Jurist-Diction
Volume 5 No. 3, Mei 2022

Aspek Pidana *Cyberstalking* Sebagai Salah Satu Bentuk *Cybercrime*

Muhammad Maulana Zaki
Muhammad.maulana.zaki-2017@fh.unair.ac.id
Universitas Airlangga

How to cite:
Muhammad Maulana Zaki, 'Aspek Pidana *Cyberstalking* Sebagai Salah Satu Bentuk *Cybercrime*' (2022) Vol. 5 No. 3 Jurist-Diction.

Histori artikel:
Submit 26 April 2022;
Diterima 23 Mei 2022;
Diterbitkan 27 Mei 2022.

DOI:
10.20473/jd.v5i3.35790

p-ISSN: 2721-8392
e-ISSN: 2655-8297

Abstract
Technology is developing, the pattern of interaction between humans is also changing. Internet is a new world where humans interact, without the limitations of distance and time. but the internet cannot be separated from dangerous actions, one of which is Cyberstalking. An act of cybercrime that is usually not considered dangerous but if it harms the victim it can potentially become a criminal act and the absence of rule causing the legality problem Based on this background, the purpose of this study is emphasizing criminal aspect by qualifying cyberstalking as maliciuos act. Continued by analyzing the criminal responsibilty of the perpetrators and the legal evidence of Cyberstalking. The research method used is a legal doctrinal method with a statutory approach, conceptual approach and comparative approach.
Keywords: *Cyberstalking; Criminal Aspect; Cybercrime.*

Abstrak
Teknologi berkembang, pola interaksi antar manusia juga berubah. Internet adalah hal baru dunia tempat manusia berinteraksi, tanpa batasan jarak dan waktu. namun internet tidak lepas dari tindakan-tindakan yang berbahaya, salah satunya adalah *Cyberstalking* yangsebuah tindakan *cybercrime* yang biasanya tidak dianggap berbahaya namun jika merugikan korban maka dapat berpotensi menjadi tindakan kriminal dan kekosongan aturannya menimbulkan problematika dalam legalitasnya Berdasarkan dari latar belakang tersebut tujuan penelitian ini adalah menitik beratkan aspek pidana nya yakni dengan menganalisis kualifikasi *cyberstalking* sebagai tindakan yang dicela. Dilanjutkan pertanggungjawaban dan pembuktian dari pelaku kejahatan *Cyberstalking*. Metode penilitian yang digunakan adalah hukum normatif dengan pendekatan perundang-undangan, pendekatan konseptual, dan pendekatan perbandingan.
Kata Kunci: *Cyberstalking*; Aspek Pidana; *Cybercrime*.

Pendahuluan

Media sosial memungkinkan pemakai berperan sebagai produsen dan konsumen pesan yang didistribusikan secara menyeluruh kepada pemakai. Beragam aplikasi media sosial seperti *Facebook, Twitter, dan Instagram* digunakan secara

luas, dengan berbagai motif mulai dari motif pertemanan, motif hiburan, motif mencari informasi dan bahkan juga motif ekonomi. Tiga media sosial ini menjadi aplikasi media sosial yang paling popular di Indonesia.[1]

Saat kita menjadi pengguna media sosial, Langkah pertama yang dilakukan adalah mengisi data yang menjadi yang menjadi proses pengaktifan akun media sosial. Sebagai pengguna, kita selama ini mungkin merasa bahwa apa yang kita isi dalam formular data berada dalam posisi yang aman. Aman di sini berarti bahwa data yang kita isi tidak digunakan oleh perusahaan secara ilegal dan aman dari peretasan pihak lain. Kasus peretasan akun media sosial yang dilakukan oleh orang yang tidak bertanggung jawab bisa terjadi kapan pun dan kepada siapa pun yang berujung sebuah tindakan perundungan.

Perundungan siber *(cyberbullying*) adalah perundungan yang dilakukan oleh individu atau sekelompok individu kepada individual atau kelompok individu lain dengan memanfaatkan media internet untuk melakukan perundungan. Hal ini berarti bahwa perundungan terjadi di internet, meskipun demikian perundungan siber bisa jadi tidak berhenti di internet, namun bisa berpindah ke dunia nyata.

