



Tindak Pidana *Cyberstalking* Ditinjau dari Undang-Undang Nomor 1 Tahun 2024 tentang Informasi dan Transaksi Elektronik (ITE)

Khusnul Latifah^{1*}, Anita Zulfiani²
¹⁻² Universitas Sebelas Maret, Indonesia

Alamat: Jl. Ir. Sutami 36 Kentingan, Jebres, Surakarta, Jawa Tengah, Indonesia

Korespondensi penulis: khusnullaa1439@student.uns.ac.id *

Abstract. *The development of information and communication technology has changed the pattern of human interaction, which was initially done face-to-face, to digital. The positive impact of internet usage is to facilitate connection and access to information, but it can also result in negative impacts such as cybercrime. The purpose of this research is to determine the crime of cyberstalking reviewed from Law Number 1 of 2024 concerning the Second Amendment to Law Number 11 of 2008 concerning Information and Electronic Transactions (ITE). This research is normative legal research that is prescriptive and uses a statutory approach, case approach, and conceptual approach. The collection of legal materials uses literature study techniques or document studies using syllogistic analysis techniques and using deductive thinking patterns. From the research, it was found that cyberstalking can be in the form of stalking followed by sexual harassment, privacy interference and continuous threats. In addition, cyberstalking is regulated in Law Number 1 of 2024 concerning Information and Electronic Transactions. However, this law has not been clearly or specifically regulated regarding stalking in the digital realm. Therefore, we need strict regulations regarding cyberstalking crimes.*

Keywords: *Cyberstalking, Criminalization, ITE Law*

Abstrak. Perkembangan teknologi informasi dan komunikasi telah mengubah pola interaksi manusia yang awalnya dilakukan dengan cara bertatap muka menjadi digital. dampak positif penggunaan internet adalah mempermudah koneksi dan akses informasi, namun juga dapat mengakibatkan adanya dampak negatif seperti kejahatan siber (*cybercrime*). Tujuan dari dilaksanakannya penelitian ini untuk mengetahui tindak pidana *cyberstalking* ditinjau dari Undang-Undang Nomor 1 Tahun 2024 Tentang Perubahan Kedua Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik (ITE). Penelitian ini merupakan penelitian hukum normatif yang bersifat preskriptif dan menggunakan pendekatan perundang-undangan, pendekatan kasus serta pendekatan konseptual. Pengumpulan bahan hukum menggunakan tehnik studi kepustakaan atau studi dokumen dengan menggunakan tehnik analisis silogisme dan menggunakan pola pikir deduktif. Dari penelitian diperoleh bahwa perbuatan *cyberstalking* dapat berupa perbuatan penguntitan yang dikuti oleh pelecehan seksual, gangguan privasi dan acaman secara terus menerus. Selain itu perbuatan *cyberstalking* ini diatur dalam Undang-Undang Nomor 1 Tahun 2024 Tentang Informasi dan Transaksi Elektronik. Namun, dalam undang-Undang ini belum diatur secara jelas atau spesifik mengenai perbuatan menguntit di dalam ranah digital. Oleh karena itu, diperlukan pengaturan yang tegas terkait tindak pidana *cyberstalking*.

Kata kunci: *Cyberstalking, Pemidanaan, Undang-Undang ITE*

1. LATAR BELAKANG

Manusia merupakan makhluk sosial yang tidak bisa hidup tanpa berdampingan dengan manusia lainnya. Manusia disebut sebagai makhluk sosial karena manusia memiliki dorongan dan kebutuhan untuk berinteraksi dengan orang lain baik secara langsung maupun tidak langsung. Sebelum era digital, interaksi sosial hanya terbatas dengan pertemuan tatap muka atau komunikasi secara langsung melalui saluran telepon atau surat menyurat tradisional. Di era globalisasi sekarang, perkembangan internet semakin pesat terutama di bidang teknologi

telekomunikasi dan teknologi komputer. Dengan adanya perkembangan yang semakin pesat ini, manusia yang sebelumnya melakukan interaksi secara tatap muka atau surat menyurat harus beralih ke bentuk interaksi elektronik. Penggunaan email, aplikasi chatting dan platform media sosial memungkinkan individu untuk saling berkomunikasi dengan lebih praktis dan efisien. Hal ini tidak hanya mengubah cara manusia dalam berkomunikasi namun juga mempengaruhi hubungansosial serta perubahan dinamika masyarakat(Ginting et al., 2024: 1-2).

