga dapat meminta perlindungan lebih dini tanpa harus menunggu adanya proses pidana. SPOs memberikan fleksibilitas, karena dapat membatasi perilaku pelaku, mengatur penggunaan internet, hingga melarang kontak langsung maupun tidak langsung dengan korban.

Untuk tindak pidana stalking biasa di bawah *Section 2A Protection from Harassment Act* 1997, pelaku dapat dikenai hukuman penjara hingga 6 bulan atau denda. Namun, jika stalking menyebabkan *fear of violence* atau *serious alarm or distress* sebagaimana diatur dalam *Section* 4A, sanksinya jauh lebih berat. Amandemen terbaru meningkatkan ancaman pidana maksimum menjadi 10 tahun penjara bagi kasus yang dikategorikan serius, mencerminkan urgensi perlindungan terhadap korban dan penegasan efek berbahaya dari *Cyberstalking* yang sering kali berdampak psikologis jangka panjang.[27]

Meskipun kerangka hukum relatif komprehensif, penegakan menghadapi tantangan signifikan. Pertama, pembuktian distress yang serius dan substansial seringkali sulit, karena dampak psikologis korban harus dibuktikan melalui laporan medis atau psikologis, yang bisa jadi menimbulkan beban tambahan bagi korban. Kedua, ruang lingkup kewenangan menjadi persoalan ketika pelaku beroperasi dari luar Inggris atau menggunakan server asing, sehingga menimbulkan hambatan yurisdiksi. Ketiga, bukti elektronik seringkali rentan dihapus atau dimanipulasi, sehingga menuntut investigasi digital forensik yang canggih. Selain itu, faktor anonimitas di dunia maya

[25] CPS. 2018. "Stalking or Harassment." *cps.gov.uk*. https://www.cps.gov.uk/legal-guidance/stalking-or-harassment?utm_source.

[26] CPS. 2018. "Stalking or Harassment." *cps.gov.uk*. https://www.cps.gov.uk/legal-guidance/stalking-or-harassment?utm_source.

[27] Fullbrook, S. 1998. "The Protection From Harassment Act." *The British journal of theatre nursing : NATNews : the official journal of the National Association of Theatre Nurses* 7(11): 18–20.

mempersulit identifikasi pelaku, terutama ketika menggunakan akun palsu atau jaringan anonim. Tidak kalah penting, terdapat risiko penyalahgunaan komunikasi anonim, di mana pelaku berulang kali membuat akun baru untuk melanjutkan perilaku stalking, sehingga menuntut strategi penegakan hukum yang lebih adaptif dan kolaboratif.[28]

d. Keteraturan, Regulasi Serta Relevansi Teknologi dan Media Sosial

Kehadiran legislasi khusus yang mengatur tentang stalking dan *Cyberstalking* dengan unsur-unsur yang tegas merupakan kebutuhan mendesak dalam menghadapi perkembangan kejahatan digital. Inggris, melalui *Protection from Harassment Act* 1997 yang kemudian diperkuat dengan amandemen dalam *Protection of Freedoms Act* 2012, memberikan dasar hukum jelas terkait perbuatan *stalking*, termasuk bentuk yang dilakukan secara daring. Kejelasan unsur, seperti tindakan berulang *(course of conduct),* tujuan mengganggu atau menimbulkan *distress*, serta kualifikasi ancaman kekerasan atau alarm serius, menjadikan regulasi ini sesuai dengan asas legalitas. Hal ini penting agar aparat penegak hukum dan korban memiliki kepastian hukum dalam membedakan perbuatan yang sah secara hukum dengan tindak pidana *stalking*.

Selain aspek pidana, regulasi di Inggris juga mengakui perlunya mekanisme perlindungan perdata untuk melindungi korban secara lebih efektif. Pengadilan dapat mengeluarkan *Restraining Orders maupun Stalking Protection Orders* (SPOs), yang berlaku baik dalam konteks tindak pidana maupun secara mandiri. Instrumen hukum ini memungkinkan korban memperoleh perlindungan tanpa harus menunggu proses pidana selesai. Dengan demikian, sistem hukum Inggris menghadirkan keseimbangan antara sanksi pidana yang bersifat represif dengan perintah perdata yang lebih preventif. Kombinasi ini meningkatkan fleksibilitas penegakan hukum serta memastikan perlindungan korban secara komprehensif dari tindakan *stalking*, termasuk yang dilakukan secara daring.