Ada beberapa bentuk dari perundungan siber yaitu antara lain:[2]

1. Pengucilan (*exclusion*);
2. Pelecehan (*harassement*);
3. *Outing;*
4. Penguntitan siber (*Cyberstalking*);
5. *Fraping;*
6. *Dissing;*
7. *Trickery;*
8. *Trolling;*
9. *Catfishing.*

Tindakan-tindakan di atas tentu sangat tidak dibenarkan secara etis. Tindakan tersebut secara tujuan maupun proses, melukai orang lain sehingga bisa disebut tindakan yang tidak bermoral.[3] Bila diperhatikan penguntitan siber (*Cyberstalking*) adalah sebuah tindakan yang amat berbahaya karena sebagian besar tindakan

[1] Fajar Junaedi, *Etika Komunikasi di Era Siber* (Raja Grafindo Persada 2020).[153].
[2] *ibid*.[173-175].
[3] *ibid*.[176].

perundungan siber berawal dari penguntitan. Penguntit dalam perundungan siber perlu diwaspadai, karena mereka mengintip dan mengikuti seluruh aktivitas dari korbannya, di surat elektronik maupun media sosial.[4]

Indonesia telah memiliki Undang-undang Nomor 11 tahun 2008 tentang Informasi dan Transaksi Elektronik, sebagaimana telah diubah dengan Undang-undang Nomor 19 tahun 2016 tentang Perubahan atas Undang-undang Nomor 11 tahun 2008 tentang Informasi dan Transaksi Elektronik (selanjutnya dalam tulisan ini, disingkat penyebutannya dengan UU ITE). Di dalam pasal 27 ayat (1) sampai (4) UU ITE dinyatakan bahwa tindakan yang dilarang adalah tindakan dengan sengaja dan tanpa hak mendistribusikan dan/atau mentransmisikan dan/atau membuat dapat diaksesnya Informasi Elektronik dan/atau Dokumen Elektronik yang memiliki muatan yang melanggar kesusilaan, perjudian, penghinaan dan/atau pencemaran nama baik, pemerasan dan/atau pengancaman. Namun seperti yang dijelaskan bahwa *Cyberstalking* adalah suatu tindakan membuntuti sedangkan UU ITE masih tidak mengenal konsep membuntuti dalam pasal-pasalnya. Di California, yang merupakan bagian Amerika terdapat regulasi yang mengatur perihal *stalking* sebagai tindakan membuntuti seseorang dengan niat untuk melecehkan dan membuat ketakutan korbannya.[5]

Pengaturan mengenai *stalking* oleh pembentuk undang-undang di AS menunjukkan bahwa perbuatan *stalking* adalah masalah serius karena menyangkut masalah pelecehan sedangkan UU ITE masih belum memiliki aturan yang jelas mengenai penguntitan yang berujung pelecehan terutama di dunia siber. Hal ini menunjukkan bahwa UU ITE memerlukan pengaturan *Cyberstalking* yang tegas dan lengkap,Karena penting bagi masyarakat memahami batasan-batasan sebelum menyatakan *Cyberstalking* sebagai tindak pidana.

Definisi *Cyberstalking*

Pengertian *Cyberstalking*, terdapat definisi dari Bojic dan McFarlane sebagai berikut:"*We define Cyberstalking as the use of information and communications*

[4] *ibid*.[174].
[5] California Penal Code (CPC) Section 646.9

technology (in particular the Internet) in order to harass individuals. Such harassment may include actions such as the transmission of offensive e-mail messages, identity theft and damage to data or equipment . Whilst a more comprehensive definition has been presented elsewhere, it is hoped that the definition here is sufficient for those unfamiliar with this field. The stereotypical stalkerrepeatedly following or tailing the object of their affection. However, not all stalking incidents are motivated by unrequited love. Stalking can also be motivated by hate, a need for revenge, a need for power and/or racism. Similarly, Cyberstalking can involve acts that begin with the issuing of threats and end in physical assault. We also make distinctions between conventional stalking and Cyberstalking. Whilst some may view Cyberstalking as an extension of conventional stalking, we believe Cyberstalking should be regarded as an entirely new form of deviant behaviour.[6]

Melihat definisi *Cyberstalking* diatas, maka dapat dikatakan bahwa *Cyberstalking* merupakan bentuk yang sama dari *stalking* biasa. Yang membedakan hanyalah sarana yang digunakan pada pelaksanaan dimana *cyberstalking* menggunakan media elektronik atau sosial media sebagai sarananya. Namun seperti yang dijelaskan oleh Bojic dan McFarlane, *Cyberstalking* harus dibedakan dengan *stalking* biasa sebab perkembangan teknologi sangat mempengaruhi perilaku dan akibat yang ditimbulkan masyarakat.

Karateristik dan Dampak *Cyberstalking*

Untuk memahami karateristik, maka penting untuk mengetahui modus operandinya. Modus operandi adalah cara operasi orang perorang atau kelompok penjahat dalam menjalankan rencana kejahatannya.[7] Istilah ini sering digunakan dalam pekerjaan polisi ketika membahas kejahatan dan menangani metode yang digunakan oleh penjahat. Ini juga digunakan dalam pembuatan profil kriminal,[8]

[6] Paul Bocij, Leroy Mcfarlane, *Cyberstalking: A New Challenge for Criminal Law* (Lecture at Criminal law Nottingham Trent University2002).[3].