Dari adanya kemajuan yang sangat pesat pada teknologi telekomunikasi dan teknologi komputer dapat menghasilkan jaringan komputer yang multifungsi. Jaringan internet yang multifungsi dapat menimbulkan pengaruh positif bagi masyarakat akan tetapi dapat juga membawa pengaruh negatif dalam kehidupan sosial. Pengaruh positif dari perkembangan internet dapat dilihat dari adanya kemudahan akses dan konektivitas global, hal ini memudahkan seseorang dalam berkomunikasi tanpa adanya batas waktu. Namun, dibalik dampak positif tersebut terdapat dampak negatif berupa meningkatnya ancaman terhadap keamanan data dan sistem, khususnya melalui jaringan internet, yang menjadi bagian dari tindak kejahatan berbasis komputer. Seiring dengan pesatnya pertumbuhan teknologi internet, muncul juga fenomena kejahatan siber (*cybercrime*) (Azhari, 2019: 151). *Cybercrime* dalam arti sempit merujuk pada kejahatan terhadap sistem komputer. Namun, secara luas *cybercrime* diartikan dengan kejahatan terhadap sistem atau jaringan komputer serta kejahatan yang melibatkan penggunaan sarana komputer (Mohamad Revaldy et al., 2024: 140-141).

Penyelesaian pada kejahatan siber (*cybercrime*) di Indonesia terus mengalami peningkatan, namun dalam prakteknya masih banyak mengalami banyak hambatan. dengan adanya pebentukan Undang-Undang Informasi dan Transaksi Elektronik (ITE) merupakan salah satu upaya penanganan atas adanya tindak kejahatan siber (*cybercrime*). Namun, faktanya, implementasi terhadap undang-undang ini sering menimbulkan perdebatan dan kritik karena dianggap tidak jelas dan berpotensi menekan kebebasan berpendapat. Selain Undang-Undang Informasi dan Transaksi Elektronik (ITE) terdapat beberapa peraturan yang berkaitan dengan kejahatan siber (*cybercrime*). Dengan adanya regulasi yang berkaitan dengan informasi ini saja masih terdapat celah hukum dan kerangka regulasi yang kurang. Kekurangan ini dapat berupa ketentuan yang belum jelas mengenai penegakan hukum terhadap pelaku kejahatan siber, serta kurangnya sanksi yang memadai untuk pelanggaran keamanan siber, hal ini disebabkan karena adanya beberapa hal seperti sumber daya dan dana yang terbatas serta tenaga kerja dan teknologi yang kurang memadai. Kurangnya kesadaran masyarakat atas bahayanya kejahatan siber dan kurangnya Kerjasama antar lembaga ini juga

dapat menjadikan tantangan besar dalam menghadapi kejahatan siber (*cybercrime*) (Mustam, 2023: 10-11).

Terdapat banyak kasus kejahatan siber di Indonesia yang diakibatkan dengan adanya dampak negatif dari perilaku menyimpang yang dianggap sebagai sisi gelap komunikasi berbasis teknologi yaitu dengan adanya kejahatan *cyberstalking*. *Cyberstalking* merupakan perbuatan mengganggu atau melecehkan seseorang dengan memanfaatkan teknologi modern. Melalui teknologi ini, pelaku dapat mengakses informasi pribadi korban dan menyalahgunakan untuk kepentingan pribadi (Putri, 2024: 2).