Definisi *stalking* dalam hukum Inggris secara eksplisit mengakomodasi perilaku yang dilakukan melalui media elektronik dan platform digital. Tindakan seperti pengiriman pesan berulang melalui email, media sosial, atau aplikasi pesan instan, pemantauan aktivitas daring korban, hingga penyalahgunaan informasi pribadi secara *online*, dapat dikualifikasikan sebagai bentuk *stalking* atau harassment. Dengan memasukkan perilaku daring dalam definisi hukum, regulasi ini tetap relevan terhadap dinamika teknologi modern. Media sosial yang memberikan kemudahan interaksi sekaligus potensi penyalahgunaan, menjadi ruang di mana *Cyberstalking* paling sering terjadi, sehingga kejelasan definisi sangat penting untuk menjamin bahwa hukum tetap adaptif terhadap perkembangan teknologi.

e. Perbandingan Pengaturan Tindak Pidana *Cyberstalking* di Indonesia dan Inggris dalam Perspektif Al-Qur'an

Regulasi *Cyberstalking* antara Indonesia dan Inggris menunjukkan adanya perbedaan yang signifikan dalam aspek komprehensivitas, kepastian hukum, dan perlindungan korban. Indonesia masih mengandalkan ketentuan yang tersebar dalam UU ITE dan KUHP, yang belum secara eksplisit menyebut *Cyberstalking* sebagai tindak pidana khusus. Unsur pelecehan, gangguan, maupun intimidasi daring sering kali diproses melalui pasal-pasal umum seperti penghinaan, ancaman, atau pencemaran nama baik. Hal ini menimbulkan problem kekosongan hukum karena tidak semua bentuk *Cyberstalking* dapat terakomodasi, terlebih dalam aspek pembuktian bukti digital dan identifikasi pelaku[1].

[28] Home Office, UK Goverment. 2021. "The Safety Of Women And Girls Across The Country Is Our Priority July 2021." *H.M. Government of United Kingdom and Northern Ireland* Chapter 28(July).

Sebaliknya, Inggris memiliki perangkat hukum yang lebih terstruktur, seperti *Protection from Harassment Act* 1997 yang diperluas dengan *Protection of Freedoms Act* 2012, serta dukungan dari *Communications Act* 2003. Regulasi ini secara eksplisit mendefinisikan *stalking*, termasuk dalam bentuk daring, dengan unsur *course of conduct* (tindakan berulang) yang menimbulkan *fear of violence* atau *serious alarm/distress*. Dengan adanya definisi yang jelas, hukum Inggris lebih menjamin asas legalitas dan melindungi korban melalui kombinasi sanksi pidana serta mekanisme perlindungan sipil seperti *Stalking Protection Orders.*

Dalam perspektif Al-Qur'an, kedua sistem hukum tersebut dapat dipahami melalui prinsip-prinsip syariat yang menekankan larangan menyakiti, mengintimidasi, atau melanggar privasi orang lain. Indonesia yang masih parsial dalam mengatur *Cyberstalking* sejalan dengan peringatan Al-Qur'an agar tidak menyakiti sesama tanpa hak (QS. Al-Ahzab:58):

وَالَّذِينَ يُؤْذُونَ الْمُؤْمِنِينَ وَالْمُؤْمِنَاتِ بِغَيْرِ مَا اكْتَسَبُوا فَقَدِ احْتَمَلُوا بُهْتَانًا وَإِثْمًا مُّبِينًا

Walladzīna yu'dzūnal-mu'minīna wal-mu'mināti bighairi mā iktasabū faqad ihtamalū buhtānan wa itsman mubīnan.[29]

"Dan orang-orang yang menyakiti orang-orang mukmin, baik laki-laki maupun perempuan tanpa kesalahan yang mereka perbuat, maka sungguh mereka telah memikul kebohongan dan dosa yang nyata."

Regulasi Inggris yang lebih jelas dalam mendefinisikan *stalking* justru lebih dekat dengan prinsip *hifz al-nafs* (perlindungan jiwa) dan *hifz al-'ird* (perlindungan kehormatan) dalam *maqashid al-syari'ah*. Larangan Al-Qur'an terhadap *tajassus* (memata-matai) dalam QS. Al-Hujurat:12 juga relevan dengan praktik *Cyberstalking,* di mana pelaku sering melanggar privasi korban:

وَلَا تَجَسَّسُوا

Wa lā tajassasū

"Dan janganlah kamu mencari-cari kesalahan orang lain."