[7] John E. Douglas, Robert Ressler, Ann Burgess, Allen G. Burgess, *Crime Classification Manual* (Wiley2013).[19].

[8] Peter Vronsky, *Serial Killers* (Berkley Books 2004).[412].

Di mana ia dapat membantu menemukan petunjuk tentang psikologi pelaku.[9]Ini sebagian besar terdiri dari memeriksa tindakan yang digunakan oleh individu untuk melakukan kejahatan, mencegah deteksi dan memfasilitasi pelarian.[10]Modus operandi tersangka dapat membantu dalam identifikasi, penangkapan, atau represi mereka, dan juga dapat digunakan untuk menentukan hubungan antara kejahatan.[11]Jika diteliti lebih lanjut, pelaku *Cyberstalking* biasanya melakukan tindakan seperti berikut:[12]

a. Mengirimkan pesan kepada korban, di mana isi pesan berupa ajakan untuk berinteraksi atau bahkan bertemu, pernyataan perasaan, dan sebagainya.
b. Pelaku mengikuti semua informasi yang ditulis oleh korban / sasarannya, melalui akun sosial media milik korban.
c. Pelaku secara berulang-ulang membuat akun anonim yang baru jika akun sebelumnya terdeteksi / dicurigai melakukan perbuatan yang mengganggu (misalnya: korban mengirimkan *report* / pengaduan kepada pengelola *platform*, korban melakukan *block* akun pelaku karena merasa terganggu).
d. Pelaku bertujuan membuat korban mau berinteraksi dengannya, atau apabila korban menolak, pelaku kemudian melanjutkan tindakan untuk membuat korban merasa kesal, terganggu atau marah atau bereaksi.

Berdasarkan poin-poin diatas maka perbuatan *Cyberstalking* melingkupi hal-hal seperti pembuatan identitas palsu, ajakan untuk bertemu hingga keinginan untuk menciptakan lingkungan yang mengintimidasi. Dengan timbulnya perbuatan-perbuatan demikian, maka dampak yang ditimbulkan dapat mengarah pada unsur-unsur *cybercrime* seperti konten ilegal, *exortion* (pemerasan), dan pencurian data.

---

[9] Robert hazelwood, *Practical Aspects of Rape Investigation A Multidisciplinary Approach* (CRC press2008).[517].

[10] John E. Douglas, Robert Ressler, Ann Burgess, Allen G. Burgess.*Op.Cit*.[20].

[11] *ibid*.[21].

[12] *Rahel Octora. 'Problematika Pengaturan Cyberstalking (Penguntitan di Dunia Maya) Dengan Menggunakan Anonymous Account Pada Sosial Media*' (2019) 11Dialogia Iuridica.[87].

Kriminalisasi terhadap perbuatan Cyberstalking

Menguntit atau *stalking* adalah perbuatan yang pada dasarnya bersifat netral, artinya *stalking* dapat dikriminalisasi apabila telah masuk ke ranah kriminal.[13] Definisi menguntit secara umum adalah mengikuti, membuntuti secara berulang-ulang namun apabila tidak menyentuh lingkup *cybercrime* maka tidak akan bisa dimasukkan sebagai tindak pidana. Oleh karena itu penting untuk membedakan *stalking* jenis apa yang dapat dipidana dan yang tidak. Pelaku *Cyberstalking* dapat diklasifikasikan menjadi beberapa tipe sebagai berikut:[14]

a. *Predatory stalker*, dimotivasi oleh gagasan kesenangan dan kendali atas korban dan keinginan untuk menyerang target, seringkali secara seksual.
b. *Intimacy Seeker*, mencoba untuk menciptakan hubungan romantis dengan target, mengidamkan target, percaya bahwa tidak seorang pun kecuali target mampu memenuhi kebutuhan mereka dan berpotensi tertipu dengan berpikir bahwa target memiliki kasih sayang untuk mereka.
c. *Incompetent Stalker*, dipaksa untuk memulai percintaan dan dilarang melakukannya karena perilaku sosial yang buruk.
d. *Rejected stalker*, umumnya sebagai akibat dari putusnya hubungan dekat. motivasi awal penguntit yang ditolak adalah mencoba untuk mendamaikan hubungan, atau untuk membalas dendam atas penolakan yang dirasakan.
e. *Resentful Stalker*, penguntit yang marah ingin menimbulkan ketakutan dan kesusahan pada korban mereka dan sering menguntit untuk membalas dendam seseorang yang telah membuat mereka marah.

