ISSN (P): (2580-8656)
ISSN (E): (2580-3883)

LEGAL STANDING
JURNAL ILMU HUKUM

Vol.8 No.3, Desember 2024

PENEGAKAN TINDAK PIDANA *CYBERSTALKING* DALAM HUKUM POSITIF INDONESIA

Akbar Yudha Pratama[1], Hafidz Amrullah Dzaky Nugroho Br[2], *Afifudin Nur Rosyid Astinda[3], Yurista Ardien Adhipradana[4]
[1,2,3,4]Universitas Airlangga, Jl. Airlangga No.4 - 6, Surabaya, Jawa Timur, Indonesia
*afifudinnr18@gmail.com

ABSTRACT

Improper use of social media often leads someone to deal with the law. Many social media users are not aware of the legal consequences of wrong treatment, for example, speaking rudely, disturbing someone, harassing someone, cyberstalking, cyberbullying, and so on. The public only realizes the mistake when the victim brings the problem to law enforcement. The purpose of this study is to explain how to enforce cyberstalking crimes from a positive legal perspective. This study is a normative legal study with a statutory approach. In the implementation of regulations in Indonesia through the Electronic Information and Transactions Law (ITE) on many legal problems that occur on social media, it often makes the perpetrators surprised and regret their actions on social media. In addition, preventive measures are also very important in reducing the risk of cyberstalking.

Penggunaan media sosial yang tidak tepat, sering membawa seseorang berurusan dengan hukum. Banyak pengguna media sosial tidak menyadari akibat hukum dari perlakuan yang salah, sebagai contoh berbicara kasar, mengganggu seseorang, melecehkan seseorang, *cyberstalking*, *cyberbullying*, dan sebagainya. Masyarakat baru sadar atas kesalahan tersebut ketika korban membawa permasalahan tersebut kepada aparat penegak hukum. Tujuan penelitian ini adalah menjelaskan bagaimana penegakan tindak pidana *cyberstalking* dalam sudut pandang hkum positif. Penelitian ini merupakan penelitian hukum normatif dengan pendekatan perundang-undangan. Dalam implementasi peraturan di Indonesia melalui UU Informasi dan Transaksi Elektronik (ITE) pada banyak permasalahan hukum yang terjadi di media sosial, sering membuat pelaku terkejut dan menyesal atas perbuatannya yang dilakukan di media sosial. Selain itu langkah-langkah preventif juga sangat penting dalam mengurangi risiko terhadap *cyberstalking*.

Kata Kunci: *Penegakan Hukum, Pidana Cyberstalking, Hukum Positif.*

A. PENDAHULUAN

Menggunakan media sosial sudah menjadi suatu kebiasaan beberapa masyarakat untuk menuangkan beberapa ide-ide kreatifnya maupun hanya sekedar sebagai alat untuk menambah relasi. Namun tidak jarang juga media sosial disalahgunakan untuk kegiatan yang negatif seperti penguntitan atau penyusupan secara diam-diam yang tidak diizinkan oleh seseorang, tindakan negatif itu disebut sebagai istilah *cyberstalking* (Natalia & Atmadja, 2013).

Cyberstalking sebagai salah satu tindakan kejahatan dunia maya yang layak mendapat perhatian di tengah maraknya penggunaan media sosial yang semakin kurang terkontrol. Kebebasan berekspresi sering digunakan seseorang sebagai alasan untuk melakukan tindakan *cyberstalking*. Namun masyarakat sering terabaikan bahwa ada hal-hal yang tidak boleh dilakukan dalam berinteraksi di dalam media sosial karena dampaknya adalah tindak pidana yang serius (Albar et al., 2022).

Cyberstalking merujuk pada praktik menggunakan teknologi dan platform online untuk melakukan penguntitan, pengejaran, atau intimidasi terhadap seseorang tanpa izin atau persetujuan mereka. Dibandingkan dengan stalking konvensional, *cyberstalking* memanfaatkan berbagai media elektronik seperti email, media sosial, pesan teks, dan aplikasi pesan instan untuk mengganggu, mengintimidasi, atau bahkan mengancam korban secara virtual. Hal ini mencakup berbagai perilaku yang mencerminkan obsesi atau keinginan untuk mengontrol, memantau, atau menyakiti korban secara online, seringkali menimbulkan dampak psikologis yang serius dan melanggar privasi individu (Andespitrikasih et al., 2024).