Jurnal Internasional Kriminologi siber mendefinisikan *cyberstalking* sebagai tindakan terus menerus mengancam, melecehkan atau mengintimidasi seseorang secara daring. *Cyberstalking* dapat disebut pelecehan terselubung karena pelaku *Cyberstalking* tidak pernah meninggalkan pandangan terhadap korban saat mengawasi mereka secara daring. Dalam upaya meneror targetnya, pelaku *cyberstalking* kerap menggunakan berbagai akun anonim untuk mengirim pesan secara berulang bahkan sampai beberapa kali dalam sehari (Nabih Amer et al, 2022: 1)

Kejahatan *cyberstalking* sendiri banyak terjadi di Indonesia. Namun dalam penelitian ini penulis tertarik pada satu kasus *cyberstalking* yang terjadi di Surabaya sebagaimana kasus ini telah diputus di Pengadilan Negeri Surabaya dengan Putusan Nomor 1842/Pid.Sus/2024/PN Sby. Dalam kasus ini pelaku tindak pidana *cyberstalking* melakukan aksinya kurang lebih selama 10 (sepuluh) tahun. Kasus ini berawal dari korban yang mengaku mendapat teror terus menerus dari pelaku selama 10 (sepuluh) tahun. Pelaku diduga membuat ratusan akun media sosial berbagai platform media sosial seperti Instagram, Twitter hingga WhatsApp agar dapat menghubungi korban secara terus menerus. Pelaku sendiri sering mengirimkan pesan godaan dan pelecehan kepada korban hampir setiap hari, tidak hanya itu pelaku diduga sering mengirimkan foto yang mengandung unsur pornografi dan mengajak korban untuk menikah dengan pelaku. Tidak hanya mengganggu korban saja, pelaku juga sempat mengganggu priapria yang sempat dekat dengan korban dengan melontarkan ancaman bernada pembunuhan. Dengan perbuatan pelaku korban mengalami gangguan kecemasan sampai dengan depresi.

2. METODE PENELITIAN

Penelitian ini menggunakan metode penelitian hukum normatif atau penelitian doktrinal. Penelitian hukum normatif merupakan suatu proses untuk menemukan suatu aturan hukum, prinsip hukum maupun doktrin-doktrin hukum untuk menjawab permasalahan hukum yang dihadapi. Sumber bahan hukum penelitian ini diperoleh dari buku yang ditulis oleh ahli, jurnal-jurnal hukum dan hasil penelitian hukum. Dalam penelitian ini penulis menggunakan pendekatan undang-undang, kasus dan konseptual. Penelitian ini bersifat preskriptif dengan menyampaikan argumentasi terkait hasil penelitian yang dilakukan. Tehnik analisis terhadap bahan-bahan hukum ini menggunakan metode silogisme dan menggunakan pola berfikir yang bersifat deduktif.

3. HASIL DAN PEMBAHASAN

Kasus Cyberstalking dalam Putusan Nomor 1842/Pid.Sus/2024/PN Sby

Menurut dakwaan dalam Putusan Nomor 1842/Pid.Sus/2024/PN Sby. Kasus ini bermula dari kesaksian korban yang disampaikan melalui media sosial Twitter yang mengungkap adanya pengalaman pelecehan dan teror yang berlangsung selama kurang lebih sepuluh tahun oleh seorang teman semasa SMP. Awalnya, hubungan korban dan pelaku berawal dari rasa empati, yakni saat korban memberikan uang jajan kepada pelaku. Namun, pemberian tersebut disalahartikan sebagai bentuk ketertarikan emosional yang kemudian berkembang menjadi perilaku obsesif dari pelaku.

Seiring berjalannya waktu, pelaku menunjukkan pola pelecehan yang semakin intens, antara lain mengirim pesan bermuatan seksual, foto eksplisit, dan menguntit baik secara daring maupun luring. Dalam kurun waktu 2016 hingga 2024, pelaku diketahui telah membuat sekitar 400 akun media sosial fiktif untuk memantau aktivitas daring korban, meski akun tersebut telah berulang kali diblokir.