Dengan demikian, perspektif Al-Qur'an menegaskan bahwa baik dalam konteks hukum Indonesia maupun Inggris, urgensi pengaturan *Cyberstalking* harus berorientasi pada perlindungan korban, penghormatan privasi, serta pencegahan gangguan psikologis maupun fisik. Perbedaan regulasi Indonesia dan Inggris dapat dilihat bukan hanya sebagai gap legal formal, tetapi juga sebagai peluang untuk menyempurnakan hukum nasional agar selaras dengan nilai-nilai keadilan universal yang terkandung dalam Al-Qur'an.

Tabel 1. Pengaturan Tindak Pidana *Cyberstalking* di Indonesia dan Inggris

Aspek	Indonesia	Inggris

[29] Al-Quran dan Terjemahan Universitas Islam Makassar,2021.

Dasar Hukum	UNDANG-UNDANG ITE (UNDANG-UNDANG No. 11/2008 jo. UNDANG-UNDANG No. 19/2016, UNDANG-UNDANG No. 1/2024), KUHP (Pasal penghinaan, ancaman, perbuatan tidak menyenangkan)	*Protection from Harassment Act 1997 (*Pasal 2A dan Pasal 4A*), Protection of Freedoms Act 2012, Communications Act 2003*
Definisi Perbuatan	Belum terdapat definisi khusus *cyberstalking* dalam peraturan perundang-undangan. Unsur-unsurnya tersebar dalam beberapa pasal, antara lain: • **Pasal 27 ayat (3)** tentang penghinaan/pencemaran nama baik melalui media elektronik; • **Pasal 27B** tentang pengiriman informasi elektronik yang bermuatan pemerasan atau ancaman; • **Pasal 29** mengenai ancaman kekerasan atau menakut-nakuti yang ditujukan secara pribadi melalui sistem elektronik. Ketentuan ini menunjukkan bahwa aspek *cyberstalking* di Indonesia masih bersifat parsial dan tersebar pada beberapa norma.	Pasal 2A *Protection from Harassment Act* mendefinisikan *stalking* sebagai "*a course of conduct*" dua atau lebih tindakan berulang seperti mengikuti, menghubungi, mengintai, memantau aktivitas daring, atau menyebarkan informasi pribadi yang menimbulkan *distress*, *alarm*, atau *fear of violence*. Pasal 4A mengatur bentuk berat apabila tindakan tersebut menyebabkan rasa takut akan kekerasan atau gangguan serius terhadap kehidupan korban.
Instrumen Perlindungan	Perlindungan masih terbatas: korban dapat melapor ke kepolisian berdasarkan ketentuan umum dalam Undang-Undang ITE dan KUHP, namun belum terdapat mekanisme khusus seperti *protection orders* atau perintah larangan berkomunikasi secara daring.	Tersedia *Restraining Orders* dan *Stalking Protection Orders (SPOs)* yang dapat diajukan secara pidana maupun perdata untuk mencegah kontak lebih lanjut, baik secara langsung maupun melalui media elektronik.
Sanksi Hukum	Sanksi dijatuhkan berdasarkan pasal-pasal relevan, seperti: • **Pasal 27 ayat (3)**: pidana penjara maksimal 4 tahun dan/atau denda maksimal Rp750 juta; • **Pasal 27B**: pidana penjara maksimal 4 tahun dan/atau denda maksimal Rp2 miliar; • **Pasal 29**: pidana penjara maksimal 4 tahun dan/atau denda maksimal Rp750 juta.	Berdasarkan *Pasal 4A Protection from Harassment Act*, pelaku *stalking* yang menyebabkan *fear of violence* atau *serious alarm/distress* dapat dipidana hingga **10** tahun penjara.

Kelemahan / Tantangan	Tidak ada definisi eksplisit *cyberstalking* sehingga aparat penegak hukum sering mengalami kesulitan pembuktian; selain itu, anonimitas pelaku dan rendahnya kesadaran korban menjadi hambatan dalam penegakan hukum.	Tantangan yang dihadapi meliputi pembuktian tingkat *distress* yang serius, pelacakan bukti elektronik, serta hambatan yurisdiksi internasional dalam kasus lintas negara.