Melihat dari tipe-tipe *cyberstalker* diatas, maka perlu dipahami bahwa masing- masing dari mereka memiliki niat dan tujuan yang berbeda. Contohnya *incompetent stalker* yang dimana mereka tidak tahu cara bersosialisasi sehingga melakukan *stalking* demi bisa berinteraksi dengan targetnya. Dari definisi tersebut, mereka adalah *stalker* yang tidak masuk ranah pidana. Namun berbeda dengan *Predatory Stalker* dan *Resentful Stalker*yang dari definisinya sudah mengindikasikan akan menyerang target secara seksual atau membalas dendam dengan cara menimbulkan ketakutan pada target. Hal ini telah sesuai dengan unsur-

[13] Brenda Charlotte, *Cyberstalking Sebagai Perbuatan Melawan Hukum Dan Pengaturannya Dalam Hukum Pidana Indonesia*, Skripsi (Program sarjana Universitas Katolik Parahyangan Bandung 2014).[66].

[14] National Centre for *Cyberstalking* Research, *A Practical Guide to Coping with Cyberstalking* (Andrews UK Limited 2015).[6-9].

unsur perbuatan *Cyberstalking* antara lain:

1. *Threat* (mengancam)

   Dalam sistem hukum di Indonesia, istilah pengancaman dapat ditemukan di kitab undang-undang hukum pidana (KUHP). Dalam pasal 368 ayat (1) terdapat istilah ancaman kekerasan dan dalam pasal 369 ayat 1 terdapat istilah ancaman pencemaran. Pasal 368 ayat 1 menyatakan :"*Barang siapa dengan maksud untuk menguntungkan diri sendiri atau orang lain secara melawan hukum, memaksa seorang dengan kekerasan atau ancaman kekerasan untuk memberikan barang sesuatu, yang seluruhnya atau sebagian adalah kepunyaan orang itu atau orang lain, atau supaya membuat hutang maupun menghapuskan piutang, diancam karena pemerasan, dengan pidana penjara paling lama sembilan tahun.*". Pasal 369 ayat 1 menyatakan: "*Barang siapa dengan maksud untuk menguntungkan diri sendiri atau orang lain secara melawan hukum, dengan ancaman pencemaran baik lisan maupun tulisan atau dengan ancaman akan membuka rahasia, memaksa seseorang supaya memberikan sesuatu barang yang seluruhnya atau sebagian milik orang lain, atau supaya memberikan hutang atau menghapus piutang, diancam dengan pidana penjara paling lama empat tahun*.".

   Dua pasal diatas mengandng unsur objektif adalah berupa memaksa dengan kekerasan, mengancam akan melakukan kekerasan. Adapun unsur subyektif berupa maksud seseorang untuk menguntungkan diri sendiri atau orang lain secara melawan hukum. Pada intinya, mengancam adalah unsur dimana menyatakan maksud (niat, rencana) untuk melakukan sesuatu yang merugikan, menyulitkan, menyusahkan, atau mencelakakan pihak lain dengan memberi tekanan agar korban mengikuti kemauan si pelaku. Ancaman akan memberi dampak secara fisik maupun psikis pada korbannya.

   Di dalam UU ITE istilah mengancam dapat ditemukan di pasal 45B yang menyatakan: "Setiap Orang yang dengan sengaja dan tanpa hak mengirimkan Informasi Elektronik dan/atau Dokumen Elektronik yang berisi ancaman kekerasan atau menakut-nakuti yang ditujukan secara pribadi sebagaimana

dimaksud dalam Pasal 29: dipidana dengan pidana penjara paling lama 4 (empat) tahun. Pasal 45B UU 19/2016, dijelaskan bahwa Ketentuan dalam Pasal ini termasuk juga di dalamnya perundungan di dunia siber (*cyberbullying*) yang mengandung unsur ancaman kekerasan atau menakut-nakuti dan mengakibatkan kekerasan fisik, psikis, dan/atau kerugian materiil.

Terkait ancaman dimana ancaman tersebut bersifat subjektif dirasakan oleh korban dan korban dirasa perlu untuk akan memutuskan apakah dirinya merasa perlu untuk melanjutkan kasus ini melalui jalur hukum pidana, maka perlu dibedakan adanya klasifikasi delik yaitu delik biasa dan delik aduan. Delik aduan adalah delik yang penuntutannya hanya dilakukan apabila ada pengaduan dari pihak yang terkena (*gelaederde partij*) misal penghinaan (Pasal 310 dst. Jo. Pasal 319 KUHP), penghinaan (pasal 284 KUHP),*chantange* (Pasal 335ayat (1) sub 2 jo. Ayat (2) KUHP delik aduan dibedakan menurut sifatnya sebagai:[15]

1. Delik aduan yang absolut misalnya pasal 284, 310, 332, 339 KUHP. Delik-delik ini menurut sifatnya hanya dituntut berdasarkan pengaduan.
2. Delik aduan yang relatif misalnya Pasal 367 KUHP, disebut relatif karena dalam delik-delik ini ada hubungan istimewa antara si pembuat dan orang yang terkena.