Selain itu, pelaku juga mengirimkan gambar tidak senonoh dan memanipulasi foto korban secara digital menggunakan teknologi berbasis kecerdasan buatan untuk membuat gambar eksplisit tanpa izin. Tindakan tersebut berdampak psikologis serius pada korban, sebagaimana dikonfirmasi melalui evaluasi lembaga kesehatan dan psikologi forensik.

Tindak Pidana *Cyberstalking* Sebagai Salah Satu Bentuk Tindak Pidana Siber (*Cybercrime*)

Cybercrime pada umumnya dianggap juga sebagai computer crime. Menurut Wisubroto, kejahatan komputer merupakan perbuatan melawan hukum yang dilakukan dengan menggunakan komputer sebagai fasilitas atau perlengkapan komputer sebagai objek, baik memperoleh keuntungan maupun tidak dengan merugikan pihak lain. Dalam artian kejahatan komputer diartikan sebagai perbuatan yang bersifat ilegal yang dilakukan dengan menggunakan teknologikomputer yang kompleks. Dari definisi diatas maka kejahatan komputer dapat disebut dengan istilah *cybercrime*(Habibi & Liviani, 2020: 407).

Cyberstalking merupakan perbuatan mengganggu dan/atau melecehkan seseorang yang dilakukan dengan memanfaatkan kemajuan teknologi. Dengan memanfaatkan kemajuan teknologi pelaku *cyberstalking* memperoleh data pribadi korban seperti alamat, nomor telfon, aktivitas media sosial, hingga informasi sensitif lainnya yang kemudian disalahgunakan untuk memenuhi kepentingan pribadi pelaku, selain itu definisi *cyberstalking* menurut Black's Law Dictionary Edisi ke-9, adalah sebagai berikut(Anisah, 2022: 164).

“The act of threatening, barrassing, or annoying someone via multiple e-mail message sent over the internet, especially with the intent of instilling fear recipient that illegal act or injury will be inflicted on the recipient, a member of the recipient's family or housebold”

“Mengancam, melecehkan atau mencoba mengintimidasi seseorang melalui berbagai komunikasi, seperti melalui internet, untuk menakut nakuti penerima kejahatan kriminal atau tindakan yang dilakukan penerima kerabatnya”

Istilah stalking sendiri memiliki arti yang bervariasi tergantung pada sitem hukum atau perundang-undangan yang berlaku di masing-masing negara. Meskipun demikian, secara umum stalking dapat di artikan sebagai suatu bentuk tindak pidana yang dilakukan secara sengaja oleh individu, yang dilakukan melalui berbagai tindakan, seperti membuntuti atau mengawasi seseorang secara berulang-ulang dengan tujaun untuk mengganggu, melecehkan atau menimbulkan rasa takut pada korban.Perilaku stalking dapat di lakukan oleh individu lain terhadap individu lainnya dan siapa saja yang memiliki sifat berupa prilaku mengganggu yang berulang-ulang. Protection of Harassment Act (PHA) 2017 mendeskripsikan perilaku *stalking* sendiri sebagai berikut (Andriyani, 2020: 150):

- a. Mengikuti seseorang;
- b. Mengontak atau berusaha mengontak orang lain dengan alasan apapun;
- c. Menyebarkan pertanyaan atau materi informasi mengenai orang lain;
- d. Mengawasi penggunaan internet, email atau komunikasi orang lain;
- e. Mengganggu properti pribadi orang lain; dan
- f. Mengawasi atau memata-matai orang lain.