Dalam konteks *cyberstalking*, pelaku seringkali menggunakan berbagai cara untuk menargetkan korban mereka. Mereka dapat melakukan pemantauan terus-menerus terhadap aktivitas online korban, termasuk melacak lokasi mereka melalui media sosial atau teknologi pelacakan, membanjiri mereka dengan pesan-pesan yang mengganggu atau mengancam melalui email atau pesan teks, atau bahkan menciptakan akun palsu untuk mendekati korban dengan identitas yang palsu. Seiring dengan kemajuan teknologi, pelaku yang melakukan kejahatan *cyberstalking* yang dikenal dengan *cyberstalkers* juga dapat menggunakan perangkat lunak atau alat otomatis untuk memantau dan melacak korban mereka dengan lebih efisien (Božić & Мичић, 2024).

Perlakuan yang diakibatkan dari *cyberstalking* seperti ini sering kali membuat korban merasa terisolasi, kehilangan rasa aman, dan merasa terus-menerus diawasi, mengganggu kehidupan sehari-hari mereka dan meningkatkan risiko gangguan mental dan emosional. Oleh karena itu, penting bagi individu dan lembaga untuk meningkatkan kesadaran tentang cyberstalking dan mengembangkan strategi perlindungan yang efektif dalam menghadapinya.

B. METODE

Penelitian ini merupakan penelitian hukum yang mengadopsi pendekatan perundang-undangan, dan pendekatan konseptual. Pendekatan perundang-undangan melibatkan penggunaan legislasi dan regulasi yang ada. Penelitian hukum normatif adalah prosedur penelitian ilmiah untuk mengungkapkan kebenaran berdasarkan logika hukum dari perspektif normatifnya. Dalam penelitian hukum normatif, ilmu hukum berfokus pada hukum itu sendiri. Sementara itu, pendekatan konseptual dilakukan manakala peneliti tidak beranjak dari regulasi yang ada, oleh karena itu penelitian ini

berpangkal pada Undang-Undang Informasi Dan Transaksi Elektronik. Sumber Bahan Hukum adalah asal dari mana data diperoleh, sumber bahan hukum yang digunakan dalam penelitian ini terbagi dalam dua jenis, yaitu sumber bahan hukum primer dan sumber bahan hukum sekunder. Sumber bahan hukum primer merupakan sumber bahan hukum yang terdiri atas peraturan perundang-undangan, catatan-catatan resmi atau risalah dalam pembentukan peraturan perundang-undangan serta putusan-putusan hakim. Sumber bahan hukum sekunder berupa publikasi tentang hukum meliputi buku-buku teks, kamus-kamus hukum, dan jurnal-jurnal hukum (Marzuki, 2016).

C. HASIL DAN PEMBAHASAN

1. *Cyberstalking* dalam Ruang Lingkup Tindak Pidana *Cyber*

Telah disadari bahwa kecanggihan teknologi komputer memberikan kemudahan terutama dalam membantu memudahkan pekerjaan manusia. Selain itu, kecanggihan teknologi komputer juga menjadi sebab munculnya kejahatan-kejahatan baru yang mana kejahatan itu diawali dengan memanfaatkan komputer sebagai modus operansinya (Maskun, 2014).

Tindak *cybercrime*, atau kejahatan dunia maya, merupakan tindakan melanggar hukum yang dilakukan dengan memanfaatkan teknologi komputer sebagai sarana utama kejahatan. Tindak kejahatan ini mencakup "kemampuan khusus di dunia maya," yang berarti jenis kejahatan baru yang memerlukan keahlian tertentu, setidaknya pemahaman tentang cara menggunakan komputer. *Cybercrime* terjadi dengan memanfaatkan perkembangan teknologi komputer, khususnya internet. Secara umum, *cybercrime* diartikan sebagai tindakan yang melanggar hukum dengan menggunakan teknologi komputer berbasis pada kemajuan internet dan media social (Royani, 2016).

Menurut Kepolisian Inggris, *cybercrime* mencangkup segala bentuk dalam menggunakan jaringan komputer untuk melakukan tindakan kriminal atau kejahatan berteknologi tinggi yang terjadi melalui penyalahgunakan teknologi digital. Kejahatan ini dianggap sebagai bagian dari dunia komunikasi berbasis komputer, yang dikenal dalam kehidupan sehari-hari sebagai “Internet” yaitu jaringan komputer global yang menghubungkan negara-negara dan benua-benua melalui protokol *transmission control protocal* (TCP) dan *internet protokol* (IP).