2 . *Harrasement* (Melecehkan)

Menurut Kamus Besar Bahasa Indonesia, melecehkan berarti: memandang rendah (tidak berharga); menghinakan; mengabaikan. Pelecehan dapat dilakukan secara verbal maupun melalui tindakan fisik. Dalam konteks interaksi secara online, pelecehan dapat terjadi melalui kalimat-kalimat yang tidak pantas, yang dikirimkan melalui pesan digital. Mengirimkan pesan digital dengan muatan konten-konten asusila juga dapat dikategorikan sebagai tindakan pelecehan.

Berdasarkan *handbook research on cyberbullying and online harassment*

[15] Junaedi Effendi, *Cepat dan Mudah Memahami Hukum Pidana* (Prenada Media 2016).[60-61].

in the workplace tahun 2020 ditemukan pengertian sebagai berikut: "*online harrasement is defined as the offensive behaviours conducted through electronic mediums to intentionally harm and embarrass another person. Online behaviour is seen as a form of verbal or sexual aggression. In addition, victims also experience Cyberstalking, receiving inappropriate and/or pornographic messages as well as threatening ones. Online harassment differs from cyberbullying in that most of the harassment incidents are not repetitive, they only happen once. Even though terms are used interchangeably, statistic showed that the number of people suffering from cyberbullying and/or online harassment increases every day.*[16]

Berdasarkan uraian diatas, penulis menekakan unsur- unsur yang terdapat pada pelecehan secara *online* antara lain:

a. Kontak yang tidak diinginkan;
b. Tujuan dari kontak tersebut adalah menciptakan lingkungan yang mengintimidasi serta menakuti korban;
c. Dalam konteks *Cyberstalking*, si *stalker* dapat memantau bahkan menghubungi korban menggunakan saluran digital;
d. Pelecehan terjadi secara *online*.

3. *Assault* (Kekerasan)

Dalam konteks *Cyberstalking*, biasanya korban tidak mengalami kekerasan secara fisik namun dapat menimbulkan secara psikis. KUHP hanya mengenal penganiayaan secara fisik, yaitu rasa sakit yang ditimbulkan akibat perbuatan-perbuatan berupa kekerasan fisik seperti antara lain: menendang, memukul, , menikam dengan pisau, dan lain-lain. Dengan kata lain, penganiayaan secara psikis tidak dikenal dalam KUHP.

Namun, atas perbuatan menyakiti orang secara psikis ini dalam praktiknya dapat dilakukan upaya hukum berupa gugatan secara perdata atas dasar Perbuatan Melawan Hukum (PMH) dan dapat menuntut ganti rugi immateriil. Dalam praktiknya, jika seseorang melakukan kekerasan psikis terhadap orang

[16] Leslie Ramos Salazar, *Handbook of Research on Cyberbullying and Online Harrasment in the Workplace* (Business Science Reference2020).[181].

lain, maka upaya hukum yang dapat dilakukan oleh korban adalah melakukan gugatan PMH sebagaimana diatur dalam Pasal 1365 *Burgerlijk Wetboek* (BW) menyatakan:"*Tiap perbuatan yang melanggar hukum dan membawa kerugian kepada orang lain, mewajibkan orang yang menimbulkan kerugian itu karena kesalahannya untuk menggantikan kerugian tersebut*.". Perbuatan melawan hukum memiliki unsur-unsur yang perlu diperhatikan antara lain:[17]

a. Bertentangan dengan kewajiban hukum si pelaku;
b. Bertentangan dengan hak subjektif orang lain;
c. Bertentangan dengan kesusilaan;
d. Bertentangan dengan kepatutan, ketelitian dan kehati-hatian.

Dari definisi yang diuraikan, *Cyberstalking* adalah sebuah tindakan yang patut untuk diwaspadai karena dapat berakhir pada kekerasan psikis yang dapat berujung pada masalah kesusilaan dan martabat seseroang. Setiap pengguna internet adalah bagian dari anggota masyarakat yang patut mendapatkan jaminan keselamatan dan kenyamanan untuk melaksanakan aktifitas nya di dunia maya.