Cyberstalking sendiri termasuk dalam salah satu bentuk *cybercrime* yang rumit dan saling berhubungan dengan kejahatan siber lainnya seperti penyebaran konten ilegal yang mengandung unsur pornografi, perjudian online, ujaran kebencian, serta tindakan pengancaman dan pemerasan secara daring. Selain itu, tindakan *cyberbullying* juga sering terjadi bersamaan dengan tindakan *cyberstalking*, dimana pelaku melakukan pencemaran nama baik, penghinaan atau penyebaran informasi palsu melalui internet yang dapat merusak reputasi dan kondisi psikologi korban. Tindakan-tindakan diatas umumnya dilakukan dengan memasukan atau menyebarkan data serta informasi palsu melalui internet yang bersifat meyesatkan, tidak etis atau tidak benar ke ranah digital. Keberadaan konten seperti ini tidak hanya melanggar norma dan etika masyarakat akan tetapi juga dapat berpotensi menimbulkan gangguan terhadap ketertiban umum serta menjadi pelanggaran terhadap hukum positif yang berlaku (Zakaria et al., 2022: 825).

Unsur-Unsur Tindak Pidana Cyberstalking

Seperti yang telah dijelaskan diatas tindak pidana *cyberstalking* merupakan bentuk gangguan atau pelecehan terhadap individu seseorang yang dilakukan melalui sarana teknologi digital. Menurut black law ditionary edisi ke-7 *cyberstalking* di definisikan sebagai berikut (Juharwati, 2024: 128):

“The act of threatening, harassing, or annoying someone through multiple email messages, as through the internet, esp. with the inten of placing the recipient in fear that an illegal act or an injury will be inflicted on the recipient or a member of the recipient’s family or household”

Dari definisi diatas terdapat unsur-unsur pokok dari tindak pidana *cyberstalking* yaitu:

1. *Act of threathening, harassing or annoying someone* (tindakan mengancam, melecehkan atau mengganggu seseorang);
2. *Through internet* (melalui internet);
3. *With the inten of placing the recipient in fear that an illegal act or an injury* (dengan maksud membuat korban takut akan tindakan ilegal atau cedera).

Bedasarkan definisi yang telah dibahas sebelumnya, dapat di simpulkan bahwa perbuatan *cyberstalking* mencakup beberapa unsur utama yaitu unsur mengancam (*threatening*), melecehkan (*harassing*) dan mengganggu (*annoying*). Perlu diingat bahwa ketiga unsur tersebut bersifat alternatif, sebagaimana ditunjukkan oleh penggunaan kata “atau” yang artinya, suatu tindakan dapat dikatakan sebagai tindak pidana *cyberstalking* meskipun hanya memenuhi salah satu unsur tersebut. Dengan kata lain, jika seseorang menggunakan media digital atau platform daring untuk melakukan tindakan yang menimbulkan rasa takut, tekanan psikologis, rasa tidak nyaman atau gangguan pada individu lain, maka tindakan tersebut sudah dapat dikatan sebagai tindakan stalking(Purnama & Haris, 2024: 110).

Dari unsur-unsur dan perilaku diatas dapat di simpulkan bahwa kasus *cyberstalking* pada Putusan Nomor 1842/Pid.Sus/2024/PN Sby Terdapat beberapa perbuatan yang termasuk dalam perbuatan *cyberstalking*, antara lain:

1. Adanya Perbuatan menguntit lewat media sosial dengan menggunakan banyak akun.

Dalam kasus ini, pelaku menggunakan sarana media elektronik dengan menggunakan sejumlah akun media sosial fiktif untuk melakukan perbatan penguntutan (*stalking*) terhadap korban melalui berbagai platform media sosial. Tindakan tersebut tidak hanya sebatas mengawasi kegiatan korban saja namun juga disertai dengan perilaku yang mengarah pada pelecehan seksual. pelaku seringkali mengirimkan foto-foto yang bermuatan pornografi kepada korban melalui pesan langsung (*direct message*).

2. Adanya tujuan yang bersifat seksual.

Tindakan pelaku menunjukkan bahwa adanya motif yang bersifat seksual. Hal ini dibuktikan dengan tindakan pelaku yang pernah meneror korban dengan mengirimkan gambar eksplisit melalui media sosial pribadinya kepada korban. Selain itu pelaku juga melakukan manipulasi digital berupa foto-foto korban tanpa seizin korban. Foto-foto tersebut diedit tanpa seizin korban dengan maksud untuk memenuhi fantasi seksual pelaku atau untuk kepentingan distribusi konten bermuatan seksual.