Kehadiran dunia maya (*cyber space*) merupakan sebuah realitas yang ada di dalam kehidupan manusia, yang dikenal dengan internet (Sugiarto et al., 2024). kehadiranya telah mengubah konsep jarak dan waktu, sehingga seolah-olah menjadi tak terbatas. Internet dapat digambarkan sebagai kumpulan besar jaringan komputer yang tersusun dari banyak jaringan kecil yang beroperasi dengan sistem yang beragam (Winarni, 2016).

Terdapat berbagai bentuk *cybercrime* yang sangat terkait dengan penggunaan teknologi berbasis komputer serta jaringan telekomunikasi, diantaranya:

a. *Unauthorized access to computer system and service*, adalah jenis kejahatan di mana seseorang secara ilegal memasuki suatu sistem jaringan komputer tanpa adanya izin dari pemiliknya. Biasanya pelaku (*hacker*) melakukan tindakan ini dengan tujuan untuk sabotase atau mencuri informasi yang bersifat penting dan rahasia. Namun, ada juga yang melakukannya semata-mata karena ingin menguji kemampuan mereka dalam menembus sistem yang memiliki perlindungan tinggi. Kejahatan ini semakin marak seiring dengan pesatnya berkembangnya teknologi internet.

b. *Illegal contents*, adalah bentuk kejahatan di mana seseorang menyebarkan data atau informasi melalui internet yang bersifat tidak benar, tidak sesuai etika, dan dianggap melanggar hukum serta dapat membuat keresahan di ketertiban umum.

c. *Data forgery*, adalah kejahatan yang dilakukan dengan memalsukan data pada dokumen-dokumen yang disimpan dalam bentuk digital melalui internet. Kejahatan ini sering kali menyasar pada dokumen-dokumen *e-commerce* dimana pelaku membuat seolah-olah terjadi kesalahan pengetikan yang pada akhirnya akan menguntungkan pada diri pelaku.

d. *Cyber espionage*, adalah bentuk kejahatan yang menggunakan jaringan internet untuk melakukan kegiatan mata-mata terhadap pihak lain, dengan cara menyusup ke dalam sistem jaringan komputer (*computer network system*) pihak sasaran. Biasanya kejahatan ini menargetkan pesaing bisnis atau data penting yang disimpan dalam sistem komputerisasi.

e. *Cyber sabotase and extortion*, adalah kejahatan yang dilakukan dengan cara mengangguan, merusak atau pmenghancurkan data, program komputer atau sistem jaringan komputer yang terhubung dengan internet. Biasanya, tindakan ini dilakukan dengan memasukan *logic bomb*, virus komputer atau program tertentu yang menyebabkan data, program komputer atau sistem jaringan komputer tidak bisa digunakan, tidak berfungsi sebagaimana mestinya, atau beroperasi sesuai dengan keinginan pelaku. Dalam beberapa kasus, setelah sabotase terjadi, maka pelaku menawarkan jasanya untuk memperbaiki kerusakan tersebut, tentunya dengan imbalan dari korbannya.

f. *Offence against intellectual property*, adalah kejahatan yang menyerang hak kekayaan intelektual seseorang di dunia maya. contohnya termasuk peniruan desain atau tampilan halaman milik pihak lain secara ilegal, atau penyebaran informasi melalui internet yang sebenarnya merupakan rahasia dagang milik orang lain, dan tindakan serupa lainnya.

g. *Infringements of privacy*, adalah kejahatan yang menargetkan informasi pribadi dan rahasia milik seseorang. Tindakan ini biasanya diarahkan pada data pribadi

yang disimpan secara digital, seperti dalam formulir elektronik, dimana jika informasi tersebut jatuh ke tangan yang tidak berwenang yang dapat menyebabkan kerugian orang secara finansial maupun non-finansial. Contohnya termasuk nomor kartu kredit, nomor PIN ATM, atau informasi terkait cacat atau penyakit yang dirahasiakan (Pan Dhadha et al., 2022).

Setelah penjelasan beberapa macam bentuk *cybercrime*, *cyberstalking* dapat dikategorikan sebagai bentuk *cyber espionage*. Karena dalam praktiknya pelaku *cyberstalking* melakukan kejahatan menggunakan jaringan internet untuk memata-matai terhadap korban yang hendak dituju. Biasanya pelaku sangat memaksa dan menggunakan beberapa kalimat tidak pantas untuk dapat meneror korban, sehingga dalam hal ini membuat korban dalam posisi terancam dan ketakutan.