Pertanggungjawaban pidana *Cybertsalking*

Untuk dapat mengenakan pidana pada pelaku karena melakukan tindak pidana, aturan hukum mengenai pertanggungjawaban pidana berfungsi sebagai penentu syarat-syarat yang harus ada pada diri seseorang sehingga sah jika dijatuhi hukuman. Pertanggungjawaban pidana yang menyangkut masalah pembuat dari tindak pidana, aturan mengenai pertanggungjawaban pidana merupakan regulasi mengenai bagaimana memperlakukan mereka yang melanggar kewajiban. Jadi perbuatan yang dilarang oleh masyarakat itu dipertanggungjawabkan pada si pembuatnya, artinya hukuman yang objektif terhadap hukuman itu kemudian diteruskan kepada si terdakwa. Pertanggungjwaban pidana tanpa adanya kesalahan dari pihak yang melanggar tidak dapat dipertanggungjawabkan. Jadi seseorang tidak mungkin dipertanggungjawabkan dan dijatuhi pidananya kalau tidak melakukan

[17] Rosa Agustina, *Perbuatan Melawan Hukum* (Penerbit Pasca Sarjana FH Universitas Indonesia2003).[117].

perbuatan pidana. Tetapi meskipun dia melakukan perbuatan pidana, tidak selalu dia dapat dipidana.[18] Dalam penuntutan sebuah delik, harus dibuktikan semua elemen delik yang dituduhkan kepada pembuat delik. Oleh karena itu jika salah satu unsur atau elemen delik tidak terpenuhi, maka pembuat delik tersebut tidak dapat dipersalahkan melakukan delik yang dituduhkan, sehingga pembuat delik harus dilepaskan dari segala tuntutan hukum (*onslaag van rechts alle vervologing*). Elemen delik umumnya terbagi dalam 2 (dua) bagian, yaitu: (1) unsur obyektif, atau yang biasa disebut *actus reus*, dan (2) unsur subyektif, atau yang biasa disebut *mens rea*.[19]

Sanksi Pelaku *Cyberstalking*

Sistem hukum di Indonesia belum memiliki aturan secara langsung dalam perihal mengenai *Cyberstalking*. Jika melihat Undang- Undang yang ada, terdapat peraturan yang mendekati ruang lingkup *Cyberstalking* yang dapat dikategorikan sebagai perbuatan yang dilarang dalam Pasal 29 Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE): "*Setiap Orang dengan sengaja dan tanpa hak mengirimkan Informasi Elektronik dan/atau Dokumen Elektronik yang berisi ancaman kekerasan atau menakut nakuti yang ditujukan secara pribadi.*"

Ancaman sanksi bagi pelaku yang melakukan perbuatan tersebut yaitu dijerat pidana penjara paling lama 12 tahun dan/atau denda paling banyak Rp. 2 (dua) miliar.[20]Dikarenkan hanya pemilik atau yang memiliki hak dapat mengakses suatu sistem elektronik. Tidak hanya itu didalam satu sistem elektronik memiliki nilai, baik nilai yang bersifat pribadi maupun nilai ekonomis, sehingga privasi dan kepentingan pemilik atau pihak yang berhak tersebut dilindungi oleh ketentuan pasal ini.[21]

---

[18] Admaja Priyatno, *Kebijakan Legislasi Tentang Sistem Pertanggungjawaban Pidana Koorporasi Di Indonesia* (Utomo 2004).[15].

[19] *ibid*.

[20] Lihat Pasal 45 ayat (3) Undang-Undang Nomor 11 tahun 2008 tentang Informasi dan Transaksi Elektronik.

[21] Teguh Arifiyandi, Joshua Sitompul, *Gadgetmu, Harimaumu (Tips Melek Hukum di Medsos)* (Literati2015).[92].

Berdasarkan penjelasan di atas, maka untuk dapat dijerat dengan Pasal 29 UU ITE, pelaku *Cyberstalking* harus mempunyai motif keuntungan ekonomis. Keuntungan ekonomis berarti segala sesuatu yang menguntungkan si pelaku atas hasil yang diperoleh dalam melakukan tindakannya. Dalam konteks *cyberstalking*, keuntungan ekonomis tidak hanya terbatas pada uang dan materi karena berdasarkan penjelasan sebelumnya bahwa motif dari *cyberstalking* bisa masuk ke lingkup seksual.

Pembuktian *Cyberstalking*

Pembuktian adalah perbuatan membuktikan. Membuktikan sesuatu berarti memberi atau memperlihatkan bukti, melakukan sesuatu sebagai kebenaran, melaksanakan, menandakan, menyaksikan dan meyakinkan.[22]R.Subekti mengemukakan bahwa membuktikan ialah meyakinkan hakim tentang kebenaran dalil atau dalil-dalil yang dikemukakan dalam suatu persengketaan.[23]

Cyberstalking termasuk salah satu bentuk *cybercrime.* Undang-undang yang digunakan untuk mengatasi *cybercrime* adalah UU no. 19 Tahun 2016 tentang perubahan UU no. 11 tahun 2008 tentang Informasi dan Transaksi Elektronik. Hal ini tidak terlepas dari proses penegakan hukumnya salah satunya yaitu penegakan hukum pidana, artinya menggunakan hukum pidana kepada orang yang melakukan tindak pidana menurut UU ITE. Singkatnya hukum acara pidana dijalankan oleh aparat penegak hukum agar dapat memintai pertanggungjawaban pidana kepada pelaku pelanggaran UU ITE.