3. Adanya perbuatan mengganggu korban

Dalam kasus ini, pelaku secara langsung dan terus menerus melakukan tindakan mengganggu terhadap korban melalui berbagai platform media sosial. Pelaku seringkali mengirimkan pesan secara berulang kepada korban meskipun pesan-pesan tersebut tidak direspon dan korban telah melakukan pemblokiran akun milik pelaku. Namun demikian, pelaku tetap membuat akun-akun baru untuk kembali menghubungi mengganggu dan mengawasi aktivitas harian korban di media sosial.

4. Adanya perbuatan mengancam terhadap korban

Dalam kasus ini, secara terus menerus melakukan tindakan mengancam terhadap korban melalui pesan langsung di akun media sosial korban. pesan-pesan tersebut berisi unsur pengancaman dan teror yang berpotensi menimbulkan ketakutan serta tekanan psikologis pada korban. Tidak hanya itu pelaku juga menyampaikan berbagai kata-kata yang bersifat merendahkan, kasar dan tidak pantas kepada korban, hal ini dapat dikategorikan sebagai pelecehan verbal di platform media sosial.

Pemidanaan Terhadap Pelaku Tindak Pidana *Cyberstalking* Ditinjau Dari Undang-Undang Nomor 1 Tahun 2024 Tentang Informasi Dan Transaksi Elektronik

Cyberstalking merupakan salah satu bentuk kejahatan siber (*cybercrime*) yang menunjukkan peningkatan seiring pesatnya perkembangan teknologi digital. Di Indonesia, upaya pengaturan hukum terhadap tindak pidana ini dilakukan melalui pendekatan regulatif, terutama melalui Undang-Undang Nomor 1 Tahun 2024 Tentang Perubahan Kedua Atas Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik serta diatur juga dalam ketentuan Kitab Undang-Undang Hukum Pidana (KUHP). Akan tetapi, meskipun telah ada peraturan yang mengatur, efektivitas implementasi masih sering menjadi sorotan. Hal ini disebabkan oleh berbagai tantangan, khususnya dalam aspek legalitas dan kepastian hukum, mengingat *cyberstalking* merupakan bentuk kejahatan yang bersifat rumit dan multidimensional sehingga memerlukan pendekatan hukum yang lebih dapat beradaptasi dan spesifik (Wahyuningsih, 2025: 3).

Bedasarkan Perbuatan diatas, Kejahatan *cyberstalking* dapat diatur dalam Undang-Undang Nomor 1 Tahun 2024 Tentang Perubahan Kedua Atas Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik. Pasal-Pasal yang dapat termasuk kedalam perbuatan *cyberstalking* adalah sebagai berikut:

- a. Pasal 27B Undang-Undang Nomor 1 Tahun 2024 Tentang Perubahan Kedua Atas Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik yang berbunyi:
 - (1) Setiap orang dengan sengaja dan tanpa hak mendistribusikan dan/atau mentransmisikan informasi 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 besar atau seluruhnya milik orang tersebut atau milik orang lain,
 - b. Memberi utang membuat pengakuan utang atau menghapuskan piutang.
- (2) 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 dengan ancaman pencemaran atau dengan ancaman akan membuka rahasia, memaksa orang supaya:
- 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.
- b. Pasal 29 Undang-Undang Nomor 1 Tahun 2024 Tentang Perubahan Kedua Atas Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik yang berbunyi:
- “Setiap Orang dengan sengaja dan tanpa hak Informasi Elektronik dan/atau Dokumen Elektronik secara langsung kepada korban yang berisi ancaman kekerasan dan/atau menakut-nakuti”.
- c. Pasal 45B Undang-Undang Nomor 1 Tahun 2024 Tentang Perubahan Kedua Atas Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik yang berbunyi:
- “Setiap Orang yang dengan sengaja dan tanpa hak mengirimkan Informasi Elektronik dan/atau Dokumen Elektronik secara langsung kepada korban yang berisi ancaman kekerasan dan/atau menakut-nakuti sebagaimana dimaksud dalam Pasal 29 dipidana dengan pidana penjara paling lama 4 (empat) tahun dan/atau denda paling banyak Rp750.000.000,00 (tujuh ratus lima puluh juta rupiah)”.