4. Kesimpulan dan Saran

Berdasarkan hasil penelitian dan pembahasan yang telah diuraikan, dapat disimpulkan bahwa pengaturan hukum terkait tindak pidana *cyberstalking* di Indonesia masih bersifat parsial dan tersebar dalam beberapa peraturan perundang-undangan seperti Undang-Undang ITE (UU No. 11 Tahun 2008 jo. UU No. 1 Tahun 2024) serta KUHP, tanpa adanya ketentuan khusus yang secara eksplisit mengkriminalisasi *cyberstalking*. Pasal-pasal yang ada, seperti penghinaan, ancaman, atau pelecehan, hanya mencakup sebagian bentuk perilaku *cyberstalking*, sehingga masih terdapat kekosongan hukum terutama dalam aspek gangguan psikologis, intimidasi berulang, dan pelanggaran privasi digital. Kondisi ini menimbulkan kendala dalam penegakan hukum, baik dari segi pembuktian bukti digital, identifikasi pelaku anonim, maupun perlindungan korban secara komprehensif. Dalam perspektif Islam, Al-Qur'an menegaskan larangan terhadap segala bentuk gangguan dan ancaman sebagaimana tercantum dalam QS. Al-Hujurat (49:12) yang melarang mencari kesalahan orang lain dan QS. An-Nur (24:27) yang menekankan pentingnya menjaga privasi. Oleh karena itu, hukum Indonesia perlu bertransformasi agar lebih selaras dengan nilai moral Islam. Sementara itu, regulasi di Inggris jauh lebih komprehensif dan spesifik melalui *Protection from Harassment Act* 1997 serta *Protection of Freedoms Act* 2012 yang secara tegas mendefinisikan *stalking*, termasuk dalam bentuk daring *(cyberstalking)*, dengan unsur *course of conduct* atau tindakan berulang yang menimbulkan ketakutan akan kekerasan atau distress serius. Inggris juga menerapkan mekanisme *Stalking Protection Orders* dan *Restraining Orders* untuk memberikan perlindungan segera kepada korban serta menjatuhkan sanksi tegas hingga 10 tahun penjara untuk kasus serius. Hal ini menunjukkan bahwa regulasi Indonesia masih perlu diperkuat agar lebih komprehensif, adaptif terhadap perkembangan teknologi dan praktik hukum internasional, serta sejalan dengan prinsip keadilan dan perlindungan korban sebagaimana diajarkan dalam QS. Al-Isra (17:53) yang menegaskan larangan berbuat kezaliman atau menimbulkan permusuhan.

Diperlukan pembaruan hukum yang secara khusus mengatur tindak pidana *cyberstalking* di Indonesia dengan merumuskan definisi, unsur, serta sanksi pidana yang tegas dan proporsional. Pemerintah perlu menyusun peraturan turunan dari UU ITE atau bahkan membuat undang-undang baru yang berfokus pada kejahatan berbasis teknologi, termasuk mekanisme perlindungan korban dan penegakan hukum yang efektif. Selain itu, peningkatan kapasitas aparat penegak hukum dalam bidang digital forensics, penyelidikan lintas negara, serta edukasi publik mengenai bahaya *cyberstalking* perlu menjadi prioritas. Dengan demikian, Indonesia tidak hanya memperkuat fondasi hukum nasional, tetapi juga menegakkan nilai keadilan substantif yang sejalan dengan prinsip moral dan kemanusiaan.

Daftar Pustaka

Al-Qur'an dan Terjemahan. (2021). Universitas Islam Makassar.

Azahra, A. P., Simanjuntak, A. C. A., Tarigan, E. S., & Hosnah, A. U. (2024). Analisa kepada para oknum yang tidak bijak dalam menggunakan media sosial atau cyberspace. Civilia: Jurnal Kajian Hukum dan Pendidikan Kewarganegaraan, 3(1), 34–47.

Benito, I. G. (2023). Online harassment and cyberstalking: A case study. Sortuz: Oñati Journal of Emergent Socio-Legal Studies, 13(2), 242–257.

Callender Smith, R. (2022). Protection of Harassment Act 1997: From anti-stalking crimes to celebrity privacy remedies. Queen Mary Law Journal, 5, 23–37.