Berkaitan dengan itu, penyidikan adalah tahap awal dalam pengumpulan bukti oleh penyidik. Pasal 42 menyebutkan bahwa: "*Penyidikan terhadap tindak pidana sebagaimana dimaksud dalam undag-undang ini dilakukan berdasarkan ketentuandalam hukum acara pidana dan ketentuan dalam undang-undang ini*". Selanjutnya, dalam pasal 43 ayat (1) disebutkan bahwa: "*Selain penyidik Pejabat Polisi Negara Republik Indonesia, Pejabat Pegawai Negara Sipil tertentu di lingkungan Pemerintah yang lingkup tugas dan tanggung jawabnya di bidang*

[22] Lilik Mulyadi, *Pembalikan Beban Pembuktian Tindak Pidana Korupsi* (Alumni 2007).[84].
[23] R. Subekti, *Hukum Pembuktian*, Cetakan ke-17 (Pranadya Paramita 2008).[1].

teknologi informasi dan trasnsaksi elektronik diberi wewenang khusus sebagai penyidik sebagaimana dimaksud dalam undang-undang tentang hukum acara pidana untuk melakukan penyidikan tindak pidana di bidang ITE".

Berdasarkan rumusan kedua norma hukum tersebut, bisa diuraikan beberapa hal, yakni *pertama*, penyidikan sebagai tahap awal pengumpulan bukti secara umum mengacu pada KUHAP menyangkut alat bukti yang rujukannya merupakan pasal 184 sampai dengan pasal 189. *Kedua*, rujukan selanjutnya mengenai pengumpulan bukti dalam tahap penyidikan adalah berdasarkan UU ITE, jika diatur yakni penyidik Polri dan Penyidik Pegawai Negeri Sipil (PPNS) di bidang ITE.

UU ITE juga mengatur mengenai penyidikan, penuntutan, dan pemeriksaan di sidang pengadilan alat bukti pada pasal 44 yang menyebutkan:

a. *alat bukti sebagaimana dimaksud dalam ketentuan perundang-undangan*.
b. *alat bukti lain berupa informasi elektronik dan/atau dokumen elektronik sebagaimana dimaksud dalam Pasal 1 angka 1 dan angka 4 serta Pasal 5 ayat (1), ayat (2), dan ayat (3)*.

Pembuktian atas tindakan *Cyberstalking* masih belum dicantumkan dalam peraturan perundang-undangan sehingga menimbulkan problematika dalam aspek legalitasnya. Seperti yang dijelaskan pada bab sebelumnya, tindakan tersebut digolongkan sebagai salah satu bentuk *cybercrime* yang harus dibuktikan untuk melindungi hak-hak korban. Oleh sebab itu penulis menekankan beberpa poin yang perlu diperhatikan dalam pembuktian tindakan *Cyberstalking* sebagai berikut:

a. Menerapkan alat bukti minimum: Prinsip alat bukti minimum tetap harus diperhatikan. Untuk menyatakan seseorang bersalah, maka diperlukan setidaknya dua alat bukti dan keyakinan hakim. Dalam kasus seperti ini, bukti yang dapat diajukan akan didominasi oleh alat bukti digital seperti misalnya *screenshoot* pesan yang dikirim, bukti riwayat interaksi melalui media sosial.
b. Mempertimbangkan keterangan terdakwa: Dalam bab sebelumnya telah diuraikan bahwa *cyberstalker* memiliki kriteria masing-masing dengan tujuan yang berbeda. maka perlu diperhatikan hal-hal yang dilakukan, diketahui dan dialaminya sendiri. Dalam pembuktian, terdakwa masih bisa membela diri

dengan mengajukan bukti lain yang bisa menyatakan bahwa dirinya tidak bersalah.[24]

c. Petunjuk: Alat bukti petunjuk merupakan otoritas penuh dan subjektivitas hakim yang memeriksa suatu tindak pidana. Hakim dalam mengambil kesimpulan tentang pembuktian sebagai suatu petunjuk haruslah menghubungkan alat bukti satu dengan alat bukti lainnya dan memiliki persesuaian antara satu dengan yang lain. Petunjuk sebagai alat bukti dalam perkara pidana merujuk pada kejujuran hakim itu sendiri yang dipercaya yang melalui pengamatannya di persidangan hakim akan menemukan keyakinan bersalah atau tidaknya terdakwa.[25]