Pada Putusan Nomor 1842/Pid.Sus/2024/PN Sby terdapat dua pasal yang dijatuhkan kepada terdakwa, antara lain:

- a. Pasal 45B jo Pasal 29 Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik sebagaimana terakhir diubah dengan Undang-Undang Nomor 1 Tahun 2024 tentang Perubahan Kedua atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik yang berbunyi: “Dengan sengaja dan tanpa hak mengirimkan informasi elektronik dan/atau dokumen elektronik secara langsung kepada korban yang berisi ancaman kekerasan dan/atau menakut-nakuti”.

- b. Pasal 14 ayat (1) huruf b Undang-Undang Nomor 12 Tahun 2022 Tentang Tindak Pidana Kekerasan Seksual yang berbunyi “Pasal 14 ayat (1) huruf c Undang-Undang Nomor 12 Tahun 2022 Tentang Tindak Pidana Kekerasan Seksual yang berbunyi: “Mentransmisikan informasi elektronik dan/atau dokumen elektronik yang bermuatan seksual di luar kehendak penerima yang ditujukan terhadap keinginan seksual”

Berdasarkan ketentuan yang telah dijabarkan diatas maka belum terdapat penjelasan secara rinci mengenai batasan serta bentuk penegakan hukum terhadap pelaku penguntitan yang memanfaatkan media elektronik atau teknologi informasi, terutama jika tindakan tersebut menimbulkan gangguan secara tidak langsung. Sebagaimana telah dijelaskan sebelumnya, *cyberstalking* merupakan tindakan penguntitan yang dilakukan di ranah sosial media, namun konsep “membuntuti” secara spesifik belum tercermin dalam norma-norma pasal yang ada dalam Undang-Undang Informasi dan Transaksi Elektronik (ITE). Hal ini menunjukkan bahwa perlunya pengaturan yang lebih tegas dan menyeluruh mengenai *cyberstalking* agar masyarakat memiliki pemahaman yang jelas mengenai batasan perilaku yang dapat dikategorikan sebagai tindak pidana. Dalam kondisi ini, urgensi perlindungan privasi dari ancaman *cyberstalking* semakin berkembang dan menuntut hadirnya kebijakan hukum pidana yang memberikan perlindungan nyata kepada korban. Selain itu, pemidanaan terhadap pelaku *cyberstalking* juga perlu dirumuskan secara tegas dan terukur guna mendukung penegakan hukum yang efektif serta efisien (Partisya et al., 2024: 10).

4. KESIMPULAN DAN SARAN

Berdasarkan analisis terhadap unsur-unsur dan perilaku yang terlibat dalam kasus *cyberstalking* pada Putusan Nomor 1842/Pid.Sus/2024/PN Sby, dapat disimpulkan bahwa suatu perbuatan tindak pidana *cyberstalking* mencakup berbagai bentuk penguntitan diantaranya seperti pelecehan seksual, gangguan privasi dan ancaman yang berpotensi menimbulkan ketakutan serta tekanan psikologi terhadap korban.