Crown Prosecution Service (CPS). (2018). Stalking or harassment. Retrieved from https://www.cps.gov.uk/legal-guidance/stalking-or-harassment

El Asam, A., & Samara, M. (2021). Cyberbullying and the law: A review of psychological and legal challenges. Computers in Human Behavior, 65, 127–141.

Fullbrook, S. (1998). The Protection from Harassment Act. The British Journal of Theatre Nursing (NATNews): The Official Journal of the National Association of Theatre Nurses, 7(11), 18–20.

Habibi, M. R., & Liviani, I. (2020). Kejahatan teknologi informasi (cyber crime) dan penanggulangannya dalam sistem hukum Indonesia. Al-Qanun: Jurnal Pemikiran dan Pembaharuan Hukum Islam, 23(2), 400–426. https://doi.org/10.15642/alqanun.2020.23.2.400-426

Home Office, UK Government. (2021). The safety of women and girls across the country is our priority (July 2021). H.M. Government of United Kingdom and Northern Ireland, Chapter 28.

Idris, J. I., & Supandi, A. (2024). Evaluasi kebijakan Undang-Undang Informasi dan Transaksi Elektronik di Indonesia: Potret bibliometric analysis. Transparansi: Jurnal Ilmiah Ilmu Administrasi, 7(1), 149–162.

Juharwati. (2024). Jerat hukum pelaku cyberstalking dalam Undang-Undang ITE 2024 dan KUHP (KUHP saat ini dan masa mendatang/Undang-Undang/1/2023). Hoc, 1. Retrieved from https://www.hukumonline.com/klinik/a/jerat-hukum-pelaku-plagiat-skripsi-cl2503/

Listiawati, N. (2023). Apa itu cybertalking? Kepolisian Daerah Kepulauan Riau (Polda Kepri). Retrieved from https://pid.kepri.polri.go.id/apa-itu-cybertalking/?utm_source

Nurdayati, et al. (2021). Eksistensi keamanan siber terhadap tindakan cyberstalking dalam sistem pertanggungjawaban pidana cybercrime. Syntax Literate: Jurnal Ilmiah Indonesia, 6(4), 1554–1572.

Oktavany, L. (2021). Terbentuknya cyberstalking pada media sosial Instagram (Doctoral dissertation, Universitas Islam Riau).

Pandie, M. M., & Weismann, I. T. J. (2021). Pengaruh cyberbullying di media sosial terhadap perilaku reaktif sebagai pelaku maupun korban cyberbullying pada siswa Kristen SMP Nasional Makassar. Jurnal Jaffray, 14(1), 43–62.

Pratama, A. Y., Nugroho Br, H. A. D., Astinda, A. N. R., & Adhipradana, Y. A. (2024). Legal standing. Legal Standing: Jurnal Ilmu Hukum, 8(3), 242–255.

Pratama, F. H., Purnomo, F., Zannethi, M. B., & Supriyadi, T. (2024). Analisa dampak psikologis cyberbullying terhadap korban. Liberosis: Jurnal Psikologi dan Bimbingan Konseling, 3(3), 11–20.

Rumlus, M. H., Kusmiadi, M. E., Rajab, A. M., & Pamungkas, A. C. (2023). Kebijakan penanggulangan tindak pidana cyberstalking pada media elektronik. Equality Before The Law, 3(2), 101–116. https://doi.org/10.36232/equalitybeforethelaw.v3i2.461

Saragih, A. E., Christian, N., & Khoirunisa, P. (2024). Analisis penggunaan barang bukti digital di dalam sistem hukum di Indonesia (Studi Kasus Putusan Nomor 3 K/Pid.Sus/2019). Media Hukum Indonesia, 2(2), 504. https://doi.org/10.5281/zenodo.12082755

Sitanggang, A. S., Darmawan, F., & Saputra, D. (2024). Hukum siber dan penegakan hukum di Indonesia: Tantangan dan solusi memerangi kejahatan siber. Jurnal Pendidikan dan Teknologi Indonesia, 4(3), 79–83. https://doi.org/10.52436/1.jpti.409

Yustia, M. (2010). Pembuktian dalam hukum pidana Indonesia terhadap cyber crime. Pranata Hukum, 5(2), 267–274.