Kesimpulan

Cyberstalking merupakan kegiatan menguntit yang dilakukan berulang kali melalui media elektronik. Kegiatan ini dapat berdiri sendiri sekaligus masuk ke ranah *cybercrime* apabila terdapat indikasi pelecehan, mengancam, memeras hingga berujung pada kekerasan psikis. Negara Indonesia belum mengatur *stalking* maupun *cyberstalking* namun lain halnya di beberapa negara di luar Indonesia seperti California, New South Wales dan Arizona dimana negara-negara bagian tersebut telah mengatur secara jelas dalam undang-undang dan memberikan sanksi yang tegas terhadap pelaku. pidana merupakan hal yang harus dikenakan pada seorang pelaku kejahatan termasuk para *cyberstalker*. Perbuatan cyberstalking dapat dihubungkan dengan ketentuan UU ITE Pasal 29dengan mengkualifikasikannya sebagai delik aduan. Dilanjutkan dengan pembuktian Cyberstalking berdasar pada pengaturan alat bukti elektronik dalam Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik diatur dalam bab III tentang informasi, dokumen, dan tanda tangan elektronik, serta Pasal 44 Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik. Pasal 5 ayat (1) UU ITE mengatur secara tegas bahwa informasi atau dokumen elektronik dan/ hasil cetaknya merupakan alat bukti hukum yang sah. dan disertai dengan prinsip

[24] Hariman Satria, *Hukum Pembuktian Pidana: Esensi dan Teori* (Rajawali Pers 2021).[89].
[25] *ibid*.[65].

alat bukti minimum, petunjuk serta pertimbangan terdakwa. Perlu pula urgensi pengaturan *Cyberstalking* dalam UU ITE disertai ruang lingkup dan batasan-batasannya mengingat bahwa akibat yang ditimbulkan serta motivasi dari pelaku bermacam-macam. Seperti halnya undang-undang mengenai *stalking* yang dimiliki oleh negara-negara di luar Indonesia, pembentuk undang-undang dapat mengambil referensi dari produk hukum luar negeri untuk merumuskan hukum baru.

Daftar Bacaan

Buku

Admaja Priyatno, *Kebijakan Legislasi Tentang Sistem Pertanggungjawaban Pidana Koorporasi Di Indonesia* (Utomo 2004).

Fajar Junaedi, *Etika Komunikasi di Era Siber* (Raja Grafindo Persada 2020).

Hariman Satria, *Hukum Pembuktian Pidana: Esensi dan Teori* (Rajawali Pers 2021).

John E. Douglas, Robert Ressler, Ann Burgess, Allen G. Burgess, *Crime Classification Manua l*(Wiley 2013).

Junaedi Effendi, *Cepat dan Mudah Memahami Hukum Pidana* (Prenada Media 2016).

Leslie Ramos Salazar, *Handbook of Research on Cyberbullying and Online Harrasment in the Workplace* (Business Science Reference 2020).

Lilik Mulyadi, *Pembalikan Beban Pembuktian Tindak Pidana Korupsi* (Alumni 2007).

National Centre for *Cyberstalking* Research, *A Practical Guide to Coping with Cyberstalking* (Andrews UK Limited 2015).

Paul Bocij dan Leroy Mcfarlane, *Cyberstalking: A New Challenge for Criminal Law* (Lecture at Criminal law Nottingham Trent University 2002).

Peter Vronsky, *Serial Killers* (Berkley Books 2004).

R. Subekti, *Hukum Pembuktian*, Cetakan ke-17 (Pranadya Paramita 2008).

Robert hazelwood, *Practical Aspects of Rape Investigation A Multidisciplinary*

Approach (CRC press 2008).

Rosa Agustina, *Perbuatan Melawan Hukum* (Penerbit Pasca Sarjana FH Universitas Indonesia 2003).

Teguh Arifiyandi dan Joshua Sitompul, *Gadgetmu, Harimaumu (Tips Melek Hukum di Medsos)* (Literati 2015).

Jurnal

Rahel Octora. 'Problematika Pengaturan Cyberstalking (Penguntitan di Dunia Maya) Dengan Menggunakan Anonymous Account Pada Sosial Media' (2019) 11 Dialogia Iuridica.

Skripsi

Brenda Charlotte, *Cyberstalking Sebagai Perbuatan Melawan Hukum Dan Pengaturannya Dalam Hukum Pidana Indonesia*, **Skripsi**, (2014) Program sarjana Universitas Katolik Parahyangan.

Perundang-Undangan

Burgelijk Wetboek (Staatsblad 1847 Nomor 23).

Kitab Undang-Undang Hukum Pidana.

Kitab Undang-Undang Hukum Acara Pidana.

Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik Sebagaimana Telah Diubah dengan Undang-Undang Nomor 19 Tahun 2016.

Arizona Statute (ARS) 13-2923 Stalking Law.