Berdasarkan ketentuan yang ada, belum ada penjelasan rinci mengenai batasan dan bentuk penegakan hukum terhadap pelaku *cyberstalking* yang memanfaatkan media elektronik. UU ITE tidak mengatur secara khusus mengenai konsep “stalking” dalam konteks digital. Maka pemidanaan terhadap tindak pidana *cyberstalking* dapat dipidana dengan Pasal 27B, Pasal 29 dan Pasal 45B Undang-Undang Nomor 1 Tahun 2024 Tentang Perubahan Kedua Atas Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik. Oleh karena itu, diperlukan pengaturan yang tegas dan komprehensif agar

masyarakat memahami batasan perilaku yang dianggap sebagai tindak pidana. Mengingat semakin meningkatnya ancaman terhadap privasi, kebijakan hukum pidana harus hadir untuk memberikan perlindungan yang nyata kepada korban dan hukuman yang jelas bagi pelaku.

DAFTAR REFERENSI

- Andriyani, S. N., & Helmi, A. F. (2020). *Riset-riset cyberpsychology* (pp. 252–281).
- Anisah, A. P., & Nurisman, E. (2022). Cyberstalking: Kejahatan terhadap perlindungan data pribadi sebagai pemicu tindak pidana. *Krtha Bhayangkara*, 16(1), 163–176. <https://doi.org/10.31599/krtha.v16i1.1047>
- Azhari, M. R. (2019). Aspek pidana mayantara (cyberstalking). *Badamai Law Journal*, 4(1), 150. <https://doi.org/10.32801/damai.v4i1.9234>
- Fairuzzen, M. R., Putra, A. A., Reihan, A., & Prihatini, L. (2024). Perkembangan hukum dan kejahatan siber “cybercrime” di Indonesia. *Indonesian Journal of Islamic Jurisprudence, Economic and Legal Theory*, 2(1), 139–153. <https://doi.org/10.62976/ijijel.v2i1.372>
- Ginting, D. C. A., Rezeki, S. G., Siregar, A. A., & Nurbaiti. (2024). Analisis pengaruh jejaring sosial terhadap interaksi sosial di era digital. *Pusat Publikasi Ilmu Manajemen*, 2(1), 22–29. <https://ejournal-nipamof.id/index.php/PPIMAN/article/view/280>
- 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>
- Juharwati. (2024). Jerat hukum pelaku cyberstalking dalam UU ITE 2024 dan KUHP (KUHP saat ini dan masa mendatang/UU/1/2023). *HOC*, 1. <https://www.hukumonline.com/klinik/a/jerat-hukum-pelaku-plagiat-skripsi-cl2503/>
- Mustam, A. M. A. (2023). Memerangi kejahatan siber di Indonesia: Analisis regulasi hukum pidana yang berlaku dan tantangannya. *Jurnal Ilmiah Gema*, 35(1), 10–14. <https://journal.uniba.ac.id/index.php/GM/index/>
- Nabih Amer, Khuan, H., Paminto, S. R., Mamu, K. Z., & Rasyid, M. F. F. (2022). Cyberstalking crime and application of criminal law in Indonesia. [*Journal name not specified*], 4(2), 58–71.
- Partisya, R., & Universitas Jambi. (2024). Jurnal rectum Reza Partisya dilakukan dengan memanfaatkan kecanggihan teknologi: Dengan memanfaatkan bentuk pengiriman email yang bersifat abusive, yaitu kata-kata yang menyerang dengan perbandingan Amerika Serikat dan Jepang, 342–354. (Purnama, Y. F., & Haris, O. K. (2024). Cyberstalking sebagai perbuatan melawan hukum dalam hukum pidana Indonesia, 6(1), 103–121.

- Putri, H. A. (2024). Strategi pencegahan cyberstalking dan upaya perlindungan hukum. *Jurnal BATAVIA: Buletin Aksi Visi Penelitian Sosial Humaniora*, 1(2), 85–95.
- Wahyuningsih, K. R. (2025). Cyberstalking sebagai kejahatan multidimensional dalam hukum pidana Indonesia.
- Zakaria, H., Samsoni, & Mulyoto, A. (2022). Cyberstalking: Sebuah kejahatan di dunia maya yang berimplikasi hukum. *AMMA: Jurnal Pengabdian Masyarakat*, 1(7), 823–829.