2. Penegakan Tindak Pidana *Cyberstalking* di Indonesia

Kejahatan terhadap privasi yang dilakukan di dunia maya ini disebut *cyberstalking*. "*cyberstalking*" adalah (Fadilah et al., 2021):

a. Tindakan mengancam, melecehkan, atau mengganggu seseorang;
b. Melalui internet, dengan maksud membuat korban takut akan tindakan ilegal atau luka. Namun seperti halnya dengan kejahatan-kejahatan komputer pada umumnya, maka definisi *cyberstalking* belum ada yang sudah diterima secara universal. Stalking sendiri memiliki arti "*harass somebody persistently: to harass somebody criminally by persistent, inappropriate, and unwanted attention, e.g. by constantly following, telephoning, e-mailing, or writing to him or her*."

Cyberstalking adalah tindakan menguntit dan memata-matai seseorang dengan menggunakan internet atau teknologi digital. Jenis penguntit ini sering dikenal juga sebagai pelecehan syber (*cyber harassement*). Individu yang melakukan tindakan ini disebut sebagai penguntit siber atau *cyberstalker*. Umumnya, perilaku *stalking* melibatkan gangguan (*harassement*) atau ancaman (*threats*) yang dilakukan berulang kali dan terus menerus terhadap korban.

Tindakan *cyberstalking* dapat berpotensi menjadi kejahatan yang serius jika tidak ditangani dengan tepat. Pelaku *cyberstalking* menggunakan berbagai strategi dan teknik untuk mengancam, mempermalukan, mengintimidasi dan mengontrol target mereka. Banyak dari para pelaku *cyberstalking* ini memiliki pemahaman yang baik tentang teknologi dan dapat memanfaatkan berbagai cara untuk menyiksa, melecehkan hingga mengancam korbannya. *Cyberstalking* dapat mengakibatkan berbagai dampak fisik dan emosional bagi korban secara online, dan sering kali korban mengalami marah, ketakutan, dan depresi yang berujung pada kematian. Pelaku *cyberstalking* melaksanakan aksinya melalui internet dengan mengumpulkan data pribadi korban dari jejaring sosial media termasuk nama, alamat, latar belakang keluarga, nomor telepon, informasi rutin harian, tanggal lahir dan lain-lain.

Sesudah mendapatkan informasi ini, pelaku kemudian mencoba untuk menghubungi korban dengan melakukan tindakan seperti melecehkan atau meninggalkan suatu pesan sebuah ancaman kepada korban melalui layanan internet. Dalam hal lain para pelaku dapat juga menyalahgunakan informasi atau data pribadi korban dengan mengunggah pada situs web yang berhubungan dengan seks atau layanan kencan yang berpura-pura menjadi korban (Anisah & Nurisman, 2022).

Ketika *cyberstalking* berubah menjadi *cyberbullying*, tindakan ini dapat melibatkan berbagai bentuk pelecehan, ancaman, spamming berlebihan, dan pelecehan dalam bentuk chat atau obrolan langsung. Tindakan ini juga bisa mencangkup penyebaran tuduhan palsu, pemantauan, ancaman, pencurian identitas, serta pengumpulan informasi untuk tujuan melecehkan. Jika diperhatikan *stalking* dan *cyberstalking* merupakan bentuk kejahatan yang serupa, perbedaanya terletak pada metode yang digunakan dalam beraksi.

Tindakan cyberstalking dapat menjadi sangat berbahaya dan menakutkan, terutama bagi-anak-anak dan remaja. Ini disebabkan oleh fakta bahwa identitas pribadi seorang sering kali tidak terlihat atau tersembunyi di internet, sehingga memberikan kesempatan bagi pelaku penguntitan (*stalker*) untuk bebas melancarkan aksinya. Banyak ditemukan kasus dimana seseorang yang baru dikenal melalui media sosial melakukan tindakan pelecehan terhadap korban yang baru saja mereka temui secara online. Di sebagian besar negara, undang-undang yang mengatur tentang penguntitan (*stalking*) biasanya mensyaratkan bahwa suatu tindakan baru dianggap sebagai kejahatan penguntitan apabila pelaku memberikan ancaman terhadap korban (Azhari, 2019; Zaki, 2022).

Hal ini tercermin dalam ketentuan yang diatur oleh UU ITE No. 19 Tahun 2016 perubahan UU ITE No 11 Tahun 2008. Dalam UU ITE tersebut, tindakan cyberstalking dapat dianggap sebagai perbuatan yang melanggar hukum. Ketentuan ini diatur dalam pasal 27 ayat (3), dan ayat (4) UU No. 19 Tahun 2016 tentang Informasi dan Transaksi Elektronik (UU ITE No.19, 2016):

Pasal 27 ayat (3) menyatakan bahwa: “Setiap Orang yang dengan sengaja dan tanpa hak menyebarkan, mentransmisikan atau membuat dapat diaksesnya Informasi Elektronik atau Dokumen Elektronik yang berisi penghinaan atau pencemaran nama baik”. Sementara itu, Pasal 27 ayat (4) menyebutkan: “Setiap Orang dengan sengaja dan tanpa hak menyebarkan, mentransmisikan atau membuat dapat diaksesnya Informasi Elektronik atau Dokumen Elektronik yang berisi muatan pemerasan atau pengancaman”. Kedua pasal ini menjadi dasar hukum untuk menindak tindakan cyberstalking yang melibatkan penghinaan, pencemaran nama baik, pemerasan, dan ancaman di ruang digital.

Sebagian besar UU diberbagai negara yang mengatur tentang *stalking* menetapkan bahwa suatu tindakan hanya dapat dikategorikan sebagai kejahatan stalking jika pelaku mengancam korban. Ketentuan ini juga tampaknya tercantum

dalam UU ITE. Namun, tindakan pelecehan atau *harassment* belum diatur dalam UU ITE tersebut, meskipun *cyberstalking* yang bersifat *harassment* dapat menjadi langkah awal menuju kejahatan lainnya, seperti penculikan anak di bawah umur oleh individu yang baru dikenal melalui platform seperti facebook atau instagram. Pelaku biasanya telah lama mengamati calon korbannya melalui media sosial. Oleh karena itu, sangat penting untuk memiliki regulasi yang lebih lengkap dan tegas mengenai tindak pidana *cyberstalking* ini.

Ketentuan mengenai tindakan *stalking* belum diatur secara spesifik dalam hukum positif di Indonesia, berbeda dengan Amerika Serikat, di mana beberapa negara bagian seperti Arkansas, Alaska, dan California, telah menglasifikasikan *stalking* sebagai tindak pidana sedangkan hukum pidana Indonesia tidak mengenali tindak pidana stalking dengan cara yang sama. Dengan demikian, berdasarkan asas legalitas pada ketentuan Pasal 1 KUHP bahwa suatu perbuatan tidak dapat dipidana, kecuali sudah ada peraturan perundang-undangan pidana yang telah mengaturnya.

Pelaku *cyberstalking* biasanya melakukan beberapa tindakan berikut ini:

a. Membuat akun sosial media palsu dengan identitas anonim atau nama samaran, yang sengaja digunakan untuk mengintai atau memantau orang lain secara diam-diam;
b. Mengirimkan pesan kepada korban, yang isinya dapat berupa ajakan untuk berinteraksi, permintaan bertemu, ungkapan perasaan, dan sebagainya;
c. Memantau secara intens segala informasi yang dibagikan oleh korban atau target di akun media sosial mereka, termasuk status, unggahan dan aktivitas lainnya;
d. Berulang kali membuat akun anonim baru jika akun sebelumnya diidentifikasi atau dicurigai melakukan aktivitas yang mengganggu seperti ketika korban melaporkan akun tersebut ke platform pengelola atau memblokir akun pelaku karena merasa tergangu;

Pelaku memiliki tujuan untuk memaksa korban agar mau berinteraksi dengannya, jika korban menolak, pelaku akan terus melancarkan tindakan yang bertujuan membuat korban merasa frustasi, terganggu atau marah atau setidaknya memberikan reaksi terhadap aksi tersebut (Kristiyadi, 2023; P.A.F. Lamintang, 2019).

Terjadinya kejahatan *stalker* ini dampak yang dirasakan membuat kondisi para korban kejiwaan mental sangat terganggu. Ada banyak hal mengapa para pelaku bisa melakukan kejahatan stalking dan *cyberstalking*. Motivasi pelaku antara lain berasal darirasa kesal, sakit hati, iri, atau keinginan untuk membalas dendam terhadap korban. Ada juga yang didorong oleh sifat dominan yang suka mengintimidasi orang lain. Namun, tidak sedikit pelaku yang melakukan aksi ini hanya untuk hiburan. Beberapa pelaku bahkan melakukannya tanpa niat jahat, meski tindakan pelecehan

atau penghinaan di dunia maya, baik disengaja maupun tidak, tetap dapat merugikan korban dan berdampak negatif pada kondisi psikologi. Sebagian besar target utama dari penguntit siber adalah perempuan dan anak-anak, yang secara emosional lebih rentan atau kurang stabil. Umumnya, korban *cyberstalking* adalah mereka yang masih baru di dunia maya dan tidak memiliki pengetahuan yang memadai tentang aturan keselamatan di internet. Jumlah korban sebenarnya sulit untuk diketahui dengan pasti karena kejahatn semacam ini seringkali tidak dilaporkan.

Cyberstalking yang merupakan bentuk terbaru dari kejahatan *stalking* di era digital kini telah muncul sebagai masalah serius dalam dunia teknologi informasi. Di Amerika Serikat, California menjadi negara bagian pertama yang mengesahkan hukum tentang stalking pada tahun 1990. Sebagai respon dari terjadinya pembunuhan terhadap aktris Rebecca Schaeffer oleh Roberr Bardo pada tahun 1989. Selanjutnya, New York mengundangkan Penal Code 240.25 pada tahun 1992 yang kemudian diperbaharui pada tahun 1994. Selain itu, negara bagian di Australia juga mengesahkan undang-undang mengenai stalking pada tahun 1998. *Cyberstalking* terus berkembang dan menjadi isu penting yang memerlukan perhatian lebih.

Dalam dunia teknologi informasi *cyberstalking* menjadi kejahatan baru dan merupakan masalah serius yang semakin berkembang. Pada tahun 1990 di Amerika Serikat, tepatnya di Negara bagian California, telah mempunyai aturan hukum tentang stalking. Aturan tersebut dibentuk dilatarbelakangi pasca kejadian pembunuhan terhadap aktris Rebecca Schaeffer oleh Rober Bardo pada tahun 1989. Kemudian di tahun 1992 New York mengundangkan Penal Code 240.25 yang kemudian diubah pada tahun 1994. Dan kemudian oleh beberapa negara seperti Australia juga membuat undang-undangan tentang stalking (Maharani et al., 2024).

Indonesia telah mengatur perihal stalking dalam UU ITE, namun cakupannya masih terbatas pada aspek ancaman yang ditimbulkan. Hukuman yang diterapkan di Indonesia untuk kejahatan siber yang serius tampaknya belum cukup memberikan efek jera bagi para pelaku. Indonesia dalam hal penegakan tindak pidana *cyberstalking* baru mengatur tentang stalking dalam UU ITE, Adapun Pasal 335 KUHP jo. Putusan MK No. 1/PUU-XI/2023 mengenai perbuatan tidak menyenangkan yang berbunyi sebagai berikut:

a. Diancam dengan hukuman penjara maksimal satu tahun atau denda paling banyak sebesar empat ribu lima ratus rupiah:
    1) Setiap orang yang secara melawan hukum memaksa orang lain untuk melakukan, tidak melakukan atau membiarkan sesuatu tindakan, dengan menggunakan kekerasan, baik terhadap dirinya sendiri maupun orang lain.
    2) Setiap orang yang memaksa orang lain untuk melakukan, tidak melakukan atau membiarkan sesuatu tindakan dengan menggunakan ancaman pencemaran nama baik atau pencemaran tertulis.

b. Dalam kasus sebagaimana diatur dalam point kedua, penuntutan hanya dapat dilakukan berdasarkan pengaduan dari pihak yang dirugikan.

Berdasarkan ketentuan Pasal 448 UU 1/2023 berbunyi:

a. Dijatuhkan hukuman penjara paling lama 1 tahun atau pidana denda maksimal kategori II, yakni sebesar Rp10 juta bagi setiap orang yang:
   1) secara melawan hukum memaksa orang lain untuk melakukan, tidak melakukan, atau membiarkan sesuatu melalui kekerasan atau ancaman kekerasan, baik terhadap orang tersebut maupun orang lain; atau
   2) memaksa orang lain untuk melakukan, tidak melakukan, atau membiarkan sesuatu dengan ancaman pencemaran atau pencemaran tertulis.
b. Tindak pidana yang diatur dalam ayat (1) huruf b hanya dapat dituntut atas berdasarkan laporan dari korban kejahatan.

Namun, pasal ini hanya mencangkup aspek pengancaman saja, karena *stalking* itu sendiri melibatkan tindakan berulang yang berlangsung secara bertahap dan dapat menyebabkan tekanan secara psikologi pada korban. Selain itu, pasal tersebut tidak mencangkup unsur harassment atau ganguan, suatu tindakan baru dapat dijatuhi tindak pidana, jika memenuhi unsur-unsur tindak pidana (delik) namun tidak semua tindak pidana dapat dijatuhi pidana jika perbuatan tersebut tercantum dalam rumusan delik. Dalam konteks ini, tindakan tersebut harus memenuhi dua syarat, yaitu harus bersifat melawan hukum dan bersifat tercela. Kedua syarat ini dianggap sebagai syarat umum untuk menjadikan suatu tindakan dapat dipidana (Makarim, 2004; Saputra, 2023).

Seseorang dapat dipidana apabila terlebih dahulu terdapat sayarat yang menentukan. Terdapat dua syarat yang membentuk satu kondisi, yaitu tindakan yang bersifat melawan hukum yang menjadi dasar bagi perbuatan pidana, dan tindakan tersebut harus dapat dipertangungjawabkan yang menjadi dasar sebagai kesalahan (Hafizah et al., 2022).

Tindakan *cyberstalking* yang tidak melibatkan unsur pelanggaran kesusilaan, perjudian, penghinaan atau pencemaran nama baik, pemerasan dan/atau pengancaman, dan ancaman kekerasan atau menakut-nakuti, belum bisa dikenakan hukuman. Unsur "mengganggu" saja belum cukup sebagai dasar untuk memberikan sanksi pidana pada pelaku (Putra et al., 2023). Tindakan *stalking* pada masa yang modern saat ini, pelaku tidak perlu lagi mengikuti korban secara langsung, cukup mengumpulkan informasi dari dunia maya seperti di media sosial, data tentang korban dapat dengan mudah dikumpulkan. Dengan cara ini, pelaku bisa melakukan teror kepada korban melalui internet tanpa harus secara langsung memantau mereka (*stalking*) atau bahkan menggunakan informasi tersebut untuk merencanakan tindakan kriminal didunia nyata.

D. SIMPULAN

Cyberstalking adalah kejahatan siber yang melibatkan penggunaan internet untuk melecehkan atau mengintai korban, yang sering memicu tindak pidana lain seperti *cyberbullying*, *hacking*, dan bahkan kejahatan konvensional seperti penculikan. Regulasi terkait *cyberstalking* di Indonesia masih belum jelas, sehingga diperlukan pengembangan hukum yang lebih kuat dalam UU ITE untuk menindak pelaku dan melindungi korban. Langkah preventif seperti meningkatkan kesadaran individu tentang keamanan digital dan kolaborasi antara pihak terkait sangat penting. Selain itu, diperlukan regulasi khusus mengenai perlindungan data pribadi serta pengaturan pidana yang jelas untuk menangani kasus *cyberstalking* secara efektif.

E. DAFTAR RUJUKAN

Albar, M. H. Y., T, W., & Novianto. (2022). Prospect of Cyberstalking Regulation in the Future in Indonesia. *International Journal of Multicultural and Multireligious Understanding*, *9*(1), 423–428. http://dx.doi.org/10.18415/ijmmu.v9i1.3331

Andespitrikasih, L., Waluyo, B., & Harefa, B. (2024). Legal Protection for Victims of Cyberstalking According to Indonesia's Law. *International Journal of Social Science and Human Research*, *7*(6). https://doi.org/10.47191/ijsshr/v7-i06-23

Anisah, A., & 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), 150–163. http://dx.doi.org/10.32801/damai.v4i1.9234

Božić, D., & Мичић, C. (2024). Interpretation Of Cyberstalking In The Austrian Criminal Code. *Evropsko Zakonodavstvo*, *23*(86), 34–46. https://doi.org/10.18485/iipe_ez.2024.23.86.3

Fadilah, A., Dan, R. A., & Putri, S. R. (2021). Eksistensi Keamanan Siber Terhadap Tindakan Cyberstalking Dalam Sistem Pertanggungjawaban Pidana Cybercrime. *Syntax Literate: Jurnal Ilmiah Indonesia*, *6*(4), 1555. https://doi.org/10.36418/syntax-literate.v6i4.2524

Hafizah, A., Ablisar, M., & Lubis, R. (2022). Asas Legalitas dalam Hukum Pidana Indonesia dan Hukum Pidana Islam. *Mahadi: Indonesia Journal of Law*, *1*(1), 1–10. https://doi.org/10.32734/mah.v1i1.8311

Kristiyadi. (2023). Pergeseran Asas Legalitas Dalam Pembaruan Hukum Pidana Indonesia. *Jurnal Dunia Ilmu Hukum (JURDIKUM)*, *1*(1), 25–27. https://doi.org/10.59435/jurdikum.v1i1.100

Maharani, P., Hafrida, H., & Rapik, M. (2024). Pertanggungjawaban Pidana Hacktivist dalam Perspektif Hukum Pidana di Indonesia. *PAMPAS: Journal of Criminal Law*, *5*(2), 242–252. https://doi.org/10.22437/pampas.v5i2.33291

Makarim, E. (2004). *Kompilasi Hukum Telematika*. Jakarta: Raja Grafindo Persada.

Marzuki, P. M. (2016). *Penelitian Hukum*. Jakarta: Prenada Media.

Maskun. (2014). *Kejahatan Siber (Cyber Crime)*. Jakarta: Kencana Prenadamedia Group.

Natalia, S. W., & Atmadja, I. D. G. (2013). Pengaturan Tindak Pidana Cyberstalking dalam UU No. 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik (UU ITE). *Kertha Semaya: Journal Ilmu Hukum*, *1*(2), 1–5. http://ojs.unud.ac.id/index.php/kerthasemaya/article/view/4687

P.A.F. Lamintang. (2019). *Dasar-Dasar Hukum Pidana di Indonesia*. Jakarta: Sinar Grafika.

Pan Dhadha, T., Rahayu, L. A., Resmi, D. S., & Kusumastuti, D. (2022). Efektivitas Peran UU ITE Dalam Rangka Melindungi Serta Menjaga Seluruh Aktivitas Siber Yang Ada Di Indonesia. *Legal Standing : Jurnal Ilmu Hukum*, *6*(1), 40. https://doi.org/10.24269/ls.v6i1.3541

Putra, C., Sugiartha, I., & Widyantara, I. (2023). Analisis Yuridis atas Keabsahan Pertanggungjawaban Pidana terhadap Pelaku Tindak Pidana Pembobolan Sistem Data Keamanan Komputer (Cracking). *Jurnal Preferensi Hukum*, *5*(1), 1–7. https://doi.org/10.22225/jph.5.1.8636.1-7

Royani, A. (2016). Tinjauan Yuridis Terhadap Tindak Pidana Pencemaran Nama Baik Dalam Kitab Undang-Undang Hukum Pidana Dan Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik. *Jurnal Independent*, *4*(1), 11. https://doi.org/10.30736/ji.v4i1.43

Saputra, C. D. (2023). Aspek Hukum Telematika dalam Perlindungan Data Pribadi. *Jurnal Kepastian Hukum Dan Keadilan*, *5*(1), 54–74. https://doi.org/10.32502/khk.v5i1.7968

Sugiarto, E., Oscar, V., & Simanungkalit, D. S. (2024). Analisa Cybercrime Pencurian Data Pribadi Modus Aplikasi Pinjaman Online dan Digital Banking. *Legal Standing: Jurnal Ilmu Hukum*, *8*(1), 173–183. https://doi.org/10.24269/ls.v8i1.8545

UU ITE No.19. (2016). *UU ITE No.19 Tahun 2016 Tentang Informasi dan Transaksi Elektronik perubahan UU ITE No.11 Tahun 2008*.

Winarni, R. R. (2016). Efektivitas Penerapan Undang-Undang ITE dalam Tindak Pidana Cyber Crime. *Jurnal Ilmiah Hukum Dan Dinamika Masyarakat*, *14*(1), 16–27. http://dx.doi.org/10.56444/hdm.v14i1.440

Zaki, M. (2022). Aspek Pidana Cyberstalking Sebagai Salah Satu Bentuk Cybercrime. *Jurist-Diction*, *5*(3), 973–988. https://doi.org/10.20473/jd.v5i3.35790